Review Article

Threat Analysis and Risk Assessment for Connected Vehicles: A Survey

Feng Luo , Yifan Jiang , Zhaojing Zhang , Yi Ren , and Shuo Hou

School of Automotive Studies, Tongji University, Shanghai 201804, China

Correspondence should be addressed to Yifan Jiang; 1811022@tongji.edu.cn

Received 14 July 2021; Revised 23 August 2021; Accepted 8 September 2021; Published 22 September 2021

Academic Editor: George Drosatos

Copyright © 2021 Feng Luo et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid development of connected vehicles, people can get a better driving experience. However, the interconnection with the external network may bring growing accidents caused by cybersecurity vulnerabilities. As a result, automakers are paying more attention to cybersecurity and spending more cost on developing cybersecurity defense mechanisms. Threat analysis and risk assessment (TARA) is an efficient method to ensure the defense effect and greatly save costs in the early stage of vehicle development. It analyzes the threat of vehicle systems and determines the hierarchical defense and corresponding mitigations according to the potential threat to the system. This paper gives an overview of threat analysis and risk assessment in the automotive field. First, a novel classification of different TARA methods has been proposed. The existing methods have been analyzed and compared. Then, we have found some commonly used tools applied to TARA and compared their performance. After that, a concept named attack-defense mapping is proposed to figure out how to map the already found threats and vulnerabilities of the system to the appropriate mitigations. At last, the future development directions of TARA in the automotive domain have been discussed.

1. Introduction

In recent years, with vehicles becoming more intelligent and connected, the automotive system is much more complex. Increasing connections with the external network of vehicles and functions realized by software can lead to a greater possibility of vehicles being used by hackers, criminals, and even terrorists. At the same time, the development of vehicle automatic driving increases the autonomy control right of the vehicle system, making vehicle system intrusion more harmful. The diversified and multidimensional attacks faced by the intelligent and connected vehicle may lead to privacy and safety threats and even national security threats.

For this reason, many countries have put forward higher standards and requirements for automotive cybersecurity, such as WP.29, which will be implemented soon. Automotive manufacturers attach great importance to strengthening the cybersecurity protection of their products. Many security solutions to provide automotive cybersecurity protection have been proposed. However, the existing security solutions provide mostly passive and single protection

for a specific security problem, so the cybersecurity problem cannot be solved immediately [1]. By identifying and evaluating potential cybersecurity threats and risks, TARA approaches can help find potential threats in the early stage of development and provide theoretical support for selecting mitigation measures. However, there is a lack of a review of TARA methods and tools in the automotive field, as well as how to use appropriate mitigation measures to mitigate the corresponding threats in theory. This study conducts a systematic review of current research that aims at TARA in the automotive field. The present study investigates the existing TARA methods in the automotive field and extracts the characteristics of the proposed methods. Common tools used in TARA are also described. In addition, this study explores the mapping relationship between threats and corresponding mitigation measures.

The rest of the paper is organized in the following way: Section 2 describes the procedure undertaken for performing a systematic literature review (SLR). Section 3 presents threat analysis and risk assessment methods. In Section 4, threat analysis and risk assessment tools are

analyzed and compared. A novel concept named attack-defense mapping is discussed in Section 5. In Section 6, the future directions of threat analysis and risk assessment developments are discussed before we sum up our paper with a conclusion in Section 7.

2. Research Methodology

2.1. Research Question Definition. The main objective of this paper is to present a picture of the recent research work about TARA methods in the automotive context. We have thus formulated the following research questions, and this step is the soul of the paper:

RQ1. What are the threat analysis and risk assessment methods used to evaluate the cybersecurity status of the vehicle?

RQ2. What tools could be applied to threat analysis and risk assessment?

RQ3. How to match the threats and vulnerabilities of the system to the appropriate mitigation measures?

RQ1 aims to explore what threat analysis and risk assessment methods are used in the automotive context. RQ2 aims to find out what tools could be applied to threat analysis and risk assessment. RQ3 aims to figure out how to match the threats and vulnerabilities of the system to the appropriate mitigation measures after finding out the threats and vulnerabilities.

2.2. Search Process. The complete searching process of this literature review involves the following stepwise process.

2.2.1. Database Selection. The digital libraries selected for this survey include the following:

- (i) IEEE Xplore Digital Library (<https://ieeexplore.ieee.org/>)
- (ii) Springer (<https://link.springer.com/>)
- (iii) Science Direct (<https://www.sciencedirect.com/>)
- (iv) ACM Digital Library (<https://dl.acm.org/>)
- (v) Wiley Online Library (<https://onlinelibrary.wiley.com/>)

2.2.2. Search Terms. In the next step of the study, we have specified the search string used to find relevant publications in selected databases. We specify the following Boolean string to search the relevant databases:

(risk **OR** vulnerability **OR** threat) **AND** (analysis **OR** assessment **OR** evaluate) **AND** (security) **AND** (vehicle **OR** automotive).

2.2.3. Search Procedure. The initial step of the search involves selecting literature using the search string described above. The second step is to filter literature by inclusion or exclusion criteria. The third step is to filter literature by selecting relevant titles and keywords. The fourth step is to

choose from the literature through screening abstracts. Finally, the full-text papers to be reviewed are obtained. The complete process from initial selection to full-text selection is summarized in Figure 1.

2.3. Selection Criteria. The research scope of this paper is from January 1, 2010, to March 31, 2021. The criteria for screening related research work should be predefined to eliminate ambiguity in the screening process. Therefore, the following inclusion criteria were considered:

- (i) Papers focus on security issues in the area of automotive
- (ii) Papers are peer-reviewed

The following criteria state when a paper was excluded:

- (i) Papers are not written in English
- (ii) Papers are not accessible in full text
- (iii) Papers are duplicates of other studies

2.4. Screening Results. Initial search has shown that there is a considerable number of research papers about the stated research questions. The search procedure was performed with an initial total number of papers being 29527. Out of the total 29527 papers, 392 papers were chosen after considering the inclusion criteria (IC) and exclusion criteria (EC). 139 papers are then selected after going through the titles and keywords. In the remaining 139 papers, snowballing was done to cover accidentally missed out papers, and then the number reached 170. Out of 170 papers, 111 were included after studying the abstracts. In the end, 38 papers were selected for the study of full text and were deemed to have the potential for answering the given research questions. A detailed description of the figures of each phase is mentioned in Table 1.

3. Threat Analysis and Risk Assessment Methods

In the development process of intelligent and connected vehicles, TARA is mainly in the relatively early development stage. Through the threat modeling and risk assessment of the intelligent and connected vehicle cyber-physical system, the risk value of potential threats can be reduced to an acceptable level at a low cost. Then, the cybersecurity level of vehicles can be improved. Figure 2 shows the process of threat analysis and risk assessment.

TARA is mainly divided into three steps:

- (i) Threat analysis: able to identify some potential threats in automotive systems
- (ii) Risk assessment: able to analyze and classify the identified threats and evaluate the corresponding risks
- (iii) Risk analysis: sorting the threats according to the risk level and determining whether the risk associated with a specific threat is at an acceptable level or whether measures to reduce the risk are needed [3]

FIGURE 1: Search and selection process.

In this section, TARA methods are divided into two categories, namely, formula-based methods and model-based methods. Formula-based methods are methods for threat analysis and risk assessment of the system, mainly through tables, texts, or formulas. Formula-based methods are divided into three types according to their different concerns: asset-based methods, vulnerability-based methods, and attacker-based methods. Model-based methods are a type of threat analysis method that uses a

variety of different models, modeling and analyzing the threats and risks of the system through data flow diagrams, graphs, and tree models. Model-based methods are divided into two types according to their different concerns: graph-based methods and tree-based methods. Model-based methods perform threat analysis on the system through different models, so they are more objective. The accuracy of the quantitative analysis results and the reproducibility of the analysis results are higher. However, this type of methods is also more complex and therefore more difficult to understand and use. Figure 3 presents a taxonomy of TARA methods which will be discussed in the following sections.

3.1. Formula-Based Methods

3.1.1. Asset-Based Methods. The asset-based approach is the most common type of TARA method in the automotive domain. This series of methods first identifies the final target asset under attack and then exhausts the attack paths and attack methods that can pose a threat to this target asset through the use of relevant experience and minds of security experts so that advance prevention can be carried out. This method is also known as a “top-down” method.

CERT/CC (Computer Emergency Response Team/Coordination Center) released OCTAVE in 1999. The OCTAVE method has become one of the mainstream TARA methods in the world. The OCTAVE methodology is an approach that divides the assessment into three phases in which management issues and technical issues are examined and discussed so that the organization’s staff can take full ownership of the organization’s information security needs. The OCTAVE method is characterized as an assessment approach that combines assets, threats, and vulnerabilities. It allows managers to use the results of the assessment to determine the OCTAVE method, which is characterized by a combination of asset, threat, and vulnerability assessments. In addition, managers can use the results of the assessment to prioritize risks to be addressed. It also incorporates how the computing infrastructure is used and its role in achieving the organization’s business objectives. OCTAVE is integrated with the interrelated technical aspects of computing infrastructure configuration. It also allows for a flexible, customizable, and repeatable approach that can be customized according to the needs of different organizations.

The EVITA method is an asset-based threat analysis method. This method provides a cost-effective security architecture that can provide comprehensive security in different development phases such as design, verification, and prototype for vehicle networks. The EVITA method performs an attack assessment for each asset in the system and then assesses the level of risk that the attack may cause. Risk is a function of the attack likelihood and the severity of the harm caused by the attack. Based on these, the threats are risk-rated, and the threat priority is determined [4]. The EVITA risk assessment method can be applied to assess potential threats. The identified potential threats can be ranked according to the risk level to further focus the analysis on the highest risk threats. Then, the network

TABLE 1: Paper filtering for each phase.

Digital library	Initial selection	Inclusion/exclusion criteria	Titles and keywords	Snowballing	Abstracts	Full-text selection
IEEE Xplore	901	109	51	66	42	15
Science Direct	191	16	15	17	15	5
Springer	17280	188	43	50	32	9
ACM	5039	69	25	32	17	7
Wiley	6116	10	5	5	5	2
Total	29527	392	139	170	111	38

FIGURE 2: The process of threat analysis and risk assessment [2].

FIGURE 3: The process of threat analysis and risk assessment.

security goals can be determined for the highest risk threats. However, the EVITA method only provides an evaluation method and does not provide a complete evaluation process, which will bring trouble to users. HEAVENS method makes up for this defect. Figure 4 shows the workflow of HEAVENS. The combination of security objectives and level of impact during threat analysis helps to assess the potential business impact of a threat on relevant stakeholders. HEAVENS is, therefore, a very suitable assessment method for evaluating the information security risks of automotive electronic and electrical systems. At the same time, the

HEAVENS method provides a detailed process of threat analysis and risk assessment, which greatly reduces the difficulty of use and increases the feasibility of the method, which is also a prerequisite for its widespread use.

The BRA (Binary Risk Analysis) assesses the assets to be protected in the system by implementing a process. The BRA method can be used for quick risk conversations to discuss specific risks in just a few minutes. Nevertheless, the resulting risks are only classified as high, medium, or low. Furthermore, a conservative analysis trend leads to threat classification solely of high risks. Additionally, no structured estimation of threat scenarios is given, and the resulting threat classification is too rudimentary for concept development phases. SHIELD is a multimetric approach to evaluate the system's level of security, privacy, and dependability. The main goal of this method is to evaluate multiple system configurations and select those that meet or achieve established requirements [5, 6]. In the NHTSA approach, all relevant onboard components and systems have been considered, and the data flow and the trust boundary between the components can be visually observed [7].

The SGM (Security Guide-word Method) makes it easy for non-security engineers to identify information assets and protection objectives. We derived ten guide words, namely, disclosure, disconnection, delay, deletion, stopping, denial, trigger, insertion, reset, and manipulation [8]. The policy-based security model can be customized according to the security requirements of the use case, and a flexible security model that is manageable and adaptable during the device life cycle is provided. By using policies to enforce security requirements, OEMs do not need to rely on the security assurances of third-party vendors. Implementation strategies can ensure that the equipment operates as expected by the OEM. If the security requirements of the device change after production; for example, a new vulnerability is discovered, the OEM can issue a policy definition update [9].

The threat analysis methods above focus on the qualitative analysis of threat levels, while other asset-based methods can quantitatively analyze risks. TVRA can define the risk level of a system based on the likelihood of an attack occurring and the impact of an attack on the system. TVRA can output a quantitative measure of system asset risk and a detailed set of security measures to minimize system risk [10]. The US² (Unified Safety and Security) uses a simple quantitative scheme to evaluate safety hazards and safety threats in parallel and effectively derive safety and security requirements [11].

In addition, there is a special type of asset-based approach, which uses software as the main protection target asset of the system. In this article, it is called the software

FIGURE 4: Workflow of the HEAVENS method [3].

logic-based approach. Macher et al. [12] proposed a method called SAHARA, which incorporates the STRIDE threat model. SAHARA enables the quantification of the probability of the occurrence and impacts of security issues on safety goals. The basic classification is aligned with ASIL classification and is thus optimal for use in combined security and safety engineering processes. The software vulnerability analysis method checks whether the software code of known software construction should be avoided to prevent potential vulnerabilities [3].

The asset-based methods focus on various forms of assets in the system. As an automobile is essentially a cyber-physical system, the ultimate goal of cybersecurity in the automotive domain is to protect the automotive system from attack and thus to operate normally. Therefore, the asset-based threat analysis and risk assessment approach is also most suitable for the automotive domain.

3.1.2. Vulnerability-Based Methods. Corresponding to the asset-based methods, the vulnerability-based methods are “bottom-up” TARA methods. They start with a vulnerability or weakness found in a system and then analyze what other larger vulnerabilities or failures the vulnerability could cause.

CVSS (Common Vulnerability Scoring System) is an industry open standard designed to help determine the urgency and importance of the required response. The main purpose of CVSS is to help establish a standard for measuring the severity of vulnerabilities so that the severity of vulnerabilities can be compared and the priority of dealing with them can be determined. CVSS scores are based on measurement results on a series of dimensions, which are called metrics. The CVSS includes three types of scores: base, temporal, and environmental metric.

FMVEA expands the security attributes based on FMEA, turning it into a safety and security coanalysis method. Its failure modes can analyze how components’ quality attributes fail, and threat modes are used to analyze how security attributes fail. Recognizing threat agents can estimate the frequency of threat modes, and the probability of occurrence of threats mode is determined by the threat agents and vulnerabilities [13]. The whole process of the CHASSIS

analysis method is divided into two steps to define functionality, safety, and security requirements. The first step mainly defines the functional requirements for the subsequent introduction of safety and security requirements. In the second step, the main focus is on the introduction of safety and security requirements. This step will rely on the brainstorming of relevant security experts in the field to propose some possible misuse scenarios as an important basis for the overall analysis results. For this reason, there are too many subjective factors in the analysis method of CHASSIS [14]. In [14], the two methods FMVEA and CHASSIS are compared in terms of six aspects: level of abstraction, comparability of repeated analysis, reusability of analysis artifacts, scope of analysis, suitability for a risk rating, and adaptability to changing context through an automotive FOTA (firmware over the air) application scenario. Moreover, in NIST SP 800-30 “Risk Management Guide for Information Technology Systems,” a methodology is proposed to conduct a risk assessment in nine sequential steps [14].

The ANP (Analytical Network Process) matrix approach can easily and effectively consider the dependencies and conflicts between attributes for joint evaluation [15]. It helps to make wise design decisions to reduce the number of design iterations. In the matrix, the hierarchical fault propagation and threat propagation structures are defined, and the interconnection between them is considered, thereby giving a network structure. The authors in [16] use three examples to analyze the effect of the cyber kill chain method. Cyber kill chain refers to the process of analyzing network attacks to identify threats to the organization at each stage of the attack, smashing and mitigating the purpose of the attacker, and planning and implementing measures to protect the organization’s system. Compared with the benchmark test, VeRA (Vehicles Risk Analysis) uses a simplified analysis process and fewer factors, thereby greatly reducing the required analysis time without affecting the accuracy of the analysis. In addition, based on VeRA, a simple and effective mathematical model is established to evaluate the risk value by considering the attack probability, severity, and human control, thereby avoiding the cumbersome process of looking up tables in the previous methods [17].

The vulnerability-based methods can find the vulnerabilities in the system and then further analyze the hazards and risks that the vulnerability may cause to the system. If these methods are combined with a rich vulnerability database, they can perform a more comprehensive vulnerability scan of the system. This type of approach makes it possible to use a database of vulnerabilities with a large number of vulnerabilities to analyze each vulnerability that could cause failure damage to the system. It can effectively avoid damage to the security of the system caused by the vulnerability.

3.1.3. Attacker-Based Methods. The attacker-based method is a type of threat analysis method that analyzes attackers. It conducts threat analysis and risk assessment of the system through the knowledge level of possible attackers, attack paths, attack motivations, and number of resources possessed. In this way, the threat can be modeled and analyzed from the root cause of the attack.

SARA is an improved security risk analysis framework for automated driving system-dedicated vehicles, including the opinions of security experts, new threat models, attack methods, asset maps, and attack tree definitions. In addition, SARA defines a new metric that considers driver or automated driving system controllability for the computation of the risk value [18]. SAM (Security Abstraction Model) closely combines safety management and model-based system engineering through an abstract description of the principles of automotive security modeling [19].

The Threat Agent Risk Assessment method is performed in six steps, and its goal is to find the critical exposure of the connected car. Threat Agent Risk Assessment method is composed of TAL (Threat Agent Library), MOL (Methods and Objectives Library), and CEL (Common Exposure Library). The Threat Agent Risk Assessment method can identify a list of possible attacks and rank these attacks according to the likelihood of occurrence [20]. However, the Threat Agent Risk Assessment method is fairly new, and there is almost no supporting documentation except for the very little content released by Intel Security. Therefore, other work must be done to successfully apply this method to the automotive industry. The Bayesian Stackelberg game methodology models the attack and defense process as a network security Stackelberg game. It provides the best hybrid strategy for the attacker and the Internet of Vehicle defense system, with the latter optimally deploying the available security resources in the transportation infrastructure to minimize the impact of attacks and improve their detection. The game belongs to the Bayesian type. According to the probability distribution determined by the strict risk assessment method, several types of data corruption attacks are considered [21]. Compared with a unified defense design that does not matter to the attacker's strategy and type, this method can reduce the impact of advanced persistent threats. This solution can be integrated into the design of the Internet of Vehicle intrusion detection system to improve its robustness.

Formula-based TARA methods are more mature and more convenient for users without too much security

experience. As a result, they are more widely spread and used. Table 2 shows the classification of the formula-based TARA methods. This classification helps to identify TARA methods with common characteristics. In addition, Table 2 describes the characteristics of each method and whether the method is a coanalysis method that takes into account both security and safety aspects.

3.2. Model-Based Methods

3.2.1. Graph-Based Methods. The graph-based methods are connected through nodes and directional edges. Graph-based methods can express the direct mathematical quantitative relationship of each node module, which provides convenience for the quantitative threat analysis of the system.

The STRIDE model consists of spoofing (S), tampering (T), repudiation (R), information disclosure (I), denial of service (D), and elevation of privilege (E). The STRIDE method has been widely used in the IT industry and has proven to be able to identify and analyze the threats in the system, which can effectively reduce the risk of the system being attacked. Due to its outstanding effect, the STRIDE method is gradually being applied in other fields. The STRIDE method is also recommended in the field of automotive information security in the SAE J3061 regulations.

In addition to the STRIDE method, UcedaVelez [23] developed a seven-stage threat analysis method called PASTA (i.e., Process for Attack Simulation and Threat Analysis) in 2012 [23]. PASTA's use of data flow diagrams is at the application decomposition layer. The LINDDUN (i.e., linkability, identifiability, nonrepudiation, detectability, disclosure of data, unawareness, and noncompliance) method provides data security and privacy protection for the system through a six-step analysis [23]. It uses data flow diagram iterative model elements to analyze and detect different types of threats. The VAST (i.e., visual, agile, and simple threat) method can be extended and can be applied to large-scale threat model analysis [23].

The advantage of the Markov chain method is that the time dimension is introduced into the threat analysis of the system. This method believes that the next state of the system is completely determined by the current state, which makes the threat analysis of the system enter a dynamic space. As a dynamic method, it enriches the dimension of the entire threat analysis by expressing the attack steps and simulating the corresponding defending methods. In addition, the Markov chain also provides the possibility of quantitative analysis of threat analysis, making the results of threat analysis of the entire system more intuitive and convincing [24–26]. The Bayesian network method uses the graph-based model to quantitatively evaluate the possibility of threats to vehicle components. It is used to obtain the relevant security risks and to achieve the security measures of the model. The Bayesian defense graph can also conduct threat analysis

TABLE 2: Formula-based TARA methods.

Category	Subcategory	Method	Brief description	Characteristics	Coanalysis
Formula-based	Vulnerability-based	EVITA method [4]	EVITA is a part of a European commission-funded research project (EVITA: E-safety vehicle intrusion protected applications).	In EVITA, security threats are classified from different perspectives: operations, security, privacy, and finance. EVITA is a suitable approach for concept evaluation but requires too many details for classification.	Yes
		HEAVENS [3]	HEAVENS is a method for threat analysis and risk assessment of automotive electronic and electrical systems.	The STRIDE threat modeling approach brings additional support structuring for the estimation of threat scenarios. It has a wide range of applicability and can be applied to passenger cars and commercial vehicles.	Yes
		OCTAVE	OCTAVE stands for operationally critical threat, asset, and vulnerability evaluation.	It is flexible, tailorable, and repeatable.	No
		BRA [5, 6]	BRA is a lightweight qualitative open license risk assessment.	It is fast and convenient but is relatively rudimentary, and it is difficult for it to conduct an overall threat assessment of complex systems.	No
		SHIELD [5, 6]	SHIELD is a method for assessing the security, privacy, and dependability of embedded systems.	It considers security, privacy, and dependability.	No
		TVRA [10]	Threat, vulnerability, and risk analysis (TVRA) identifies assets in the system and their associated threats by modeling the likelihood and impact of attacks.	It provides the possibility for a more detailed analysis of threats.	No
		SGM [8]	This method is based on security guide words, which allow a structured identification of possible attack scenarios.	It is easy to use and can reduce the workload of analysts.	Yes
		US ² [11]	This method uses a simple quantitative scheme to simultaneously assess security risks and security threats.	The quantitative method of US ² is less complicated and requires less analytical work.	Yes
		Policy-based security modeling [9]	This method is a strategy-based security modeling method, which uses a configurable strategy engine to apply new strategies to deal with serious threats.	This method allows the strategy to be updated to deal with new threats; otherwise, the product may need to be redesigned to alleviate the problems under the traditional method.	No
		NHTSA [7]	This method uses a threat matrix in the technical report of the US National Highway Traffic Safety Administration (NHTSA).	It can display the system intuitively.	No
	Attacker-based	SW vulnerability analysis	The method could find vulnerabilities in codes.	The software code of the known software structure can be checked to prevent potential vulnerabilities, but this method is aimed at the software development level, so it is not suitable for the early development stage.	No
		SAHARA [12]	SAHARA (security-aware hazard analysis and risk assessment) is an expansion of the inductive analysis method called hazard analysis and risk assessment (HARA) and encompasses threats of the STRIDE threat model.	It is able to quantify the possibility and impact of threats.	Yes
		CVSS	CVSS captures the main attributes of vulnerabilities and generates numerical and textual forms of scores representing the severity of the vulnerabilities.	CVSS provides vulnerability priority and an open framework.	No
		FMVEA [13]	FMVEA is based on the FMECA and extends the standard approach with security-related threat modes.	This method can identify the frequency and probability of threat modes.	Yes
		CHASSIS [14]	CHASSIS is a systematic method for an information system to analyze safety and security interactively by using HAZOP guide words.	CHASSIS can easier adapt to different scenarios and environments and is more suitable for dynamic system analysis, but it depends too much on expert knowledge.	Yes
		ANP matrix [15]	The ANP matrix method allows a combined risk assessment that considers dependencies and conflicts among attributes. This approach provides risk assessment results for different dependability attributes.	It considers the relationship between failures and threats and the impact of propagation and can reduce the number of design iterations.	Yes
		Cyber kill chain [16]	The cyber kill chain consists of seven levels. The seven levels are reconnaissance, weaponization, delivery, utilization, installation, command and control, and target action.	This methodology is good at analyzing cyberattacks, threats, or vulnerabilities related to the automotive industry.	No
		VeRA [17]	Vehicle risk analysis (VeRA) is suitable for assessing the risk of attacks to autonomous vehicles and connected autonomous vehicles. VeRA is the first task that considers human capabilities and vehicle automation levels when assessing safety risks.	It can reduce the time required for the risk assessment process.	No
	Attacker-based	NIST SP 800-30 [22]	This method is proposed in NIST SP 800-30 and can be used to identify, estimate, and prioritize various risks for security-critical targets.	Security-critical systems are considered.	No
		Threat Agent Risk Assessment [20]	The threat modeling was carried out with the support of domain experts and the project manager responsible for the Threat Agent Risk Assessment method in Intel's Security Department.	It has clear organization, is easy to understand and operate, and is able to adapt according to the dynamic structure.	No
		SAM [19]	SAM is a proposal to extend the attachment of EAST-ADL with the security modeling function, which is not covered by the current existing language specifications.	The SAM method clarifies the difference between security modeling and functional safety modeling. The language specification is defined for the security abstract model of the automobile system modeling environment.	Yes
		Bayesian Stackelberg game [21]	This method is a resource-aware Bayesian Stackelberg game whose goal is to provide IDS with the best detection load distribution strategy for the set of RSUs monitored in the transportation network, while maximizing detection of multiple types driven by advanced persistent threats.	This method only needs to solve a mixed integer linear program (MILP) and does not need to solve a set of linear programs proposed by other solutions, so it can further improve the performance.	No
		SARA [18]	SARA is a systematic threat analysis and risk assessment framework, including improved threat models, new attack methods, asset maps, attackers' participation in the attack tree, and new driving system observation indicators.	SARA provides a framework for security experts to participate in the security process.	Yes

with corresponding mitigation measures, which can provide a reference for security defense design [27, 28].

The GTS (graph transformation system) method is a formal method of transforming the system structure graph that follows certain rules. The entire graph transformation system can be abstracted as a tuple (G, R) , where G represents the graph and R represents a series of transformation rules. The GTS method contains three transformation rules, which are used to describe the behavior of services, the normal behavior of the hardware components, and the attack actions. With the help of transformation rules, GTS can easily and quickly realize the conversion between the overall architecture and the module architecture, which is very beneficial for OEMs in the development of large-scale projects. At the same time, [29] also introduces the conversion method from attack graph to attack tree, which establishes a mapping relationship between the two threat analysis methods. Accordingly, the system can be analyzed from multiple dimensions.

UML is a universal graphical modeling language used to specify, design, and verify complex hardware and software systems, as well as the organization and program workflows. UML use cases and state machines can be used to represent attack scenarios. In [30], a UML-based metamodel is developed specifically for autonomous vehicles, attacks, and defense measures. UML-based analysis methods have many advantages. UML symbols have good semantics and will not cause ambiguity. The visual model based on UML makes the system structure intuitive and easy to understand. Modeling the software system with UML is not only conducive to the communication between system developers and system users but also conducive to system maintenance. However, UML language is more costly for nonprofessional engineers to learn. SysML-Sec is a method that combines a target-oriented method for obtaining requirements and a model-oriented method for threats and system architecture. Its analysis process is based on Y-chart and V-cycle models. It can cover all design and development stages [31].

Schmittner et al. [32] proposed improvements when applying STPA-Sec for security and safety coanalysis and identified several limitations of STPA-Sec. STPA-Sec will output a list of system-level scenarios that can cause losses. The threat analysis process of the STPA-Sec method can be divided into four steps. The first step is to establish basic system engineering. The second step is to build a high-level control structure model. The third step is to identify unsafe or risky control actions. The fourth step is to develop security requirements and constraint causal scenarios. In addition, given the limitations of some terms in the STPA-Sec method that cannot take into account the analysis of safety and security scenarios, the article improves the defect by aligning important terms in the safety and security context. Friedberg et al. [33] extended the STPA method, further refined and integrated the physical and information security analysis process, proposed the control layer and component layer security constraint mapping method, added information security-related attribution factors, and formed the integrated STPA-SafeSec analysis system. The STPA-SafeSec integrated physical security and information security

analysis method uses a unified analysis framework and process, which can not only identify vulnerabilities and loss scenarios at the system level but also further add control constraints and focus on threats. The STPA-SafeSec method includes two core contributions. First, to determine information security constraints, analysts must extend the relatively abstract system control layer to a component layer. Second, the analysis method has expanded the attribution elements to meet the needs of information security analysis.

3.2.2. Tree-Based Methods. Tree-based methods can represent the affinity between nodes and describe the hierarchical relationship between nodes. The most typical of this type of method is the attack tree model, which can express the attack faced by the system and clearly show the attack path.

Attack tree analysis is a threat analysis method that uses a tree as a structure. The general structure of the attack tree is shown in Figure 5. The top event is used to describe the attack target, and the nodes below the attack target represent all possible events that can cause the attack target to occur. The logical relationship between these events can be connected through “OR” gate and “AND” gate. Attack tree analysis can be performed in a top-down manner, that is, first determining the final attack target and then analyzing all possible attack paths according to the attack target. It can be also performed in a bottom-up manner, that is, analyzing possible attack surface and then analyzing the possible vulnerabilities based on this [34]. However, when faced with threat analysis of large systems, the traditional attack tree analysis method requires manual construction of a large number of attack combinations. It is inevitable that attack paths will be lost and the possibility of vehicle systems being attacked will increase, which is unacceptable to the OEMs. In response to this shortcoming of attack tree analysis, Salfer et al. [35] proposed a method for automatically constructing attack forests for automotive networks for software attacks. The algorithm can automatically find the optimal attack path between the attacker and the asset with the aid of the system model. Reference [35] also proves that even in the worst case, this method can complete the threat analysis and security assessment of a large system within a few minutes. This is very beneficial to OEMs, who often need to perform large-scale threat analysis on vehicle systems. The RISKEE method adds probability distributions based on attack tree analysis, thus realizing quantitative risk assessment of security and safety. In addition, the RISKEE method also uses the RISKEE propagation algorithm to calculate risk through forward propagation of frequencies and backward propagation of risk [36]. In addition, The BDMP (Boolean-logic Driven Markov Processes) method expands the ability of fault tree analysis and attack tree analysis to describe threats. Nevertheless, the BDMP method is unsuitable for the early development stage of threat analysis and risk assessment [5, 6].

Compared with formula-based methods, the model-based TARA methods can show the entire evaluated system more completely, thus providing a more intuitive

FIGURE 5: Attack tree general structure.

perspective for the evaluation process. However, the model-based TARA methods use different models, so users need to study the model in depth before using the TARA method to analyze threat analysis on the system. Table 3 shows the classification of the model-based TARA methods and whether these methods take both security and safety into consideration.

How to make a reasonable and objective evaluation of different TARA methods is also a problem that scholars are very concerned about. Different evaluation methods have different application scenarios and different applicable conditions. It is necessary to create a platform for the evaluation process so that different TARA methods can be fairly evaluated on this platform. Table 4 lists the ways to evaluate the TARA method in the literature.

4. Threat Analysis and Risk Assessment Tools

Microsoft Threat Modeling Tool 2016 (MTMT) is a threat modeling and analysis tool based on the STRIDE method, which can help users find potential threats in the early stage of system design. The user should first establish a data flow diagram (DFD) to describe the communication between different components of the system. Then, MTMT automatically detects and analyzes the DFD. Finally, it will present a list of the potential threats in the system. Figure 6 is a DFD established with MTMT, which shows the scenario of information interaction between OBU and RSU. MTMT can also record the results of threat modeling and analysis by generating reports so that users can view them at any time. Although MTMT can accurately and comprehensively display the potential threats in the system, it can neither link the threats with the asset losses caused by the attack nor provide a complete system view for threat analysis and risk management.

SecuriCAD can help users to complete network modeling. It can simulate different types of network attacks and obtain the quantitative results of the system risks. The threat model in SecuriCAD is mainly composed of three components: host, network, and attacker. Figure 7 is a partial model of the 2015 Cadillac Escalade vehicle network constructed by Xiong et al. [38], where host mainly refers to ECUs and network includes CAN, LIN, MOST, and ethernet. These are the assets that need to be protected in the

system. Then, it assigns corresponding security settings to different assets and classifies the impact of different attacks. Finally, SecuriCAD acts as an inference engine to simulate the attacks on the created threat model. The results of the simulation are as follows:

- (i) Risk matrix: according to the consequence and probability, the risks are divided into four levels: critical, high risk, medium risk, and low risk
- (ii) Attack path: it shows the attack path of an attack, which presents the possible composition of vulnerabilities used by an attack; it also shows the likelihood of the attack path
- (iii) Time-to-compromise (TTC): it presents the effort for an attacker to implement a successful attack under a given probability

GROOVE is a tool, which uses simply labeled graphs and single push-out (SPO) transformation rules to transform a general graph. GROOVE can recursively apply transformation rules to a given graph. Karray et al. [29] used GROOVE to model the car architectural graph and transformation rules, in order to construct attack trees and analyze attacks to a connected vehicle. GROOVE can model the network architecture of the vehicle. According to the initial state of the model and the preset conversion mechanism, it can generate the corresponding state space, which is the attack graph. If there are vulnerabilities in a state in the attack graph, this state can be regarded as the root of the attack tree. Then, check the other state in the attack tree, and the corresponding attack tree can be derived.

OMNeT++ is an open-source, modular, component-based C++ simulation library and framework that can be used to simulate vehicle networks. OMNeT++ can easily build network models and has high simulation granularity. In addition, it can also perform network attack simulation and threat analysis. The data recording function can reflect the impact of different types of attacks on the data in the network. Figure 8 shows the network model of automotive ethernet architecture. Santhosh et al. [39] used this tool to establish a Sybil attack model against vehicle queues and evaluated the impact of the attack on vehicle network performance.

Practical Threat Analysis (PTA) is a tool that can be used for threat modeling and automatic calculation of risk assessment results. At first, it needs to set various parameters such as system assets, threats, exploited vulnerabilities, corresponding mitigation measures, attack types, and attack entry points in a PTA project. The threat model is stored in a dynamic database so that the model parameters can support dynamic changes. By continuously revising the parameters of the model, it can ensure that the risk assessment and security management process can be carried out continuously and effectively. Figure 9 shows a threat builder of the replay attack in CAN bus. It constructs a specific threat scenario to show the vulnerabilities that a certain threat can use to attack the assets of the system. At the same time, countermeasures for the threat should be added. Finally, PTA can simulate and calculate information such as the extent of damage to assets and the effectiveness

TABLE 3: Model-based TARA methods.

Category	Subcategory	Method	Brief description	Characteristics	Coanalysis
Model-based	Graph-based	STRIDE (Microsoft)	STRIDE is a threat modeling method that abstracts component elements in the system.	It extends the original confidentiality, integrity, and availability model and is suitable for identifying the relationship between threats, assets, and security attributes.	No
		PASTA [23]	The goal of the PASTA method is to have a risk-centric framework and rely on an attacker-centric perspective to generate asset-centric output.	PASTA uses risk and impacts analysis to improve the weakness of the STRIDE method.	No
		LINDDUN [23]	LINDDUN stands for linkability, identifiability, nonrepudiation, detectability, disclosure of data, unawareness, and noncompliance.	It can ensure data security and privacy protection. However, when the number of threats in the system increases rapidly, the complexity of the system will also increase, which is not conducive to large-scale system analysis.	No
		VAST [23]	VAST stands for visual, agile, and simple threats.	It is extensible and suitable for large system analysis.	No
		Markov chain [24, 25, 26]	Markov chain is a stochastic process with Markov property in probability theory and mathematical statistics and exists in discrete index set and state space.	It is able to make a quantitative analysis of threats. The concept of time is introduced to make the process of threat analysis dynamic. It can model and analyze the attack process and defense process at the same time.	No
		GTS (graph transformation system) [29]	This method is a rule-based modeling approach that allows capturing the structural as well as behavioral aspects of a system.	Its structure is simple, and its logic is clear. It is easy to understand and able to split and combine the structure quickly, facilitating cooperative development.	No
		Bayesian network [27, 28]	Bayesian network is an extension of the Bayesian method. It is one of the most effective theoretical models in the field of uncertain knowledge expression and reasoning, and it is a probabilistic graphical model.	It can realize the quantitative analysis of threat risk. It can be combined with threat analysis methods such as EIVTA and CVSS.	No
		UML-based model [30]	This method proposes a formal framework to detect attack surfaces automatically on systems modeled in UML.	The formal expression is clear and will not cause ambiguity. UML makes the system structure intuitively displayed and easy to understand, but UML language is difficult for nonprofessional engineers.	No
		SysML-Sec [31]	SysML-Sec is a SysML-based model-oriented approach.	It is a coanalysis method that considers safety and is capable of covering all design and development phases.	Yes
		STPA-Sec [32]	STPA-Sec is a top-down safety and security risk analysis method.	This method can analyze the safety and security scenario in the concept phase. However, this method does not consider the network and system architecture. It is difficult for some important terms in this method to take into account both safety and security scenarios.	Yes
Tree-based		STPA-SafeSec [33]	STPA-SafeSec inherits STPA's technical achievements in system theory, attribution models, safety constraints, and hazard control activity analysis. It refines the analysis process framework for information-physical systems and expands the integration of physical security and information security requirements.	Security constraints are added, and the attribution mapping between the control layer and component layer is provided.	Yes
		ATA (attack tree analysis) [34, 35]	Attack tree analysis is a formal and clear method used to describe the security threats faced by the system and the various attacks that the system may be subjected to.	It is able to describe the complex attack process in the form of a tree, but this method requires more details of the system design. Detailed system design is required, so it is not suitable for concept evaluation. In addition, for large systems, the refinement of the attack tree may be a tedious task and error-prone.	No
		RISKEE (risk tree) [36]	RISKEE is based on attack graphs and the diamond model in combination with the FAIR method for assessing and calculating risk.	The RISKEE method can realize the quantitative calculation of risk, but it did not consider the dynamic impact of mitigation measures on the system.	Yes
		BDMP (Boolean-logic Driven Markov Processes) [5, 6]	BDMP is an approach where fault tree and attack tree analysis are combined and extended with temporal connections.	It expands the ability of fault tree analysis and attack tree analysis to describe threats. Nevertheless, BDMP is inappropriate for an early development phase of threat analysis and risk assessment.	Yes

TABLE 4: Ways to evaluate TARA methods.

Study	Evaluation
HAIDAR et al. [10]	They apply TVRA methodology to the pseudonymity mechanisms used for V2X communication aspects of C-ITS.
Dürrwang et al. [8]	They evaluate the effectiveness of the method by letting 30 non-security-professional employees of the University of Applied Sciences in Karlsruhe use the method.
Cui and Sabaliauskaite [11]	They use US ² to analyze the threat of autonomous vehicles and demonstrate the analysis results.
Hagan et al. [9]	They present a realistic use case of a connected car and several attack scenarios.
Macher et al. [12]	They apply the SAHARA approach for an automotive battery management system (BMS). For this specific example, the SAHARA approach identifies more hazardous situations than the traditional HARA (34%) approach.
Schmittner et al. [14]	The scenario they consider is an attack or failure in the firmware over the air (FOTA) functionality.
Lee et al. [16]	Use case 1: enhanced Android app-repackaging attack on in-vehicle network. Use case 2: viable attack path and effective protection against ransomware in modern cars. Use case 3: wireless attack on the connected car and security protocol for CAN.
Halabi et al. [21]	The evaluation is mainly based on the effectiveness of the defense system compared with other defense strategies that do not consider the attacker's ability to launch intelligent attacks.
Monteuuis et al. [18]	They show SARA feasibility with two uses: vehicle tracking and comfortable emergency brake failure.
Karray et al. [29]	They use the modeling of the vehicle speed acquisition system as an example.
Li et al. [27]	A typical dynamic scene is used to demonstrate the proposed method. A car equipped with GNSS/INS will go through a city canyon where GNSS navigation signals are blocked. They apply the method to infer a belief for the likelihood of threats and risks for GPS signals.
Kaja et al. [37]	The method is benchmarked against EVITA and HEAVENS for validation purposes.

FIGURE 6: DFD of the information interaction between OBU and RSU.

of the countermeasures in the specific threat scenario. The results of the simulation can be displayed in the form of a report. The content of the report includes the basic

parameters of the threat model, the analysis of the effectiveness of countermeasures, and the security level of the system.

FIGURE 7: In-vehicle cyber threat model diagram of 2015 Cadillac Escalade [38].

FIGURE 8: Network model of automotive ethernet architecture.

SeaMonster is a security modeling tool for threat models. It supports the use of common graphic symbols to build attack tree models and misoperation models. The newly created models can be connected to the database to be shared and reused. OWASP Threat Dragon is also a tool, which uses graphic symbols to create a threat model diagram. Figure 10 shows a simple model of FOTA made by OWASP Threat Dragon. It supports STRIDE, LINDDUN, and CIA (confidentiality, integrity, and availability). According to the provided threat modeling diagram and rule engine, it can automatically generate potential threats in the model and give corresponding mitigations.

The comparison of the performance of TARA tools above is summarized in Table 5. By comparing the performance of different TARA tools, we can understand the characteristics of existing tools so that users can quickly find suitable threat analysis tools.

5. Attack-Defense Mapping

Attack-defense mapping is a method to map threats to mitigations. Analysis of mitigation commonly used is mainly based on expert experience. It makes the process of finding mitigation inflexible and difficult to expand. Even

FIGURE 9: The threat builder of replay attack in CAN bus.

FIGURE 10: Threat modeling of FOTA with OWASP Threat Dragon.

though the best mitigation measures for the same threat may be different under different application scenarios, completely copying expert experience will reduce the defense effect. Compared to relying entirely on expert experience, the process of attack-defense mapping should

contain some theoretical bases, such as quantitative analysis and model-based method. It shows how to methodically select an effective and efficient countermeasure against the attack after finding threats. Designing the defense strategy with an attack-defense mapping approach

TABLE 5: Comparison of performance of TARA tools.

Tool	Developer	Function	Quantitative	Difficulty	Output
MTMT	Microsoft	Threat modeling and analysis	×	Easy	Reports of threat analysis
SecuriCAD	—	Generating a possible attack path and the result of risk assessment	✓	Medium	Risk level/quantitative threat analysis results
GROOVE	—	Modeling the network architecture and generating an attack graph	×	Medium	Attack graph
OMNeT++	Simulcraft	Performing network attack simulation and threat analysis	✓	Medium	Results of network attack simulation and threat analysis
PTA	PTA technologies	Threat modeling and calculating risk assessment results	✓	Medium	Security level/parameters of the threat model/effectiveness analysis of countermeasures
SeaMonster	SourceForge	Building attack tree models and misoperation model	×	Easy	Threat models
Threat Dragon	OWASP	Generating potential threats and corresponding mitigations	×	Easy	List of a potential threat and corresponding mitigations

can also help researchers to design mitigations for their systems. This section presents a review of attack-defense mapping. The methods are mainly the following five: attack-defense tree, game-theoretic approach, feedback-based method, designed-rule-based method, and benefit-cost assessment, which are listed in Table 6.

5.1. Attack-Defense Tree Approach. Attack-defense tree model is a systematic and intuitive approach used to analyze the ability of networks to handle various types of attacks. It combines the attacks with the defending strategies. An attack tree is an analysis-based technique that uses a tree-based structure to simulate multistage attacks. The defending nodes express countermeasures that can mitigate the potential harm caused by the attacks. The validity and the objectivity of defending nodes should be verified. The structure of the attack-defense tree model is illustrated in Figure 11.

In 2016, Bahamou et al. [40] added countermeasures to the attack trees and obtained the attack-defense tree model. They built an attack-defense tree for vehicular network privacy, where they combined attacks with defense mechanisms. They introduced countermeasures to mitigate the risk for each subgoal or leaf node. For example, reinforcing the network firewall is the mitigation against the application layer attack according to their attack-defense tree. In 2020, Cui and Zhang [17] proposed an efficient security risk analysis method, Vehicles Risk Analysis (VeRA). They assessed the risk value by considering the attack probability, severity, and human control and used the attack-defense tree to describe the risk analysis process. The attack nodes are formed like “attack goal -> attack method -> detailed attack -> attack entry point,” and the defending nodes can show the mitigation to relieve the related attack.

5.2. Game-Theoretic Approach. The game-theoretic approach combines attack-defense tree with game theory. Game theory is a study of the mathematical model of strategic interaction among rational decision-makers. The game-theoretic approach can provide in-depth knowledge of the strategies adopted by attackers and defenders. According

to the attack-defense tree, the attacker has several attack methods to achieve the attack goal, and each attack method may correspond to several countermeasures. The meaning of the game theory is to help defenders choose the best mitigation and maximize their payoff. First, an attack-defense tree should be established, so all the potential attacks and mitigations can be listed. Then by applying game theory on the tree, the defender can reach optimal mitigation, which is tightly related to the attack strategies. However, the game-theoretic approach is founded on the fact that the players act rationally, which sometimes is not possible in reality. Besides, the utility function needs to be properly designed.

In different papers, the calculation of Return on Investment (ROI) and Return on Attack (ROA), which are the utility functions, may be different. Table 7 compares the different calculations of ROI and ROA. In 2016, Garg and Aujla [41] combined an attack-defense tree with a game-theoretic approach to analyze SSL SYN attacks in VANETs. They built the attack-defense tree to identify and tackle the attacks. The risk priority number (RPN) of each leaf node is calculated by three parameters, namely, severity, occurrence, and detection, to identify the priority in which risk needs to be addressed. They used RPN, expected gain (EG), expected loss (EL), cost of investment (COI), and additional cost (AC) to calculate ROI and ROA. The defender needs to choose the countermeasure to maximize his/her own payoff. They considered different levels of the parameters to calculate ROI and ROA so that the effectiveness can be maintained. In 2019, Garg et al. [42] evaluated a game-theoretic scheme by using a case study for the distributed denial-of-service attack. An attack-defense tree was designed to depict every move of the defender concerning the attacker’s strategies. The attacker’s move and the defender’s move are shown in Figure 12. They used a game-theoretic scheme to analyze the impact of ROI and ROA on attacker’s and defender’s moves. Calculation of ROI and ROA is shown in Table 7, where EL is the expected loss incurred to attack, RR is the risk reduction with the countermeasure, COI is the cost of investment, EG is the expected gain, C_A is the cost to launch an attack, and C_{AD} is the additional cost to attack the countermeasure. The defense strategy is designed preemptively for each step of the attack. In 2017, Bahamou et al. [43] built an attack-defense

TABLE 6: Attack-defense mapping methods.

Attack-defense mapping methods	Brief description	Characteristics
Attack-defense tree approach	It adds corresponding countermeasures to the attack tree.	It is systematic and intuitive. The validity and objectivity of the defending nodes need to be verified.
Game-theoretic approach	It reflects the strategies adopted by attackers and defenders.	The mitigations are tightly related to the risks. It assumes that the players' actions are rational, which is not always possible.
Feedback-based approach	It iterates and compares the mitigations by reevaluating the risk levels to find the appropriate mitigation.	It is an effective method to design the mitigations, but the process often contains heavy computation and requires semiautomated software.
Designed-rule-based approach	It performs mapping with a designed table.	The mapping process is efficient and easy, but the designed table should be clear and precise.
Benefit-cost assessment approach	It performs mapping from the benefit-cost perspective.	It balances benefit and cost. The estimate of benefit and cost needs to be precise enough.

FIGURE 11: The structure of the attack-defense tree model.

TABLE 7: Calculation of ROI and ROA.

Paper	ROI	ROA
Garg and aujla [41]	$(EL * RPN - COI)/COI$	$(EG * (1 - RPN) - (COI + AC))/(COI + AC)$
Garg et al. [42]	$(EL * RR - COI)/COI$	$(EG * (1 - RR) - (C_A + C_{AD}))/C_A$
Bahamou et al. [43]	$((ALE * RM) - CSI)/CSI$	$(GI * (1 - RM) - (Coast_a + Coast_{ac}))/Coast_{ac}$

tree for location privacy of VANET with the game-theoretic approach. Their goal was to determine the most probable attack scenario and how to deploy the appropriate countermeasures to make the risks acceptable. ROI is calculated by Annual Loss Expectancy (ALE), Risk Mitigated (RM), and Cost of Security Investment (CSI). ROA is calculated by GI (expected gain), Coast_a (cost sustained by the attacker to succeed), Coast_{ac} (cost brought by the countermeasure), and RM. The defender is the leader and the attacker is the follower. The goal of each player is to maximize their return.

5.3. Feedback-Based Approach. This kind of method finds the appropriate mitigation by reevaluating the risk value. By iterating or comparing different mitigations, the most effective mitigation will be found. It is an effective method for the engineers to design the mitigation according to the risk assessment. However, the iterative process has a heavy workload and often requires semiautomated software

support. It also takes much time to build the mitigation testing scenarios.

Longari et al. [45] demonstrated a semiautomated and topology-based risk analysis framework. This framework can assess the security of automotive onboard networks and give some mitigations. It takes the topology as input and evaluates its global risk value. Then, the mitigation is iteratively implemented by changing the network topology. Finally, it finds mitigation that minimizes the global risk value. This kind of method is also effective for connected and autonomous driving scenarios. Le and Maple [44] used a knowledge-based system to identify the critical threats and detected the changes in the security context of the CAV and the surrounding environments. Then, they captured the dynamic risks and adjusted the countermeasures as needed. In Figure 13, dynamic mitigation was applied, which combined the two best mitigations in a jamming attack. Therefore, the CAV could gain the lowest risk in different situations with the dynamic mitigation.

FIGURE 12: Moves of attacker and defender [42].

FIGURE 13: Dynamic mitigation strategies [44].

Suo and Sarma [46] presented a framework for constructing testing scenarios driven by cyber threats. The engineers can select the highest risk threats in the attack tree and build test cases with several scenarios. Each mitigation strategy will be tested against a set of scenarios and iterated. It can help the engineers to find the appropriate mitigation against the risk effectively and quickly in the design process. Besides, the Bayesian defense graph provides a method to calculate the likelihood of threats, which helps to achieve feedback analysis. Behfarnia and Eslami [28] used Bayesian defense graphs to analyze the risk of autonomous vehicles in order to study the effect of countermeasures. They built a defense graph using the

Bayesian network model and parameterized elements of the graph. Then, the probability of risk for a set of countermeasures could be inferred with the graph. Their case study used the model and found that the likelihood of threats for GPS signals could be reduced to 0.001% when several kinds of antispoofing techniques were employed.

5.4. Designed-Rule-Based Approach. This method designs a table that maps the corresponding countermeasures to the results of threat analysis. Although it is an efficient and easy way for mapping, it will lead to subjectivity and bias in the

countermeasures if the designed table lacks clear and precise definitions.

In 2018, Rosenstatter and Olovsson [47] introduced a mapping from automotive security levels to security mechanisms. They classified the threat into six security attributes, and each attribute had a security level ranging from zero to four. Then, they designed a direct mapping, with which the designers can easily obtain the mandatory countermeasures required for specific security levels. It makes the security design much more efficient and easier, but the mechanisms have to be validated with more cases. In 2019, Cui and Sabaliauskaite [11] demonstrated a Unified Safety and Security (US²) analysis method. It evaluates the security risks with a security level (SEL), which uses three parameters, namely, attack potential, threat criticality, and DAL focus. US² provides a table that combines the SEL, the ASIL, and the corresponding countermeasures. It is a useful tool for selecting appropriate safety and security countermeasures for autonomous vehicles depending on the risk level.

5.5. Benefit-Cost Assessment Approach. Benefit-cost assessment is a method that provides mitigation to reduce costs as much as possible while achieving the best defending effect. Since the efforts undertaken for protection may be exceeded by the efforts undertaken to break the protection, the selection of countermeasures is usually based not only on the technical possibility but also on a cost-benefit assessment. Many factors need to be considered in the estimate of cost and benefit. The more precise the estimate, the more effective the mapping that can be obtained.

Rocchetto et al. [48] performed a cost/benefit trade-off analysis to justify the necessary costs implied by the corresponding countermeasures and the adoption of specific security requirements. They proposed two different costs, the cost for the attackers and the cost to mitigate the vulnerability. The estimate of the mitigation cost depends on many factors, such as the value of the asset to be protected. The estimate of attack cost can be defined by the CVSS.

6. Discussion of Future Developments

In this section, the directions of future developments in TARA in the automotive field are discussed. The future research fields include the formal quantitative TARA approaches, the TARA methods with trade-off considerations, and the data-driven TARA process.

6.1. Formal and Quantitative TARA Approaches. At present, domestic and foreign scholars have established a variety of cybersecurity threat analysis frameworks, but the analysis process is highly subjective and lacks quantitative analysis. The formal and quantitative TARA approaches are a research direction that can effectively solve this problem. The formal quantitative threat analysis method uses standardized languages such as SysML to formally describe the system under test and conduct threat modeling at the system level. In addition, through formal modeling, probabilistic analysis

of vehicle system network security can be achieved, thereby achieving more detailed quantitative TARA.

6.2. TARA Methods with Trade-Off Considerations. The increasing interactivity between cyber and vehicle systems and connectivity give rise to new safety and security challenges. Since cybersecurity attacks can affect the functional safety of vehicles, it is unrealistic to strengthen the overall defense level without either side. In addition, too many security defense mechanisms not only will increase the overall vehicle cost, but may even affect the user experience [22]. Therefore, considering the trade-offs of security, safety, vehicle cost, and user experience is an important direction of TARA methods.

6.3. Data-Driven TARA Process. As modern vehicles increasingly exchange data with the cloud, OEMs can collect more real data from users' vehicles. A large amount of data can bring many possibilities for TARA. For example, the TARA process based on machine learning algorithms has very high requirements for data magnitude. Large-scale data can provide a guarantee for the accuracy of threat model training. The data-driven TARA process is a new research direction.

7. Conclusion

In this survey, the methods of TARA in the automotive field have been analyzed and compared. All the methods are classified so that researchers can quickly and deeply understand the field of TARA. The ways to evaluate the TARA methods in the literature are also summarized. We have introduced several commonly used TARA tools, and the performance of these tools is compared. In addition, a concept of attack-defense mapping has been proposed, which focuses on how to match the appropriate mitigation measures after finding threats and vulnerabilities. This concept provides a theoretical basis for TARA and makes the whole process more flexible and convincing. We have classified the attack-defense mapping methods into five categories and then analyzed and compared them. Furthermore, the directions of future developments in TARA for automotive domain are discussed.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was financially supported by prospective study funding of Nanchang Automotive Innovation Institute, Tongji University (No. TPD-TC202010-13).

References

- [1] Y. Wang, Y. Wang, and H. Qin, "A Systematic Risk Assessment Framework of Automotive Cybersecurity," *Automotive Innovation*, vol. 4, pp. 1–9, 2021.
- [2] ISO, *ISO/SAE FDIS 21434-2021, Road Vehicles—Cybersecurity Engineering*, ISO, Geneva, Switzerland.
- [3] S. V. E. S. S. Committee, *SAE J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems*, SAE Standard, Warrendale, PA, USA, Work-in-Progress, 2017.
- [4] O. Henniger, A. Ruddle, S. Herve, W. Benjemin, and M. Wolf, "Securing vehicular on-board it systems: the evita project," in *Proceedings of the VDI/VW Automotive Security Conference*, Ingolstadt, Germany, October 2009.
- [5] G. Macher, "A review of threat analysis and risk assessment methods in the automotive context," in *Proceedings of the International Conference on Computer Safety, Reliability, and Security*, September 2016.
- [6] A. Skavhaug, G. Jeremie, S. Erwin, and F. Bitsch, *Computer Safety, Reliability, and Security*, Springer, Berlin, Germany, 2016.
- [7] D. Dominic, M. E. Ryan, M. Di, and C. Sumeet, "Risk assessment for cooperative automated driving," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, October 2016.
- [8] J. Dürrwang, K. Beckers, and R. Kriesten, "A lightweight threat analysis approach intertwining safety and security for the automotive domain," in *Proceedings of the International Conference on Computer Safety, Reliability, and Security*, September 2017.
- [9] M. Hagan, F. Siddiqui, and S. Sezer, "Policy-based security modelling and enforcement approach for emerging embedded architectures," in *Proceedings of the 2018 31st IEEE International System-On-Chip Conference (SOCC)*, pp. 84–89, IEEE, Arlington, VA, USA, September 2018.
- [10] F. Haidar, A. Kaiser, B. Lonc, and U. Pascal, "Risk analysis on C-its pseudonymity aspects," in *Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, IEEE, Canary Islands, Spain, June 2019.
- [11] J. Cui and G. Sabaliauskaite, "US2: an unified safety and security analysis method for autonomous vehicles," in *Proceedings of the Future of Information and Communication Conference*, Springer, Singapore, April 2018.
- [12] G. Macher, H. Sporer, R. Berlach, A. Eric, and K. Christian, "SAHARA: a security-aware hazard and risk analysis method," in *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 621–624, Springer, Grenoble, France, March 2015.
- [13] C. Schmittner, Z. Ma, and P. Smith, "FMVEA for safety and security analysis of intelligent and cooperative vehicles," in *Proceedings of the International Conference on Computer Safety, Reliability, and Security*, September 2014.
- [14] C. Schmittner, Z. Ma, S. Erwin, and G. Thomas, "A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, April 2015.
- [15] S. Verma, G. Thomas, P. P. Peter, and S. Christoph, "Combined approach for safety and security," in *Proceedings of the International Conference on Computer Safety, Reliability, and Security*, September 2019.
- [16] Y. Lee, S. Woo, Y. Song, J. Lee, and D. H. Lee, "Practical vulnerability-information-sharing architecture for automotive security-risk analysis," *IEEE Access*, vol. 8, Article ID 120009, 2020.
- [17] J. Cui and B. Zhang, "VeRA: a simplified security risk analysis method for autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, Article ID 10494, 2020.
- [18] J. Monteuis, B. Ayman, Z. Jun, H. Laïod, S. Alain, and U. Pascal, "SARA: security automotive risk analysis method," in *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, ACM, Incheon, Republic of Korea, June 2018.
- [19] M. Zoppelt and R. T. Kolagari, "SAM: a security abstraction model for automotive software systems," in *Proceedings of the Security and Safety Interplay of Intelligent Software Systems*, pp. 59–74, Springer, Barcelona, Spain, September 2018.
- [20] S. Kim and R. Shrestha, "AUTOSAR embedded security in vehicles," in *Automotive Cyber Security*, Springer, Berlin, Germany, 2020.
- [21] T. Halabi, O. A. Wahab, R. A. Mallah, and M. Zulkernine, "Protecting the Internet of vehicles against advanced persistent threats: a bayesian Stackelberg game," *IEEE Transactions on Reliability*, IEEE, vol. 70, no. 3, pp. 1–16, 2021.
- [22] J. Yu and F. Luo, "A systematic approach for cybersecurity design of in-vehicle network systems with trade-off considerations," *Security and Communication Networks*, vol. 2020, Article ID 7169720, 14 pages, 2020.
- [23] S. Kim and R. Shrestha, "Internet of vehicles, vehicular social networks, and cybersecurity," in *Automotive Cyber Security*, Springer, Berlin, Germany, 2020.
- [24] J. Zhong, S. Du, Z. Lu, H. Xhu, C. Fan, and Q. Xue, "Security modeling and analysis on intra vehicular network," in *Proceedings of the 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, Toronto, ON, Canada, September 2017.
- [25] R. C. Rinaldo and D. Hutter, "Integrated analysis of safety and security hazards in automotive systems," in *Proceedings of the ESORICS 2020 International Workshops, CyberICPS, SECPRE, and ADIoT*, pp. 3–18, Springer, Guildford, U.K., September 2020.
- [26] P. Mundhenk, S. Sebastian, L. Martin, A. S. Fahmy, and C. Samarjit, "Security analysis of automotive architectures using probabilistic model checking," in *Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, IEEE, San Francisco, CA, USA, June 2015.
- [27] D. Li, T. Liu, T. Cao, and P. Deng, "The risk assessment for unmanned vehicle using bayesian network," in *Proceedings of the International Conference on Geo-Informatics in Resource Management and Sustainable Ecosystem*, Springer, Wuhan, China, October 2016.
- [28] A. Behfarnia and A. Eslami, "Risk assessment of autonomous vehicles using bayesian defense graphs," in *Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, IEEE, Chicago, IL, USA, August 2018.
- [29] K. Karray, J. L. Danger, S. Guilley, and M. E. Abdelaziz, "Attack Tree Construction And Its Application To The Connected Vehicle," in *Cyber-Physical Systems Security*, pp. 175–190, Springer, Berlin, Germany, 2018.
- [30] S. Ouchani and A. Khaled, "Security assessment and hardening of autonomous vehicles," *International Conference on Risks and Security of Internet and Systems*, Springer, Berlin, Germany, 2020.
- [31] Y. Roudier and L. Apvrille, "SysML-Sec: a model driven approach for designing safe and secure systems," in *Proceedings of the 2015 3rd International Conference on Model-Driven Engineering and Software Development*

- (MODELSWARD), pp. 655–664, Springer, Loire Valley, France, February 2015.
- [32] C. Schmittner, Z. Ma, and P. Puschner, “Limitation and improvement of STPA-Sec for safety and security co-analysis,” in *Proceedings of the International Conference on Computer Safety, Reliability, and Security*, September 2016.
 - [33] I. Friedberg, K. McLaughlin, P. Smith, D. Lavery, and S. Sezer, “STPA-SafeSec: safety and security analysis for cyber-physical systems,” *Journal of information security and applications*, vol. 34, pp. 183–196, 2017.
 - [34] D. Ren, S. Du, and H. Zhu, “A novel attack tree based risk assessment approach for location privacy preservation in the VANETs,” in *Proceedings of the 2011 IEEE International Conference on Communications (ICC)*, pp. 1–5, IEEE, Kyoto, Japan, June 2011.
 - [35] M. Salfer, H. Schweppe, and C. Eckert, “Efficient attack forest construction for automotive on-board networks,” in *Proceedings of the International Conference on Information Security*, October 2014.
 - [36] M. Krisper et al., “RISKEE: a risk-tree based method for assessing risk in cyber security,” in *Proceedings of the European Conference on Software Process Improvement*, September 2019.
 - [37] N. Kaja, A. Shaout, and D. Ma, “Fuzzy based threat assessment model (FTAM),” in *Proceedings of the 2019 International Arab Conference on Information Technology (ACIT)*, pp. 144–149, Springer, Al Ain, December 2019.
 - [38] W. Xiong, F. Krantz, and R. Lagerström, “Threat modeling and attack simulations of connected vehicles: proof of concept,” in *Proceedings of the International Conference on Information Systems Security and Privacy*, Springer, Prague, Czech Republic, February 2019.
 - [39] J. Santhosh and S. Sankaran, “Defending against Sybil attacks in vehicular platoons,” in *Proceedings of the 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–6, IEEE, Goa, India, December 2019.
 - [40] S. Bahamou, J. Bonnin, and M. I. E. Ouadghiri, “Vehicular ad-hoc network’s privacy assessment based on attack tree,” in *Proceedings of the International Workshop on Communication Technologies for Vehicles*, San Sebastián, Spain, June 2016.
 - [41] S. Garg and G. Aujla, “Assessing risk priority of SSL SYN attack using game theoretic attack defense tree model for VANETs,” in *Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 729–734, Springer, New Delhi, India, March 2016.
 - [42] S. Garg, G. S. Aujla, N. Kumar, and S. Batra, “Tree-based attack-defense model for risk assessment in multi-UAV networks,” *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 35–41, 2019.
 - [43] S. Bahamou, D. E. Ouadghiri, and J. Bonnin, “When game theories meets security and privacy related risk assessment of vehicular networks (VANET),” *Journal Mobile Multimedia*, vol. 12, pp. 213–224, 2017.
 - [44] A. Le and C. Maple, “A simplified approach for dynamic security risk management in connected and autonomous vehicles,” in *Proceedings of the Living in the Internet of Things (IoT 2019)*, May 2019.
 - [45] S. Longari, C. Andrea, M. Carminati, and Z. Stefano, “A secure-by-design framework for automotive on-board network risk analysis,” in *Proceedings of the 2019 IEEE Vehicular Networking Conference (VNC)*, pp. 1–8, Springer, Los Angeles, CA, USA, December 2019.
 - [46] D. Suo and S. Sarma, “A test-driven approach for security designs of automated vehicles,” in *Proceedings of the 2019 IEEE Intelligent Vehicles Symposium (IV)*, pp. 26–32, Springer, Paris, France, June 2019.
 - [47] T. Rosenstatter and T. Olovsson, “Towards a standardized mapping from automotive security levels to security mechanisms,” in *Proceedings of the 2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pp. 1501–1507, Springer, Maui, HI, USA, November 2018.
 - [48] M. Rocchetto, A. Ferrari, and V. Senni, “Challenges and opportunities for model-based security risk assessment of cyber-physical systems,” in *Resilience of Cyber-Physical Systems*, pp. 25–47, Springer, Berlin, Germany, 2019.