Information Security Risk Analysis of Vehicular Ad Hoc Networks

Kanza Bayad(✉), Mohammed Rziza, and Mohammed Oumsis

LRIT Associated Unit with CNRST (URAC No 29), Faculty of Sciences,
Mohammed V University in Rabat, B.P 1014, Rabat, Morocco
bayadkanza17@gmail.com

Abstract. The main purpose of VANETs is to improve road safety and to provide passengers' comfort. Thus, information security is one of the most important issue which attracts researchers' attention due to its open access environment. VANET requires high degree of reliability with an acceptable risk, that develops the trust between the system and users. The risk management is an essential method whose main objective is to advise and determine the appropriate actions as well as priorities to ensure information security. In this paper, we aim to apply the ISO/IEC 27005 Standard - Information Security Risk Management - on VANETs in order to classify and mitigate risks in this technology. Our contribution is an essential process that will help researchers to propose adequate solutions against the attacks in VANET based on classification results.

Keywords: VANET · Information security risk · ISO/IEC 27005

1 Introduction

In recent years, Vehicular ad hoc networks (VANETs) have become a popular concept in the Intelligent Transportation System (ITS) due to their application for improving road safety and providing passengers' comfort. Otherwise, information security has received a lot of executive attention in the new technologies and products. In this context, the security is a crucial issue in different fields especially vehicular ad hoc networks which is the scope of our work.

Security is defined as the absence of unacceptable risk, from this point onwards the analysis of risk is an essential process to determine threats, vulnerabilities and risk estimation of information security. This need is growing to achieve the final objective of developing trust between the system and users.

The communication of vehicle networks will make them vulnerable to all sorts of information security related attacks or offensive operations deployed by individuals or organizations that targets such information systems. Therefore, there is a lack of application in management tools that facilitate the analysis of risks and their mitigations in VANETs to obtain the necessary resources for information security solutions. There are several international methods related to risk management, such as Cobit and Mehari, but this paper will consider

R. Agüero et al. (Eds.): MONAMI 2016, LNICST 191, pp. 192–205, 2017.
DOI: 10.1007/978-3-319-52712-3_14

ISO/IEC 27005 (Security Risk Management Information) as being the most recent and recommended standard. So our solution undertakes the application of ISO/IEC 27005 method in VANET in order to mitigate risks in this technology.

The paper is organized as follow, Sect. 2 provides background of VANET security issues. ISO 2700x Family will be presented in Sect. 3. Section 4 will survey ISO 27005 risk management. Section 5 will offer an application of ISO 27005 standard for VANET networks. Finally, a conclusion will be given in Sect. 6.

2 VANET Security Issues

2.1 VANET Concept

The raise of mobile technologies has increased rapidly as well as it becomes more appreciated due to its ease of deployment. It has given rise to establish a new scheme called MANETs (Mobile Ad-hoc Networks), which is established without a centralized infrastructure (ad hoc). Vehicular ad hoc networks (VANET) is a particular case of MANET that provide communications into vehicles and link vehicles with roadside nodes. Its applications have several objectives such as sending safety information to avoid accidents or collisions and comfort applications (traffic jams, parking, collaborative driving, Access Internet, and so forth).

The VANET is a set of communicating entities organized under communication architecture equipped with communication units called OBUs (i.e. On Board Units) and fixed equipment called RSUs (i.e. Roadside Units). Each vehicle must also be equipped with systems to collect its position details, such as GPS (Global Positioning System). Other acronyms used in the VANETs are: V2V (Vehicle-to-Vehicle) for communication between vehicles, V2I (Vehicle-to-Infrastructure) for communication between vehicle and infrastructure - and hybrid architecture which is the combination of two approaches V2V and V2I. Figure 1 illustrates the general architecture in VANET.

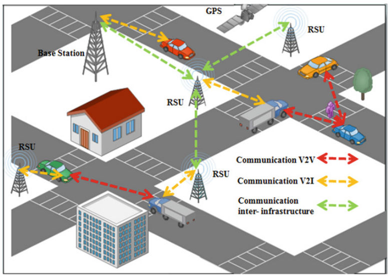


Fig. 1. General architecture in VANET

2.2 VANET Security Issues

Security Requirements

In the concept of vehicular network, several security measures should be taken to prevent cyber attacks and offensive operations. The major security requirements in vehicular network can form an acronym of CIA for Confidentiality, Integrity and Availability [1]. According to ITIL[1] (Information Technology Infrastructure Library), these can be defined as:

- **Confidentiality**: A security principle that requires that data should be accessed by authorized people only;
- **Integrity**: A security principle that ensures data and configuration items are modified by authorized personnel and activities only. Integrity considers all possible causes of modification, including software and hardware failure, environmental events, and human intervention;
- **Availability**: Ability of an IT service or other configuration item to perform its agreed function when required, and its determined by reliability, maintainability, serviceability, performance and security. Availability is usually calculated as a percentage. This calculation is often based on agreed service time and downtime. It is best practice to calculate availability of an IT service using measurements of the business output.

Attacks in VANET

VANET is vulnerable to several threats and attacks which can damage the functionality of a network, decrease its performance or compromise the security requirements [2]. In this section, we will discuss some possible threats and vulnerabilities in VANETs related to the security goals (CIA) through different scenarios.

DoS/DDoS (Denial of Service/Distributed Denial of Service): This attack [3] is one of the most dangerous threat in ITS systems, due to its major impact on the network resources. Indeed, the main goal behind these attacks is to prevent legitimate vehicles from using the network services and accessing its resources. The attacker sends various irrelevant messages to occupy a large amount of bandwidth and to consume more resources of the network. In this end, the communication channel between vehicles is blocked hence those vehicles are unable to communicate with each other on the network. In the case of DDoS Attack, several attacks are launched from different locations for the same purpose.

Message Alteration Attack: The misbehaved vehicles alter the sent messages in order to change their contents to achieve some objectives, such as injecting incorrect messages in the network to affect the behavior of other users. There are a lot of scenarios in this kind of attack that can compromise the integrity of messages in the VANET architecture by modifying, deleting, or intercepting their content [4].

[1] ITIL: http://www.itilfrance.com/.

Sybil Attack: This attack uses various false pseudonymous or identities of vehicles [5], and its major objective is to disable the network functionality by creating traffic illusion. Sybil attack makes legitimate vehicles communicate with the attacker who appear as different nodes while hiding the real identity and distribute false traffic congestion. This kind of attacks can inject false information in the network (e.g. traffic jams or accidents) [6].

Jamming Attack: The core purpose of such attack is to disrupt the communication channel between vehicles and RSU stations, by creating jams with high frequency [7]. The attacker can introduce different jamming techniques in a domain to make the network unavailable and to prevent nodes from exchanging messages in that domain.

Eavesdropping/Sniffing: In this type of attack, the adversary tries to listen to the transmission medium in order to extract information about the traffic or to collect data for analysis and perform other types of attacks (e.g. Message Alteration Attack).

3 ISO 2700x Family

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) created the global standardization system (ISO/IEC). The main purpose of international standards published by ISO/IEC, related to information security, is to maintain trust between the services and treatments of information [8].

ISO/IEC 2700x family is an overview of international standards for Information Security Management System (ISMS), which provides a framework of guidelines necessary for continuous improvement of information security. ISO 2700x family comes in 8 volumes depicted in the Table 1.

4 Methodology: ISO 27005 Risk Management

ISO/IEC 27005:2011 [9] establishes a methodology for information security risk management, which gives more details about the phases of assessment and treatment of information security risks, it is necessary to use the background of ISO/IEC 27001 and ISO/IEC 27002 to implement this standard based on a risk management technique [8].

The main objective of risk management is to advise and determine the appropriate actions as well as priorities for the management of information security risks to protect the organisational information.

ISO 27005 applies the continuous improvement cycle to the management of risks, which is known also as PDCA (Plan, Do, Check and Act) or Deming Cycle. The latter is used in all management system standards. Table 2 shows the existing alignment between the ISMS management system based on the PDCA and the risk management process.

Table 1. Descriptions of ISO/IEC 2700x family [8].

Standard	Description	Publication date
ISO/IEC 27000	This is known as **ISMS standard – Overview and vocabulary**, which provides mostly the definitions, vocabulary and terms used in the family of Information Security Management Systems (ISMS)	2014
ISO/IEC 27001	This is known as **ISMS standard - Requirements**, which is the most popular standard in this family and defines the requirements for designing, planning, implementing, monitoring as well as improving the information security of organization	2013
ISO/IEC 27002	This is known as **Code of practice for information security controls**, which describes the best practices for information security management. This standard provides guidelines for organizations to select, implement and develop their own appropriate controls for information security	2013
ISO/IEC 27003	This is known as **Information security management system implementation guidance**, which describes the steps for design and implementation plans in an ISMS project	2010
ISO/IEC 27004	This is known as **ISMS standard - Measurement**, which concerns the guidance and the assessment of how to measure the effectiveness of such aspects in ISMS of the organization	2009
ISO/IEC 27005	This is known as **Information security risk management** and it provides a methodology for information security risk management. The details of ISO 27005 are explained in the next section	2011
ISO/IEC 27006	This is known as **Requirements for bodies providing audit and certification of ISMS**. This accreditation standard aims to guide the audit and certification bodies on the requirements for being accredited as a certification body of an ISMS	2015
ISO/IEC 27007	This is known as **Guidelines for information security management systems auditing**, which provides guidance for organizations auditing an ISMS, including the compliance auditing and the competence of auditors	2011

Table 2. Alignment of ISMS and information security risk management process [9].

ISMS process	Information security risk management process
Plan	Establishing the context
	Risk assessment
	Developing risk treatment plan
	Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the information security risk
	Management process

According to this standard, the risk management process includes Context Establishment (Clause 7), Risk Assessment (Clause 8), Risk Treatment (Clause 9), Risk Acceptance (Clause 10), Risk Communication (Clause 11) as well as Risk Monitoring and Review (Clause 12). As illustrated in the Fig. 2, the risk assessment process has three main parts: Risk Identification, Risk Analysis and Risk Evaluation. The process can be interactive for both assessment as to the phases of treatment of risks, thus helping increase the breakdown of ratings in every interaction.

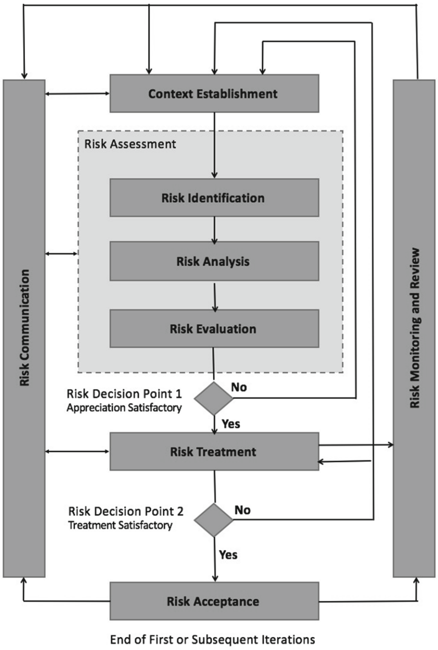


Fig. 2. Information security risk management process [9]

(1) Context Establishment

Establishment of context is the first phase of risk management process and structured in the ISO/IEC 27005 as follows:

General Considerations defines the objective of risk management activities that affects the process in the context establishment. Basic Criteria requires some measures, to warrant the risks, such as: risk evaluation criteria, risk impact criteria and risk acceptance criteria.

The scope and boundaries defines the limitations of risk management process to ensure that all assets are considered, including the definition of the process environment.

Organization for information security risk management defines roles and responsibilities for risk management process approved by the responsible manager in the organization.

(2) Information Security Risk Assessment

The process of risk assessment for information security consists of three phases: Risk Identification, Risk Analysis and Risk Evaluation.

Risk Identification determines those events which can compromise one of security requirements (CIA) following these sub-activities:

- Identification of assets;
- Identification of threats;
- Identify existing controls;
- Identification of vulnerabilities;
- Identification of consequences.

Risk Analysis describes qualitatively or quantify the level of risk in order to sort them depending on their gravity and the criticality of assets. This methodology estimates the impact of risk and probability of its occurrence.

Risk Evaluation is carried out from the results of risk analysis to make decisions about risk, it depends on the risk assessment criteria and risk acceptance criteria determined in the context establishment.

(3) Information Security Risk Treatment

The objective of this step is to establish risk treatment plan as well as define security measures and controls in order to reduce, retain, prevent or transfer risks.

Risk Reduction is accomplished by selecting of controls to make the residual risk as acceptable.

Risk Retention is the decision to allow the risk-existence without any further action based on its evaluation, this may be due to organizational policy or other reasons (e.g. cost, complexity).

Risk Prevention is used in the cases of very high risk where there are no implementing controls feasible for technical or economic reasons, it may be required to avoid them or prevent them.

Risk Transfer, in certain situations, the risk may be transferred to another party capable of treating it more appropriately or better endure the consequences.

(4) Information Security Risk Acceptance

In this phase, a decision is made to accept the risks and validate their treatment, it describes how the risks will be treated to be accepted (risk acceptance criteria). In some cases, the level of residual risk does not conform to the risk acceptance criteria, but it is used because of other reasons for the risks that are accepted.

(5) Information Security Risk Communication

During all stages of risk management, risk information should be communicated to all decision makers and stakeholders, so that all those concerned are well informed to act accordingly to implement the suitable controls and measures for the risks.

(6) Information Security Risk Monitoring and Review

The risks and their factors may vary over time. New threats and vulnerabilities may arise during the steps of risk management.

Monitoring and review of risk factors: The factors of risks must be monitored and reviewed regularly to identify any changes while maintaining a complete view of risk.

Risk management monitoring, reviewing and improving: It is important to monitor the information security incidents, to review and improve the risk factors periodically.

5 Application of ISO 27005 Standard for VANET Networks

This section demonstrates the application of the ISO 27005 standard for vehicular networks, to manage the security risk by identifying and estimating the security risks of existing information in VANETs.

5.1 Risk Identification in VANETs

Assets Identification

According to ISO27005 standard, the assets can be distinguished between primary and secondary.

Concerning the primary assets, it consists the business processes - to achieve the main objective of VANETs and to maintain its functionality as well as the activity information - it consists personal information of vehicle, information shared over the network, storage and gathering information. It can be grouped into three classes (Table 3):

Table 3. Assets identification.

Id assets	Assets	Information type
AS1	Safer roads	Warning
		Collision
		Speed
AS2	Efficient driving	Improve traffic information
		Manage traffic flow
		Parking
AS3	Entertainment information	Internet
		Mp3 download

Secondary assets consists of the support and infrastructure used in VANETs. We can classify the assets in VANETs: Users (Drivers, passengers), physical transmission medium, OBU, RSU, Global Positioning System (GPS) receivers, Control centre, Event Data Recorders (EDR), Omnidirectional antennas, Providers of commercial services, Auto-makers and Maintenance.

Threats, Existing Controls, Vulnerabilities and Consequences Identification

According to ISO 27005 standard, each threat can have one or more origins. It can be due to deliberate, accidental or environmental actions. We presented in Sect. 2.2 some possible attacks that succeed due to the vulnerabilities of VANETs. These threats made the researchers to identify and implement several solutions to address the security issue of VANETs by detecting or preventing the attacks.

The Table 4 presents major vulnerabilities in VANETs that cause such attacks, their impacts on the primary goals of information security and their solutions proposed by researchers.

Table 4. Threats, existing controls, vulnerabilities and consequences identification.

Vulnerabilities	Attacks	Compromised goals	Solutions
High dynamic topology	DOS/DDOS	Availability	Approaches to overcame Denial of Service Attack [3,10,11]
Unprotected wireless communication	Message alteration attack	Integrity	Detection of radio interference in VANET [12,13]
Same secret key used many times	Sybil attack	Availability	Cryptographic countermeasures [4,14]
Difficult to detect the malicious node	Jamming attack	Availability	Anti-jamming attack [15]
Easy to inject fault message	Eavesdropping/ Sniffing	Confidentiality	Sybil attack detection [5]
			Efficient certificate management [16]

5.2 Risk Analysis in VANETs

This phase is very important in risk assessment, it has two methods for measuring risk namely qualitative and quantitative or both. For our risk analysis, we can use a metric to calculate and estimate the level of risk. The degree for impact are 1: negligible; 2: small; 3: Limited: 4: significant and 5: severe. These levels depend on the level of exploitation of the vulnerabilities over the security goals (CIA) and the importance of the assets. However, in general, higher impacts have been assigned to threats involving road safety information, control centres or large areas of VANETs; Average impacts when they involve smaller areas of RSUs; lower impact if they are restricted to only a vehicle of convenience or information and commercial services. We can attribute criteria threat or probability for exploit as 1: rare; 2: unlikely; 3: moderate; 4: susceptible; 5: very likely. These levels depend on the degree of vulnerability of the assets and the existing controls and measures.

For this purpose, we consider scenarios from the previous attacks and estimate the risk according to the criticality of assets, the impact assessment, the frequency of the threat, the degree of vulnerability, the probability of the incident and calculate the level of risk for each identified scenario.

Scenario 1: Overload the resources of one vehicle by sending repeated messages.
Scenario 2: Overload the resources of a set of vehicles, RSUs or wireless devices vehicle by sending repeated messages.
Scenario 3: Configure vehicle sensors to generate false warning messages.
Scenario 4: Modify or delete an important packet that contains critical information.
Scenario 5: Send multiple messages from one node to others with different identifiers.
Scenario 6: Inject a stream of random data on the channel to disrupt communication.
Scenario 7: Send a malicious code to the neighbours of the target vehicle to listen to the data traffic and obtain the target vehicles ID and its location.

The final determination of the risk which is used for the estimation value of attacks is obtained by multiplying the probability of threats and their impact.

$$Risk = Impact \times Probability\,(Threat) \tag{1}$$

We can notice from the table that the value of impact and probability of threat can be inconstant depending on the scenario, for example, the first scenario (DOS Attack) has a small impact 2 on efficient driving assets because it can affect only one vehicle, the probability of threat is estimated as very likely 5 because of the ease of this attack simulation. The fifth scenario (Sybil Attack) has a severe impact 5 on safer roads and efficient driving assets, because this kind of attacks can inject false information in the network to cause incidents, the probability of threat is estimated as susceptible 4 (Table 5).

This phase can give a risk classification previously calculated, we'll derive ranking matrix from that used by ISO-27005 (Fig. 3):

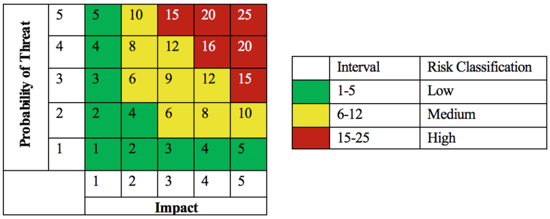
We can attribute our proposed scenarios in the matrix to classify the risk of each scenario. We are limited to these scenarios because we want to provide different examples to calculate risk.

5.3 Risk Evaluation in VANETs

This matrix shows the risk assessment of our scenarios that may result in impacts on primary assets. Incident scenarios positioned in the green area are considered

Table 5. Risk values of our scenarios.

Scenario	Assets	Impact	Probability of threat	Risk
1	2	2	5	10
2	2	4	4	16
3	1	4	3	12
4	1, 2, 3	4	3	12
5	1, 2	5	4	20
6	1, 2, 3	4	4	16
7	2	5	3	15



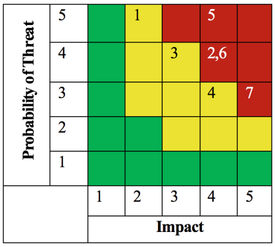
Probability of Threat						
	5	🟩 5	🟨 10	🟥 15	🟥 20	🟥 25
	4	🟩 4	🟨 8	🟨 12	🟥 16	🟥 20
	3	🟩 3	🟨 6	🟨 9	🟨 12	🟥 15
	2	🟩 2	🟩 4	🟨 6	🟨 8	🟨 10
	1	🟩 1	🟩 2	🟩 3	🟩 4	🟩 5
		1	2	3	4	5
		Impact				

	Interval	Risk Classification
🟩	1-5	Low
🟨	6-12	Medium
🟥	15-25	High

Fig. 3. Ranking matrix used by ISO-27005

as low risk; those positioned in the yellow area are considered as medium risk; and those placed in the red area are considered as high risk for the information security of VANETs. As we observe in our scenarios that is no low-risk scenario that is obvious in risk assessment, hence zero risk does not exist and we cannot guarantee a total security.

We tried to give examples from the attacks presented in the first section to give an idea about the risk value of each scenario, researchers may use this method to think about the risk that reached a high risk level for developing their own solutions against that attack (Fig. 4).



Probability of Threat						
	5	🟩	🟨 1	🟥	🟥 5	🟥
	4	🟩	🟨	🟨 3	🟥 2,6	🟥
	3	🟩	🟨	🟨	🟨 4	🟥 7
	2	🟩	🟩	🟨	🟨	🟨
	1	🟩	🟩	🟩	🟩	🟩
		1	2	3	4	5
		Impact				

Fig. 4. Risk assessment of our scenarios (Color figure online)

5.4 Risk Treatment in VANETs

According to ISO 27005 Standard, each scenario carries out an analysis of risk treatment in order to reduce, retain, prevent or transfer risks, based on the establishment of controls and solutions suggested in the literature. In this vein, those solutions are used to reduce the risk, the other options are used according to the level and the type of risks.

The solutions, measures and controls against those attacks [17] will be applied to reduce the risks of our scenarios. As depicted in the following table, the risks of the scenarios are lowered - from high level to medium, and from medium to low level - due to the solutions proposed (Table 6).

The objective of this phase is to eliminate high-risk scenario by removing the possible scenarios from the red zone as shown in the Fig. 6.

Table 6. Risk values after risk treatment.

Scenario	Assets	Impact	Probability of threat	Risk
1	2	1	3	3
2	2	4	3	12
3	1	3	2	6
4	1, 2, 3	2	1	2
5	1, 2	4	1	4
6	1, 2, 3	4	2	8
7	2	3	3	9

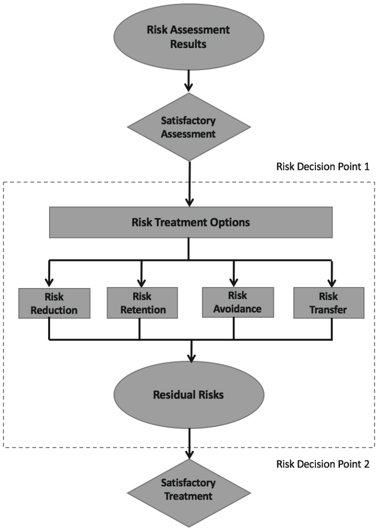
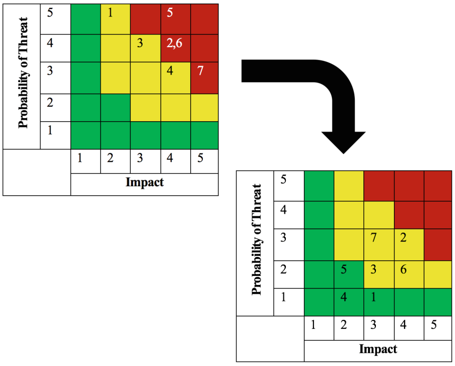


Fig. 5. Risk treatment activity [9]



Probability of Threat					
5	🟩	🟨 1	🟥	🟥 5	🟥
4	🟩	🟨	🟨 3	🟥 2,6	🟥
3	🟩	🟨	🟨	🟨 4	🟥 7
2	🟩	🟩	🟨	🟨	🟨
1	🟩	🟩	🟩	🟩	🟩
	1	2	3	4	5
	Impact				

Probability of Threat					
5	🟩	🟨	🟥	🟥	🟥
4	🟩	🟨	🟨	🟥	🟥
3	🟩	🟨	🟨 7	🟨 2	🟥
2	🟩	🟩 5	🟨 3	🟨 6	🟨
1	🟩	🟩 4	🟩 1	🟩	🟩
	1	2	3	4	5
	Impact				

Fig. 6. Risk treatment of our scenarios (Color figure online)

According to Fig. 5, the last step after the treatment of risks is to check whether the measures are satisfactory, that is, if those steps meet the risk acceptance criteria set out above.

In this study it was assumed that all the solutions presented are efficient to achieve the risk reduction estimated, and that the residual risk meet the acceptance criteria established for VANETs. Otherwise, it would take new interactions of the risk management process as illustrated in Fig. 2.

6 Conclusion

This paper performed a detailed risk analysis for VANET based on ISO 27005 standard. Through this analysis we highlighted all the phases of this standard to determine its application feasibility based on the different contexts of VANET. The main purpose of this risk analysis is to monitor incidents and process continuous improvement of security to mitigate risk as much as possible. In this paper, We have illustrated that implementing risk management on VANET will help the researchers to propose new countermeasures for any kind of attacks. Our future target is to propose a framework to facilitate risk management over VANET, it will be a pre-study for researchers before proposing solutions against attacks.

References

1. Sumra, I.A., Hasbullah, H.B., AbManan, J.B.: Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey. In: Laouiti, A., Qayyum, A., Mohamad Saad, M.N. (eds.) Vehicular Ad-hoc Networks for Smart Cities. AISC, vol. 306, pp. 51–61. Springer, Heidelberg (2015). doi:10.1007/978-981-287-158-9_5
2. Tyagi, P., Dembla, D.: Investigating the security threats in vehicular ad hoc networks (VANETs): towards security engineering for safer on-road transportation. In: 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2084–2090. IEEE (2014)

3. Malla, A.M., Sahu, R.K.: Security attacks with an effective solution for dos attacks in VANET. Int. J. Comput. Appl. **66**(22), 45–49 (2013)
4. Hamida, E.B., Noura, H., Znaidi, W.: Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic countermeasures. Electronics **4**(3), 380–423 (2015)
5. Hussain, R., Oh, H.: On secure and privacy-aware sybil attack detection in vehicular communications. Wirel. Pers. Commun. **77**(4), 2649–2673 (2014)
6. Ali Mohammad, M., Pouyan, A.A.: Defense mechanisms against sybil attack in vehicular ad hoc network. Secur. Commun. Netw. **8**(6), 917–936 (2015)
7. Malebary, S., Xu, W.: A survey on jamming in VANET. Int. J. Sci. Res. Innovative Technol. **2**, 142–156 (2015)
8. ISO/IEC 2700x Family (2016). http://www.iso.org/
9. ISO/IEC, ISO/IEC 27005, Information technology - Security techniques - Information security risk management. ISO/IEC (2011)
10. Hasbullah, H., Soomro, I.A., et al.: Denial of service (dos) attack and its possible solutions in VANET. World Acad. Sci. Eng. Technol. Int. J. Electr. Comput. Energ. Electron. Commun. Eng. **4**(5), 813–817 (2010)
11. Pathre, A.: Identification of malicious vehicle in VANET environment from ddos attack. J. Glob. Res. Comput. Sci. **4**(6), 30–34 (2013)
12. Hamieh, A., Ben-Othman, J., Mokdad, L.: Detection of radio interference attacks in VANET. In: IEEE Global Telecommunications Conference, GLOBECOM 2009, pp. 1–5. IEEE (2009)
13. Vijayalakshmi, V., Sathya, M., Saranya, S., Selvaroopini, C.: Survey on various mechanisms for secure and efficient VANET communication. In: 2014 International Conference on Information Communication and Embedded Systems (ICICES), pp. 1–5. IEEE (2014)
14. Mejri, M.N., Ben-Othman, J., Hamdi, M.: Survey on vanet security challenges and possible cryptographic solutions. Veh. Commun. **1**(2), 53–66 (2014)
15. Azogu, I.K., Ferreira, M.T., Larcom, J.A., Liu, H.: A new anti-jamming strategy for VANET metrics-directed security defense. In: 2013 IEEE Globecom Workshops (GC Wkshps), pp. 1344–1349, IEEE (2013)
16. Horng, S.-J., Tzeng, S.-F., Huang, P.-H., Wang, X., Li, T., Khan, M.K.: An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. Inf. Sci. **317**, 48–66 (2015)
17. Mokhtar, B., Azab, M.: Survey on security issues in vehicular ad hoc networks. Alexandria Eng. J. **54**(4), 1115–1126 (2015)