ONLINE ISSN: 3007-3197 | PRINT ISSN: 3007-3189

http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 5 (2025)

Empirical Investigation of Cybersecurity Challenges in Autonomous Vehicular Communication

Naeem Ullah[1#], Siffat Ullah Khan[1], Ghulam Murtaza Khan[2]

Article Details

Keywords: Empirical Study, Cybersecurity, V2V communication

[1^]**Naeem Ullah**
Ph.D Scholar
Software-Engineering-Research-Group (SERG-UOM), Department of Computer Science and IT, University of Malakand, Pakistan.
Naeemullah72@gmail.com

[1]**Siffat Ullah Khan**
Software-Engineering-Research-Group (SERG-UOM), Department of Computer Science and IT, University of Malakand, Pakistan
Siffatullah@uom.edu.pk

[2]**Ghulam Murtaza Khan**
Department of Computer Science, Shaheed Benazir Bhutto University Sheringal, Dir Upper, KP, Pakistan
gmkhan@sbbu.edu.pk

ABSTRACT

Cars without drivers are gaining reputation due to the growth in wireless communication technology. Driverless vehicular communication is a Vehicle-to-Vehicle (V2V) technology that is evolving rapidly, addressing modern transportation needs and driving both economic and technological progress. V2V offers numerous benefits by enabling vehicles to communicate with each other and with infrastructure such as Roadside Units (RSUs). This communication helps minimize collisions, reduce fatalities, and enhance road safety for passengers. This paper aims to identify and analyze significant cybersecurity challenges that automotive organizations need to address to develop secure V2V communication for autonomous vehicles. We conducted an online survey with 51 experts from various countries. Participants were asked to rank each challenge on a five-point scale to determine its perceived significance. We identified cybersecurity challenges such as location falsification, bogus warning messages, malware attacks, and repudiation attacks as critical, according to expert feedback. Our results show that Authorization and authentication challenges, bogus warning messages, eavesdropping attacks, location falsification, malware attacks, and spoofing attacks are commonly recognized across three expert levels (i.e., junior, intermediate, and senior). Additionally, location falsification and bogus warning messages were reported as common challenges across all types of organizations (i.e., small, medium, and large). Therefore, location falsification and bogus warning messages should be prioritized by automotive organizations to ensure the development of secure V2V communication systems.

1 Introduction

The objective of Vehicle-to-Vehicle (V2V) communication is to share critical information with drivers and provide real-time warnings about potential incidents. Using Dedicated Short-Range Communication (DSRC) technology [1], vehicles can interact with one another and broadcast data electronically. This includes parameters such as vehicle speed, GPS location, route, track history, vehicle control information, steering wheel angle, brake status, and transmission state. According to the National Highway Traffic Safety Administration (NHTSA), V2V communication messages

are classified as Basic Safety Messages (BSMs). These messages facilitate the transmission of dynamic information between vehicles, such as speed, location, and heading [2]. There are several motivations for the development of V2V communication. In the context of the Internet of Vehicles (IoV), vehicles exchange critical messages to support various applications, including traffic rerouting, crash avoidance, traffic data analysis, content caching, and entertainment services [3]. Moreover, V2V communication provides multiple benefits, such as improved traffic management, driver assistance applications, enhanced road safety, and optimized routing. Road traffic collisions claim approximately 1.35 million lives globally each year [4]. However, despite its advantages, V2V communication faces several issues and threats [4-6]. Numerous challenges have been identified in the V2V communication process. One key challenge is impersonation or spoofing, where an attacker attempts to pose as another node to intercept messages or gain unauthorized access, as well as threats from real-time adversaries [7]. Other notable challenges include denial-of-service attacks, bogus warning messages, location falsification, and unreliable communication channels [8-11]. Despite the importance of V2V communication, limited empirical research has been conducted on its development practices in general, and on the identification of cybersecurity challenges that significantly impact stakeholders in automotive organizations in particular. To address this gap, initially, we conducted Multivocal Literature Review (MLR) to review the literature with the intent to identify the cybersecurity challenges and practices in V2V communication. The results of the MLR have been published [12, 13]. To validate the findings of the MLR and to find any new challenges and practices, if any, we conducted a questionnaire survey in the industry to explore the following research questions:

RQ1. What challenges do automotive organizations need to address in order to have a positive impact on secure V2V communication?

RQ2. Do the identified challenges vary among the various experts based on their experience levels?

RQ3. How are these challenges relevant to the organizations size?

RQ4. Do the identified challenges vary among the different experts from continent to continent?

In this paper, we critically analyze each identified challenge and provide a detailed description of the research methodology used. Additionally, we employ various analyses to compare the identified challenges across automotive industry experts, considering their experience levels, organizational sizes, and geographic locations. The long-term aim of this research is to offer V2V communication development companies a comprehensive body of knowledge that can guide them in designing and adapting effective vehicular communication initiatives.

The organization of this paper is as below:

Section 2 provides background information.

Section 3 describes the research methodology.

Section 4 includes the results and discussion of this study.

Section 5 provides the summary of findings.
Section 6 outlines the study's limitations.
Section 7 presents the conclusion and directions for future work.

2 Background

The implementation of Vehicle-to-Vehicle (V2V) communication technology has brought significant advantages and new opportunities to the automotive sector [14-16]. Vehicles equipped with V2V capabilities can exchange real-time data regarding traffic, weather, and other environmental conditions. V2V communication supports optimal routing and congestion reduction [17] while also enhancing road safety through its various applications [18, 19]. Several researchers have evaluated the benefits of V2V communication in enabling smart traffic systems. A survey study [20] found that V2V communication improves traffic flow efficiency by enabling vehicles to coordinate their movements and identify optimal routes. V2V communication occurs between On-Board Units (OBUs) and may also involve Roadside Units (RSUs) as intermediaries [21]. Despite these merits, several challenges must be addressed before the widespread adoption of V2V communication systems. While the technology holds great promise for enhancing road safety and traffic flow in intelligent transportation systems [22], further research is needed to overcome existing challenges and to develop more advanced, cost-effective V2V solutions. This research paper presents insights from experts in automotive organizations and evaluates the current state of V2V communication in smart traffic systems. It highlights potential benefits, such as improved safety and efficiency, and analyzes challenges based on organizational size and the experience levels of various experts. The findings can inform future research and guide the development and implementation of V2V communication in smart traffic systems.

3 Research Methodology

This section discusses the data collection and analysis process.

3.1 Data Collection

Based on the nature of this research, we ultimately decided to conduct an industrial survey (online survey) to collect data from V2V communication practitioners in automotive organizations regarding their opinions and experiences in employing various techniques for secure V2V communication development. The questionnaire survey consisted of two main phases: design and sampling. During the design phase, the survey questions were formulated. Sampling can be conducted using either systematic or non-methodical approaches, with data collected directly from the target population [23, 24]. However, in this study, it was not feasible to obtain data directly from experts across different countries. Therefore, a non-methodical approach was adopted, utilizing an online poll for data collection. This method has also been used by other researchers [25, 26]. The questionnaire primarily consisted of closed-ended questions designed to gather specific insights from experts. Additionally, a few open-ended questions were included to identify any cybersecurity challenges and practices related to V2V communication that may not have been captured in the Multivocal Literature Review (MLR). A five-point Likert scale was used to assess participants' opinions on the cybersecurity challenges and practices listed in the closed-ended section, with response options ranging from "Strongly Agree" to "Strongly Disagree."

Table 1. Summary of LinkedIn automotive organizations related groups

Group Name	Members
Automotive Security Research Group (ASRG)	5,800
Mexico Automotive Industry	32,300
Arilou Automotive Cybersecurity	3,400
(AIAG) Automotive Industry Action Group	21,700
Automotive Cybersecurity Network (ACSN)	1,304
Automotive Industry	5,424
Italy Automotive Industry	1,422
ISO/SAE 21434 Automotive Cybersecurity	547
Sewell Automotive Companies	9,205
Cyber Security for Automotive	1,440

Initially, to validate the questionnaire, we conducted a pilot study with four V2V communication experts. The feedback retrieved from these experts helped us finalize the questionnaire. The finalized version was divided into three sections: Section 1 collected basic information about the experts; Section 2 was designed to gather demographic data; and Section 3 focused on eliciting expert perspectives on eighteen cybersecurity challenges in V2V communication. The first page of the survey provided essential information about the research project. It also included a statement outlining the researcher's ethical responsibilities, assuring participants that their data would be kept confidential. This statement emphasized that only the research team would have access to the data, and no participant or organizational identity would be disclosed to any third party. As previously mentioned, our target population was large and geographically dispersed. To gather responses from experts in automotive organizations involved in V2V communication projects, we employed non-traditional methods. We used two primary approaches to invite experts to participate in our online survey. First, we contacted 17 V2V communication experts via personal networks, of whom 9 agreed to participate. Second, we joined relevant LinkedIn groups related to automotive organizations (as shown in Table 1). By reviewing the profiles available in these groups, we identified 76 experts relevant to our research and obtained their publicly available email addresses. Out of these, 44 experts participated in the online survey. Each received response was reviewed. Among the 53 total responses (9 from personal contacts and 44 via LinkedIn), we excluded 2 responses due to a lack of relevant expertise. Consequently, we retained 51 complete and valid responses for analysis. The final response rate was approximately 54%.

3.2 Data Analysis Method

The first step of organizing qualitative or quantitative data involves grouping of values or scores into frequencies [27], since frequency analysis is one of the best methods of analyzing descriptive data. Frequency tables help us to show the number of occurrences and percentages for each data variable. This method can be used to compare sets of variables and can be used on ordinal, nominal, and numeric data. Frequency analysis formed part of this research in interpreting data quite often. In order to analyze each cyber security challenge, the number of times each of the challenge was

included in the questionnaires was recorded. From comparing the rate at which one problem exists relative to others, we could arrive at the conclusion as to which of them is most important.

4 Analysis and results

This section discusses the results related to the research questions.

4.1 Cybersecurity challenges identified through empirical study

To answer RQ1, Table 2 presents the list of cybersecurity challenges identified through the empirical study. The results show that among the 18 cybersecurity challenges, two received occurrence rates greater than 90%, while one challenge "Malware attack" scored exactly 90%. Fourteen of the remaining challenges received positive score percentages above 80%, while only one challenge (CC17: Sybil and man-in-the-middle attacks) had a score below 80%. These findings indicate strong consensus among practitioners that the majority of these challenges represent significant barriers to secure V2V communication. Therefore, addressing and mitigating these challenges is essential for developing secure V2V communication systems.

Table 2. Summary of identified cybersecurity challenges via empirical study

Challenges ID	Cybersecurity Challenges	Experts perceptions (n=51)							
		Optimistic			Pessimistic			Impartial	
		Strongly Agree	Agree	% of positive	Strongly Disagree	Disagree	% of negative	Not sure	% of Not sure
CC-1	Authorization and authentication challenges	22	23	88	2	3	10	1	2
CC-2	Grey hole, Black hole, and Worm hole attacks (GBW)	18	25	84	3	4	14	1	2
CC-3	Bogus warning messages	22	25	92	1	0	2	3	6
CC-4	Botnet and brute force attacks	19	25	86	0	0	0	7	14
CC-5	Denial of service attacks	22	21	84	2	3	10	3	6
CC-6	Eavesdropping attacks	19	26	88	3	3	12	2	4
CC-7	Fuzzy injection attacks	24	17	80	4	3	14	3	6
CC-8	Information and hardware tampering	23	19	82	2	3	10	4	8
CC-9	Location falsification	22	26	94	1	1	4	1	10
CC-10	Malware attacks	18	28	90	1	0	2	4	12
CC-11	Real-time adversaries	22	20	82	2	4	12	3	6
CC-12	Repudiation attacks	20	23	88	1	3	8	4	8
CC-13	Session hijacking	19	23	82	1	2	6	6	12
CC-14	Social engineering attacks	21	20	80	7	0	14	3	6
CC-15	Spamming and replay attacks	25	16	80	2	3	10	5	10
CC-16	Spoofing attacks	18	26	86	2	3	10	2	4
CC-17	Man in the middle and Sybil attacks	19	21	78	2	4	12	5	10
CC-18	Unreliable	28	14	82	3	1	8	5	10

communication channel

Amongst 18 cybersecurity challenges, 8 challenges have a frequency of 85% or above, while 9 cybersecurity challenges have a frequency of 80% or above and less than 85%. We identified only a single cybersecurity challenge that has a frequency less than 80%.

4.2 Cybersecurity challenges in the perceptions of various groups of experts

To answer RQ2, the participants in the questionnaire survey had varying levels of experience in secure V2V communication projects, ranging from 2 to 17 years. Based on consultations with V2V communication experts, we categorized the participants into three levels: junior-level experts (≤6 years of experience), intermediate-level experts (6–10 years), and senior-level experts (>10 years). A summary of expert perceptions is presented in Table 4.2, with a detailed analysis provided in Appendix 1. Among junior-level experts, CC8: Information and hardware tampering was ranked 1st (95%), while CC3: Bogus warning messages, CC4: Botnet and brute force attacks, CC9: Location falsification, CC10: Malware attacks, and CC16: Spoofing attacks were ranked 2nd (90%). Additionally, CC1: Authorization and authentication challenges, CC5: Denial of service attacks, CC12: Repudiation attacks, and CC18: Unreliable communication channel were ranked 3rd (86%).

For intermediate-level experts, CC3: Bogus warning messages, CC9: Location falsification, and CC10: Malware attacks were ranked 1st (94%), followed by CC1: Authorization and authentication challenges, CC5: Denial of service attacks, CC6: Eavesdropping attacks, CC12: Repudiation attacks, and CC18: Unreliable communication channel in 2nd place (89%). CC11: Real-time adversaries was ranked 3rd (88%).

Among senior-level experts, CC11: Real-time adversaries was ranked 1st (100%), CC17: Sybil and man-in-the-middle attacks was ranked 2nd (94%), and CC3: Bogus warning messages was ranked 3rd (93%).

By analyzing Table 4.3, we identified eight cybersecurity challenges where all three groups showed a consensus with a positive agreement rate exceeding 80%: CC1: Authorization and authentication challenges, CC2: Black hole, grey hole, and wormhole (BGW) attacks, CC3: Bogus warning messages, CC4: Botnet and brute force attacks, CC6: Eavesdropping attacks, CC9: Location falsification, CC10: Malware attacks, and CC16: Spoofing attacks. No statistically significant differences were observed in the perception of these challenges across experience levels, indicating a strong consensus among experts regarding the importance of addressing these issues for secure V2V communication.

To identify any significant differences, we applied the linear-by-linear association (chi-square test) across junior, intermediate, and senior-level experts. However, no significant differences were found for any of the challenges, as detailed in Appendix 1. This suggests that experts at all experience levels are well aware of the importance of considering these cybersecurity challenges.

Table 3. Summary of cybersecurity challenges across the experts from small, medium and large organizations.

Cybersecurity Challenges	Experts Perceptions		
	Junior-level experts (N=21) % of positive	Intermediate-level experts (N=18) % of positive	Senior-level experts (N=12) % of positive
Authorization and authentication challenges	86	89	92
Grey hole, Black hole, and Worm hole attacks (GBW)	81	83	92
Fake warning alerts	90	94	93
Botnet and brute force attacks	90	83	83
Denial of service attacks	86	89	75
Eavesdropping attacks	81	89	83
Fuzzy injection attacks	71	83	92
Information and hardware tampering	95	78	67
Location falsification	90	94	92
Malware attacks	90	94	83
Real-time adversaries	67	88	100
Repudiation attacks	86	89	75
Session hijacking	81	78	92
Social engineering attacks	76	78	92
Spamming and replay attacks	71	78	92
Spoofing attacks	90	83	83
Man in the middle and Sybil attacks	71	78	94
Unreliable communication channel	86	89	67

In Figure 1, the identified cybersecurity challenges are presented along the X-axis, while the frequencies of expert responses are shown on the Y-axis. These frequencies are calculated by aggregating the responses from the "Strongly Agree" and "Agree" categories.

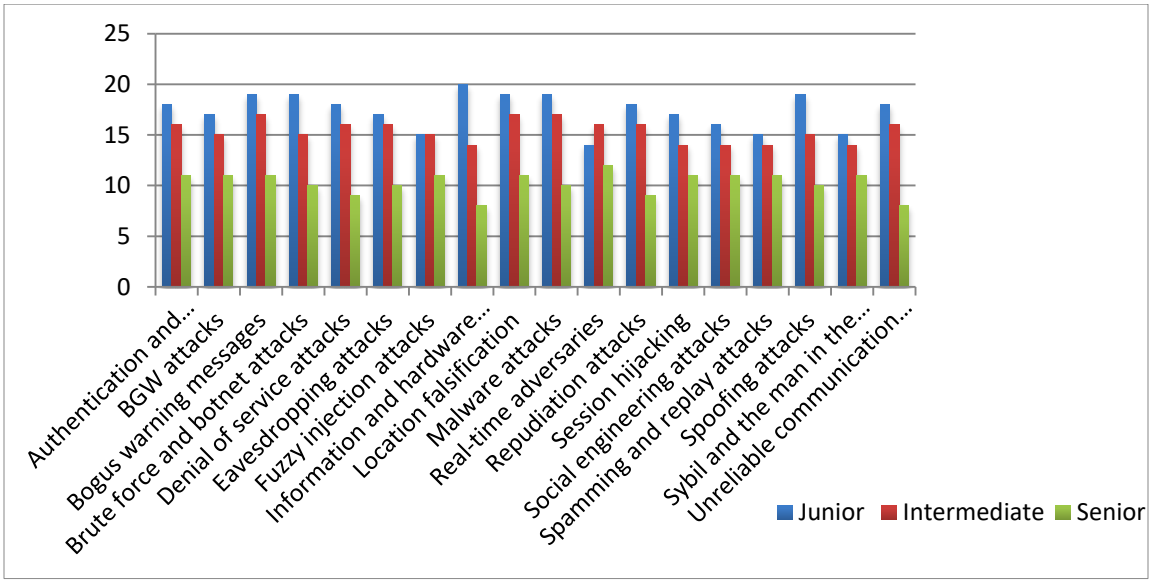

Figure 1. Respondents experience based analysis of the identified challenges

4.3 Cybersecurity challenges based on organization's size

To answer RQ3, the V2V communication experts who participated in this survey represented organizations of various sizes. Some experts worked in small companies with only a few employees, while others belonged to large organizations with over a hundred employees. To classify the organizations by size, we adopted the definition from the Australian Bureau of Statistics [28], which has also been utilized by other researchers [27]. According to this classification, organizations were grouped into three categories: small (1–19 employees), medium (20–100 employees), and large (100+ employees), as shown in Table 4.3, with detailed analysis provided in Appendix 2. Of the 51 respondents, 18 were from small organizations, 20 from medium-sized organizations, and 13 from large organizations. Experts provided their feedback based on their job roles and work environments; however, it is important to note that the size of their employer's organization may or may not have influenced their responses. According to Table 4.3, experts from small organizations identified CC9: Location falsification as the top-ranked challenge (100% positive response—Strongly Agree + Agree), followed by CC8: Information and hardware tampering (95%), and a shared third rank for CC3: Bogus warning messages and CC14: Social engineering attacks.Among experts from medium-sized organizations, CC3: Bogus warning messages ranked 1st (96%), followed by CC1: Authorization and authentication challenges and CC9: Location falsification in 2nd place (95%), and CC11: Real-time adversaries in 3rd (94%). For respondents from large organizations, the highest-ranked challenges (each with 100% positive responses) were CC4: Botnet and brute force attacks, CC5: Denial of service attacks, CC10: Malware attacks, and CC14: Social engineering attacks. These were followed by **CC16:** Spoofing attacks in 2nd place (93%) and CC1: Authorization and authentication challenges and CC6: Eavesdropping attacks in 3rd (92%).

Upon reviewing Table 4.3, we identified seven cybersecurity challenges that received more than 80% positive agreement across all organization sizes: CC2: Black hole, grey hole, and wormhole (BGW) attacks, CC3: Bogus warning messages, CC4: Botnet and brute force attacks, CC9: Location falsification, CC10: Malware attacks, CC12: Repudiation attacks, and CC16: Spoofing attacks.

A chi-square test (linear-by-linear association) was employed to identify statistically significant differences in expert responses across organization sizes. Interestingly, only one challenge, CC10:

Malware attacks, showed a significant difference. Experts from large organizations had the highest frequency of "Strongly Agree" responses for this challenge, while those from small organizations had the lowest. This could be attributed to the fact that large organizations are generally more mature and have greater experience in vehicular communication projects, whereas small organizations are relatively newer and may lack extensive exposure to V2V development.

Table 4.3 Summary of cybersecurity challenges across the experts based on organization's size

Cybersecurity Challenges	Organization's size		
	Small (N=18) % of positive	Medium (N=20) % of positive	Large (N=13) % of positive
Authorization and authentication challenges	78	95	92
Grey hole, Black hole, and Worm hole attacks (GBW)	89	80	85
Bogus warning messages	94	96	85
Botnet and brute force attacks	83	80	100
Denial of service attacks	83	75	100
Eavesdropping attacks	78	85	92
Fuzzy injection attacks	83	75	85
Information and hardware tampering	94	75	77
Location falsification	100	95	85
Malware attacks	83	90	100
Real-time adversaries	78	94	69
Repudiation attacks	89	80	85
Session hijacking	89	80	77
Social engineering attacks	94	55	100
Spamming and replay attacks	78	80	85
Spoofing attacks	83	85	93
Man in the middle and Sybil attacks	67	85	85
Unreliable communication channel	89	80	77

In Figure 2, the X-axis represents the 18 identified cybersecurity challenges, while the Y-axis displays the positive response frequencies from experts in small, medium, and large-sized organizations. Positive frequency refers to the combined count of responses marked as "Strongly Agree" and "Agree," as collected through the empirical study.

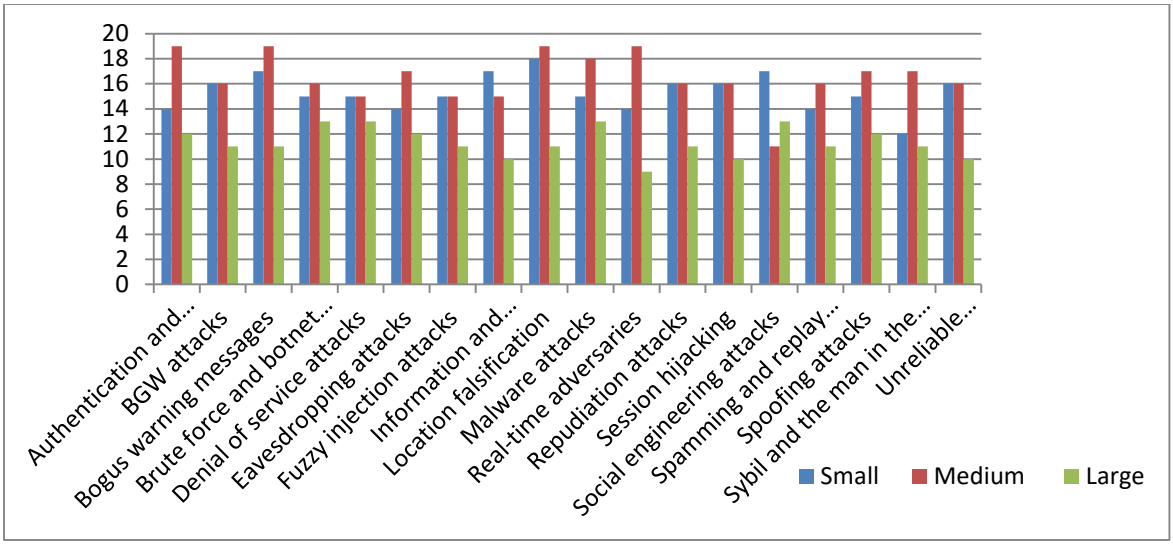

Figure 2. Organizations size based analysis of the identified challenges

4.4 Continents based analysis of the identified cybersecurity challenges

To answer RQ4, we manually reviewed the responses of the 51 selected participants and identified that the respondents were from various continents, including Asia, Europe, Australia, and America. Our analysis revealed that the majority of respondents were from two continents, while the remaining participants were distributed across regions such as America, Canada, and Australia. Specifically, out of 51 respondents, 26 participants were from Asia, 11 from Europe, and the remaining 14 from other continents.

Table 4.4 presents the regional distribution of experts and their agreement levels with cybersecurity challenges. In Asia, the highest-ranked challenges (96% strongly agree + agree) were CC3: Bogus warning messages, CC7: Fuzzy injection attacks, and CC9: Location falsification, followed by CC1: Authorization and authentication challenges (92%), and CC2: Black hole, grey hole, and wormhole (BGW) attacks, CC10: Malware attacks, and CC11: Real-time adversaries (88%).

For Europe, the top-ranked challenges (strongly agree + agree) were CC4: Botnet and brute force attacks, CC5: Denial of service attacks, CC8: Information and hardware tampering, and CC16: Spoofing attacks. CC10: Malware attacks followed at 92%, while CC1: Authorization and authentication challenges, CC9: Location falsification, CC12: Repudiation attacks, CC13: Session hijacking, and CC17: Sybil and man-in-the-middle attacks ranked third at 91%.

In other continents (America + Australia), CC18: Unreliable communication channel ranked first at 100%, followed by CC5: Denial of service attacks (94%), and CC3: Bogus warning messages, CC9: Location falsification, CC10: Malware attacks, and CC16: Spoofing attacks (93%). By analyzing Table 4.4, we identified five cybersecurity challenges with >80% positive agreement across all continents: CC3: Bogus warning messages, CC6: Eavesdropping attacks, CC9: Location falsification, CC10: Malware attacks, and CC12: Repudiation attacks. The detailed analysis of these challenges is provided in Appendix 3. A linear-by-linear chi-square test was conducted, revealing a significant difference only for CC7: Fuzzy injection attacks, while no statistical difference was found for the other identified challenges.

Table 4.4 Summary of cybersecurity challenges across the experts based on continents

Cybersecurity Challenges	Continents'		
	Asia (N=26) % of positive	Europe (N=11) % of positive	Others (N=14) % of positive
Authorization and authentication challenges	92	91	79
Grey hole, Black hole, and Worm hole attacks (GBW)	88	82	79
Bogus warning messages	96	82	93
Botnet and brute force attacks	85	100	79
Denial of service attacks	73	100	94
Eavesdropping attacks	85	82	86
Fuzzy injection attacks	96	64	64
Information and hardware tampering	73	100	86
Location falsification	96	91	93
Malware attacks	88	92	93
Real-time adversaries	88	73	79
Repudiation attacks	81	91	86
Session hijacking	77	91	86
Social engineering attacks	81	82	79
Spamming and replay attacks	73	90	86
Spoofing attacks	77	100	93
Man in the middle and Sybil attacks	81	91	64
Unreliable communication channel	73	82	100

In Figure 3, the X-axis represents the cybersecurity challenges identified through the empirical study, while the Y-axis represents the positive frequencies of responses from experts across various continents. The positive frequency is calculated by combining the counts of "Agree" and "Strongly Agree" responses.

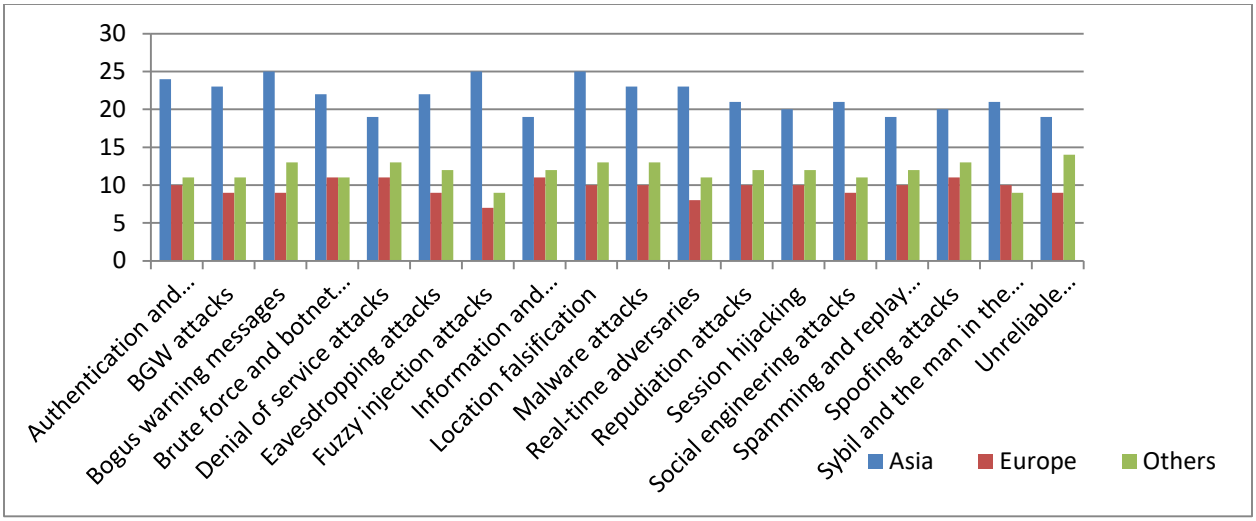

Figure 3 Continents based analysis

5 Summary of Findings

Through empirical study, it has been determined on the challenges of cybersecurity that can influence the autonomous vehicles in shaping V2V communication. Cybersecurity challenges are the areas of priority where the top management should pay attention to design better V2V communication initiatives. In order to determine the importance of a cybersecurity challenge, the following criterion was applied:

- We consider a cybersecurity challenge to be a critical one in case it is agreed or strongly agreed by ≥ 85% of the experts..

Other researchers have also applied their own criteria for determining the criticality of factors [26, 29]. To answer RQ1, applying the above criterion, we identified eight challenges as critical challenges that negatively impact the development of secure V2V communication projects. These critical cybersecurity challenges are:

- CC-1 Authorization and authentication challenges (88%)
- CC-3 Bogus warning messages (92%)
- CC-4 Botnet and brute force attacks (86%)
- CC-6 Eavesdropping attacks (88%)
- CC-9 Location falsification (94%)
- CC-10 Malware attacks (90%)
- CC-12 Repudiation attacks (88%)
- CC-16 Spoofing attacks (86%)

However, other challenges with a frequency percentage ≤ 85% (Strongly Agree + Agree) may also require attention from relevant stakeholders in order to design and develop secure V2V communication projects.

For RQ2, based on the criterion for critical cybersecurity challenges (≥ 85%), we identified:

- Three challenges common across all three expert levels (junior, intermediate, and senior): Authorization and authentication challenges, bogus warning messages, and location falsification.
- Botnet and brute force attacks, denial of service attacks, hardware tampering, malware attacks, repudiation attacks, spoofing attacks, and unreliable communication channel are considered critical challenges by junior-level experts.

- Denial of service attacks, eavesdropping attacks, malware attacks, real-time adversaries, repudiation attacks, and unreliable communication channels are considered critical by intermediate-level experts.
- Black hole, grey hole, and wormhole attacks (BGW), fuzzy injection attacks, real-time adversaries, session hijacking, social engineering attacks, spamming and replay attacks, and Sybil and man-in-the-middle attacks are considered critical by senior-level experts.

It is when the problems identified in the three expert levels are compared, that similarities outweigh differences because no significant difference was observed (see Appendix-1). The findings summary for RQ2 is given in Table 5. Our findings' summary on RQ3 as shown in Table 6 is discussed below. A comparison of the challenges identified regarding the organizational size (small, medium and large) reveals more similarities than differences of the challenges. We only had a significant difference in one challenge: 'Malware attacks' (see Appendix-2). Table 7 contains the summary of our finding for RQ4. We only had a significant difference in one challenge: 'Fuzzy injection attacks' (see Appendix-3).

Table 5 Distribution of challenges across various experts

Experts' Experience level	Total number of challenges cited as agree and strongly agree	No. of critical challenges (cited in >85% of the 'agree' and 'strongly agree' list)
Junior (n=21)	18	The following ten Critical Cybersecurity Challenges (CCCs) are identified. • Information and hardware tampering (95%) • Bogus warning messages (90%) • Botnet and brute force attacks (90%) • Location falsification (90%) • Malware attacks (90%) • Spoofing attacks (90%) • Authorization and authentication challenges (86%) • Denial of service attacks (86%) • Repudiation attacks (86%) • Unreliable communication channel (86%)
Intermediate (n=18)	18	The following nine CCCs are identified. • Bogus warning messages (94%) • Malware attacks (94%) • Location falsification (94%) • Authorization and authentication challenges (89%) • Denial of service attacks (89%) • Eavesdropping attacks (89%) • Repudiation attacks (89%) • Unreliable communication channel (89%) • Real-time adversaries (88%)
Senior (n=12)	18	The following ten challenges are identified as critical • Man in the middle and Sybil attacks (94%) • Bogus warning messages (93%) • Authorization and authentication challenges (92%) • Fuzzy injection attacks (92%) • Location falsification (92%) • Session hijacking (92%) • Social engineering attacks (92%) • Spamming and replay attacks (92%)

Table 6 Distribution of challenges based on organizations size

Experts' Affiliation of organization	Total number of challenges cited as agree and strongly agree	No. of critical challenges (cited in >85% of the 'agree' and 'strongly agree' list)
Small (n=18)	18	The following eight CCCs are identified. • Location falsification (100%) • Bogus warning messages (94%) • Information and hardware tampering (94%) • Social engineering attacks (94%) • Grey hole, Black hole, and Worm hole attacks (GBW) (89%) • Repudiation attacks (89%) • Session hijacking (89%) • Unreliable communication channel (89%)
Medium (n=20)	18	The following five CCCs are identified. • Bogus warning messages (96%) • Authorization and authentication challenges (95%) • Location falsification (95%) • Real-time adversaries (94%) • Malware attacks (90%)
Large (n=13)	18	The following seven challenges are identified as critical • Denial of service attacks (100%) • Botnet and brute force attacks (100%) • Malware attacks (100%) • Social engineering attacks (100%) • Man in the middle and Sybil attacks (93%) • Authorization and authentication challenges (92%) • Eavesdropping attacks (92%)

Table 7 Distribution of challenges based on various continents

Experts' continent affiliation	Total number of challenges cited as agree and strongly agree	No. of critical challenges (cited in >85% of the 'agree' and 'strongly agree' list)
Asia (n=26)	18	The following seven CCCs are identified. • Bogus warning messages (96%) • Fuzzy injection attacks (96%) • Location falsification (96%) • Authorization and authentication challenges (92%) • Grey hole, Black hole, and Worm hole attacks (GBW) (88%) • Malware attacks (88%) • Real-time adversaries (88%)
Europe (n=11)	18	The following eleven CCCs are identified. • Botnet and brute force attacks (100%) • Denial of service attacks (100%) • Information and hardware tampering (100%) • Spoofing attacks (100%) • Bogus warning messages (96%) • Real-time adversaries (94%) • Malware attacks (92%) • Authorization and authentication challenges (91%) • Location falsification (91%) • Repudiation attacks (91%) • Session hijacking (91%) • Sybil and man in the middle attacks (91%) • Spamming and replay attacks (90%)
Others (n=14)	18	The following eleven challenges are identified as critical • Unreliable communication channel (100%) • Denial of service attacks (94%) • Bogus warning messages (93%) • Location falsification (93%) • Malware attacks (93%) • Spoofing attacks (93%) • Eavesdropping attacks (86%) • Information and hardware tampering (86%)

- Repudiation attacks (86%)
- Session hijacking (86%)
- Spamming and replay attacks (86%)

6 Limitations

Construct validity refers to whether the measurement scales reflect the characteristics that they are used to measure. The characteristics employed in this research were obtained from previous works that were published in [13]. Responses of the participants suggest that all the considered attributes were relevant to their work. Internal validity sustains the overall assessment on the findings. According to the findings of the pilot study, the research variables, which we studied, have an appropriate level of internal validity, since they were derived from an extensive review of literature and from piloting the questions. External validity is concerned with the generalization of the findings to the expanse external to the environment studied in the first place [30]. External validity in this study has been taken into consideration because the findings represent the perceptions of 51 experts who are from 10 different countries. But we could not also assume that every participant from such 10 countries would concur with the results. However, we can say that the sample is representative. We employed a questionnaire survey, and the main limitation of this approach is that participants are presented with a list of possible challenges and asked to identify those that have a negative impact on the development of secure V2V communication. This approach might limit the challenges investigated, confining them to those cited in the available literature, with respondents focusing only on the challenges listed. However, we addressed this issue by including open-ended questions in the questionnaire, allowing respondents to list additional challenges, if any. Drawing on the findings of other researchers in several studies [26, 31, 32]. We are sure of our results as we gathered information directly from experts in various roles and who were directly dealing with vehicular communication activities in their organizations. Besides, the experts' experiences were expounded openly without any advice and suggestions from the researchers.

7 Conclusion and future work

Through an empirical study, we investigated the cybersecurity challenges that are commonly considered critical by stakeholders in the development of secure V2V communication. We recommend that concentrating on these challenges can assist automotive organizations and their

relevant stakeholders in improving their readiness towards secure V2V communication development.

Our findings reveal that 'authentication and authorization problems', 'bogus warning messages', and 'location falsification' are relevant to the V2V communication because the majority of the experts in the sample agreed and strongly agreed with these challenges. Apart from these challenges, other challenges are also of great importance for the development of secure V2V communication such as 'malware attacks' 'denial of service attacks' 'repudiation attacks' 'Sybil and man-in-the-middle attacks' 'spoofing attacks' and 'unreliable communication channels'. This paper aims to provide automotive organizations in general and companies involved in V2V communication projects in particular with a body of knowledge that can assist them in designing and developing successful V2V communication initiatives. We recommend that the automotive organizations concentrate on the commonly cited challenges identified in Table 2 (RQ1). Any organization that is interested in understanding the experiences of junior, intermediate, and senior-level experts should focus on the often reported challenges identified in Appendix-1 (RQ2). If any organizations are interested in understanding the experiences of organizations based on their size, then they should concentrate on the most reported challenges identified in Appendix-2 (RQ3). If organizations are interested in checking the most frequently reported challenges based on continents, then they should focus on the challenges identified in Appendix-3 (RQ4). We believe that a good understanding of these critical challenges is important in developing the automotive organizations' readiness for vehicular communication activities. Based on the results of this study, we have identified the following goals for the future:

- To identify why some factors are not considered important in the views of V2V communication experts.
- To perform more analysis of the identified critical challenges based on various variables, such as company scope, expert roles, etc.
- To conduct empirical studies to identify how to implement those challenges that have been most reported in our study.

Our final aim is to develop the Cybersecurity Challenges Mitigation Model (CCMM). This paper contributes to only one component of the CCMM, i.e., the identification of cybersecurity challenges. The ultimate outcome of the study is the development of CCMM to help automotive organizations in assessing and improving their readiness towards V2V communication initiatives. The suggested model will advance the work that has been undertaken in the form of models and frameworks for V2V communication development. Our contribution to improving V2V communication activities will provide other researchers with a firm basis on which to develop various techniques that are based on an understanding of how and where they fit into vehicular communication activities.

8 Acknowledgements

We are grateful to the members of the Software Engineering Research Group (SERG-UOM) at the University of Malakand and our senior colleagues for their assistance in piloting and validating the questionnaire. We also extend our thanks to all the respondents who participated in the survey.

9 References

1. Kenney, J.B., *Dedicated short-range communications (DSRC) standards in the United States.* Proceedings of the IEEE, 2011. **99**(7): p. 1162-1182.
2. Demba, A. and D.P. Möller. *Vehicle-to-vehicle communication technology*. in *2018 IEEE International Conference on Electro/Information Technology (EIT)*. 2018. IEEE.

3. Hildebrand, B., et al., *A comprehensive review on blockchains for Internet of Vehicles: Challenges and directions.* Computer Science Review, 2023. **48**: p. 100547.
4. Schmittner, C. and G. Macher. *Automotive cybersecurity standards-relation and overview*. in *Computer Safety, Reliability, and Security: SAFECOMP 2019 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, Turku, Finland, September 10, 2019, Proceedings 38*. 2019. Springer.
5. Seetharaman, A., et al., *Impact of Factors Influencing Cyber Threats on Autonomous Vehicles.* Applied Artificial Intelligence, 2021. **35**(2): p. 105-132.
6. El Zorkany, M., A. Yasser, and A.I. Galal, *Vehicle To Vehicle "V2V" Communication: Scope, Importance, Challenges, Research Directions and Future.* The Open Transportation Journal, 2020. **14**(1).
7. Salek, M.S., et al., *A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications.* IEEE Internet of Things Journal, 2022. **9**(11): p. 8250-8268.
8. Quyoom, A., A.A. Mir, and A. Sarwar, *Security attacks and challenges of VANETs: a literature survey.* Journal of Multimedia Information System, 2020. **7**(1): p. 45-54.
9. Hamdi, M.M., et al., *A review on various security attacks in vehicular ad hoc networks.* Bulletin of Electrical Engineering and Informatics, 2021. **10**(5): p. 2627-2635.
10. Sharma, S. and B. Kaushik, *A survey on internet of vehicles: Applications, security issues & solutions.* Vehicular Communications, 2019. **20**: p. 100182.
11. Asplund, M., *Combining Detection and Verification for Secure Vehicular Cooperation Groups.* ACM Transactions on Cyber-Physical Systems, 2019. **4**(1): p. 1-31.
12. Ullah, N., S.U. Khan, and S.M.S. Bukhari, *Multivocal Literature Review Protocol for theIdentification of Cybersecurity Challenges anditssolutions in the Context of Vehicle-to-VehicleCommunications from Software EngineeringPerspective.* Spectrum of engineering sciences, 2025. **3**(2): p. 58-89.
13. Ullah, N., et al., *Solutions to cybersecurity challenges in secure vehicle-to-vehicle communications: A Multivocal Literature Review.* Information and Software Technology, 2024: p. 107639.
14. Zhu, M., X. Wang, and J. Hu, *Impact on car following behavior of a forward collision warning system with headway monitoring.* Transportation research part C: emerging technologies, 2020. **111**: p. 226-244.
15. Ameen, H.A., et al., *A review on vehicle to vehicle communication system applications.* Indonesian journal of electrical engineering and computer science, 2020. **18**(1): p. 188-198.
16. Al Musalhi, N. and S.M.S. Otman, *Network Traffic Assignment Model for Vehicle-To-Vehicle Communication.* East Journal of Computer Science, 2025. **1**(1): p. 1-20.
17. Wang, N., et al. *Cooperative autonomous driving for traffic congestion avoidance through vehicle-to-vehicle communications*. in *2017 IEEE Vehicular Networking Conference (VNC)*. 2017. IEEE.
18. Eze, E.C., S. Zhang, and E. Liu. *Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward*. in *2014 20th international conference on automation and computing*. 2014. IEEE.
19. Yousef, M., et al. *Dual-mode forward collision avoidance algorithm based on vehicle-to-vehicle (V2V) communication*. in *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*. 2018. IEEE.

20. Ameen, H.A., et al., *A deep review and analysis of data exchange in vehicle-to-vehicle communications systems: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions.* IEEE Access, 2019. **7**: p. 158349-158378.
21. Li, D., et al., *Notice of retraction: intelligent transportation system in Macao based on deep self-coding learning.* IEEE Transactions on Industrial Informatics, 2018. **14**(7): p. 3253-3260.
22. Bintoro, K.B.Y., et al., *V2V Communication in Smart Traffic Systems: Current status, challenges and future perspectives.* Jurnal PROCESSOR, 2024. **19**(1).
23. Ali, S., et al., *Barriers to software outsourcing partnership formation: an exploratory analysis.* IEEE Access, 2019. **7**: p. 164556-164594.
24. Leavy, P., *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches*. 2022: Guilford Publications.
25. Wagner, S., et al., *Status quo in requirements engineering: A theory and a global family of surveys.* ACM Transactions on Software Engineering and Methodology (TOSEM), 2019. **28**(2): p. 1-48.
26. Niazi, M., D. Wilson, and D. Zowghi, *Critical success factors for software process improvement implementation: an empirical study.* Software Process: Improvement and Practice, 2006. **11**(2): p. 193-211.
27. Khan, S.U., M. Niazi, and R. Ahmad, *Empirical investigation of success factors for offshore software development outsourcing vendors.* IET software, 2012. **6**(1): p. 1-15.
28. Hadler, P., *The effects of open-ended probes on closed survey questions in web surveys.* Sociological Methods & Research, 2023: p. 00491241231176846.
29. Hall, T., A. Rainer, and N. Baddoo, *Implementing software process improvement: an empirical study.* Software Process: Improvement and Practice, 2002. **7**(1): p. 3-15.
30. Regnell, B., P. Runeson, and T. Thelin, *Are the perspectives really different?–further experimentation on scenario-based reading of requirements.* Empirical Software Engineering, 2000. **5**: p. 331-356.
31. Baddoo, N. and T. Hall, *Motivators of Software Process Improvement: an analysis of practitioners' views.* Journal of systems and software, 2002. **62**(2): p. 85-96.
32. Beecham, S., T. Hall, and A. Rainer, *Software process improvement problems in twelve software companies: An empirical analysis.* Empirical software engineering, 2003. **8**: p. 7-42.

Appendix 1. Distribution of cybersecurity challenges upon the Experts experience

Cyber security Challenges	Experts experience level (n=51)															Chi-square Test Linear-by-linear Association $\alpha = 0.05$, df = 1	
	Junior (2-5) years' experience (N=21)					Intermediate (6-10) years' experience (N=18)					Senior (11+) years' experience (N=12)						
	SA	A	D	SD	N	SA	A	D	SD	N	SA	A	D	SD	N	X^2	P
Authorization and authentication challenges	6	12	0	2	1	12	4	2	0	0	4	7	0	1	0	0.912	0.340
Grey hole, Black hole, and Worm hole attacks (GBW)	5	12	1	2	1	7	8	2	1	0	6	5	0	1	0	2.069	0.150
Bogus warning messages	11	8	1	0	1	8	9	0	0	1	3	8	0	0	1	0.804	0.370
Botnet and brute force attacks	9	10	0	0	2	3	12	0	0	3	7	3	0	0	2	0.108	0.743
Denial of service attacks	9	9	0	1	2	9	7	0	2	0	4	5	2	0	1	0.032	0.858
Eavesdropping attacks	6	11	2	1	1	8	8	0	1	1	5	5	1	1	0	0.423	0.515
Fuzzy injection attacks	9	6	3	1	2	9	6	1	2	0	6	5	0	0	1	0.828	0.363
Information and hardware tampering	10	10	0	0	1	10	4	1	2	1	3	5	1	1	2	3.399	0.065
Location falsification	11	9	0	1	0	5	12	1	0	0	6	5	0	0	1	0.518	0.472
Malware attacks	4	15	0	0	2	9	8	1	0	0	5	5	0	0	2	0.103	0.748
Real-time adversaries	7	7	2	3	2	10	6	0	1	1	5	7	0	0	0	3.739	0.053
Repudiation attacks	8	10	0	2	1	7	9	0	1	1	5	4	1	0	2	0.184	0.668
Session hijacking	10	7	1	0	3	6	8	0	2	2	3	8	0	0	1	0.010	0.922
Social engineering attacks	8	8	3	0	2	10	4	3	0	1	3	8	1	0	0	0.440	0.507
Spamming and replay attacks	11	5	2	0	3	10	4	0	3	1	4	7	0	0	1	0.035	0.852
Spoofing attacks	7	12	0	1	1	6	9	1	1	1	5	5	1	1	0	0.016	0.899
Man in the middle and Sybil attacks	7	8	1	2	3	8	6	1	1	2	4	7	0	1	0	1.235	0.266
Unreliable communication channel	10	8	0	1	2	13	3	1	0	1	5	3	2	0	2	0.260	0.610

Appendix 2. Distribution of cybersecurity challenges based on organizations size

Cyber security	Company's Size	Chi-square

Challenges																Test Linear-by-linear Association α = 0.05, df = 1	
	Small (N=18)					Medium (N=20)					Large (N=13)						
	SA	A	D	SD	N	SA	A	D	SD	N	SA	A	D	SD	N	X^2	P
Authorization and authentication challenges	7	7	1	2	1	10	9	0	1	0	5	7	1	0	0	1.420	0.233
Grey hole, Black hole, and Worm hole attacks (GBW)	10	6	1	1	0	6	10	2	1	1	2	9	0	2	0	2.658	0.103
Bogus warning messages	9	8	0	0	1	10	9	1	0	0	3	8	0	0	2	2.126	0.145
Botnet and brute force attacks	6	9	0	0	3	7	9	0	0	4	6	7	0	0	0	1.551	0.213
Denial of service attacks	7	8	0	1	2	8	7	2	2	1	7	6	0	0	0	1.890	0.169
Eavesdropping attacks	7	7	2	2	0	7	10	0	1	2	5	7	1	0	0	0.365	0.546
Fuzzy injection attacks	10	5	0	1	2	9	6	2	2	1	5	6	2	0	0	0.055	0.815
Information and hardware tampering	7	10	0	0	1	9	6	0	2	3	7	3	2	1	0	0.011	0.916
Location falsification	6	12	0	0	0	10	9	1	0	0	6	5	0	1	1	0.623	0.430
Malware attacks	3	12	0	0	3	9	9	1	0	1	6	7	0	0	0	4.690	0.030
Real-time adversaries	6	8	1	1	2	12	7	0	1	0	4	5	1	2	1	0.012	0.912
Repudiation attacks	9	7	0	1	1	7	9	1	1	2	4	7	0	1	1	0.571	0.450
Session hijacking	7	9	1	0	1	8	8	0	2	2	4	6	0	0	3	1.413	0.235
Social engineering attacks	8	9	1	0	0	6	5	6	0	3	7	6	0	0	0	0.007	0.932
Spamming and replay attacks	6	8	1	0	3	14	2	1	2	1	5	6	0	1	1	0.344	0.558
Spoofing attacks	6	9	0	2	1	6	11	2	0	1	6	6	0	1	0	0.959	0.327
Man in the middle and Sybil attacks	8	4	1	2	3	7	10	1	1	1	4	7	0	1	1	0.392	0.531
Unreliable communication channel	10	6	1	0	1	12	4	1	0	3	6	4	1	1	1	0.566	0.452

Appendix 3. Distribution of cybersecurity challenges based on continents

Cyber security Challenges	Continents'			CST LBLA α = 0.05, df = 1
	Asia (N=26)	Europe (N=11)	Others (N=14)	

	SA	A	D	SD	N	SA	A	D	SD	N	SA	A	D	SD	N	X^2	P
Authorization and authentication challenges	12	12	0	2	0	5	5	1	0	0	5	6	1	1	1	1.297	0.255
Grey hole, Black hole, and Worm hole attacks (GBW)	13	10	2	1	0	1	8	0	1	1	4	7	1	2	0	2.146	0.120
Bogus warning messages	12	13	0	0	1	2	7	0	0	2	8	5	1	0	0	0.019	0.889
Botnet and brute force attacks	13	9	0	0	4	4	7	0	0	0	2	9	0	0	3	1.178	0.278
Denial of service attacks	12	7	2	2	3	5	6	0	0	0	5	8	0	1	0	1.108	0.292
Eavesdropping attacks	11	11	3	1	0	4	5	0	1	1	4	8	0	1	1	0.955	0.328
Fuzzy injection attacks	16	9	0	1	0	4	3	2	1	1	4	5	2	1	2	7.165	0.007
Information and hardware tampering	9	10	2	3	2	7	4	0	0	0	7	5	0	0	2	0.831	0.362
Location falsification	9	16	0	0	1	7	3	0	1	0	6	7	1	0	0	0.332	0.565
Malware attacks	10	13	0	0	3	3	7	0	0	1	5	8	1	0	0	0.430	0.512
Real-time adversaries	10	13	0	1	2	6	2	1	1	1	6	5	1	2	0	0.002	0.967
Repudiation attacks	12	9	1	2	2	6	4	0	0	1	2	10	0	1	1	0.276	0.599
Session hijacking	10	10	1	1	4	5	5	0	0	1	4	8	0	1	1	0.154	0.695
Social engineering attacks	11	10	5	0	0	5	4	0	0	2	5	6	2	0	1	0.574	0.449
Spamming and replay attacks	12	7	1	3	3	5	5	0	0	1	8	4	1	0	1	1.150	0.284
Spoofing attacks	10	10	2	2	2	3	8	0	0	0	5	8	0	1	0	0.955	0.328
Man in the middle and Sybil attacks	9	12	1	2	2	6	4	0	1	0	4	5	1	1	3	0.909	0.340
Unreliable communication channel	12	7	3	0	4	6	3	0	1	1	10	4	0	0	0	3.783	0.052