Security Analysis of Vehicular Ad-hoc Networks based on Attack Tree

Meriem HOUMER[1], Moulay Lahcen HASNAOUI[1] and Abdeslam ELFERGOUGUI[2].
[1]Research Team: ISIC ESTM, L2MI Laboratory, ENSAM Moulay-Ismail University, Meknes, Morocco
[2]RSI Laboratory, Faculty of Sciences, Moulay Ismail University (UMI), Meknes, Morocco.
houmer.m@gmail.com, myhasnaoui@gmail.com, elfergougui@gmail.com.

Abstract. Nowadays, Vehicular ad hoc network confronts many challenges in terms of security and privacy, due to the fact that data transmitted are diffused in an open access environment. However, highest of drivers want to maintain their information discreet and protected, and they do not want to share their confidential information. So, the private information of drivers who are distributed in this network must be protected against various threats that may damage their privacy. That is why, confidentiality, integrity and availability are the important security requirements in VANET.

This paper focus on security threat in vehicle network especially on the availability of this network. Then we regard the rational attacker who decides to lead an attack based on its adversary's strategy to maximize its own attack interests. Our aim is to provide reliability and privacy of VANET system, by preventing attackers from violating and endangering the network. to ensure this objective, we adopt a tree structure called attack tree to model the attacker's potential attack strategies. Also, we join the countermeasures to the attack tree in order to build attack-defense tree for defending these attacks.

Keywords: VANET, Security, Confidentiality, Integrity, Availability, Attack Tree, attack-defense tree.

I. INTRODUCTION

The evolution of technologies using electronics, computers, telecommunication, advanced sensors and embedded systems lead to the emergence of intelligent transport systems. This ITS intervene in a global context of traffic congestion and sometimes rail, metro or air, as well as in development of new information technologies and particularly in the areas of simulation, Real-time control and wireless networks. VANET is one of the most prominent and challenging research area in automotive societies [1] and also a key component of intelligent transportation systems to improve safety, efficiency and minimize traffic jam [2].

Each vehicle, in VANET, is equipped with a sensor whereby vehicles are able to communicate with each other via inter-vehicle communication (IVC) as well as with road side equipment via Roadside to Vehicle Communication (RVC). This communication can be used for a broad range of safety and non-safety applications, allow for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services such as finding the closest fuel station, restaurant or travel lodge and infotainment applications such as providing access to the Internet [3].

The main goal of VANET is to serve users across its potential applications and by providing timely information to drivers and interested authorities plus protecting drivers privacy from attacks perpetrated by adversaries. For that reason, the network should be available every time, but if the network is unavailable for the communication, the main goal of this network has become useless [4].

Based on attack and attack-defense tree, we propose in this study two models: the first is about the possible attacking strategies, the attacker may lead against the availability of network and the second about how to defending these attacks.

The rest of this paper is organized as follows: Section 2 introduce the fundamental attack tree and how to build its. Section 3 present the attack-defense tree. The attack tree and attack-defense tree models for VANET availability is given in Section 4. We conclude this paper in section 5.

II. ATTACK TREE FUNDAMENTALS

A. Definition

Attack tree is a conceptual diagram showing the various ways in which a system can be attacked [5]. Attack trees have been used in several applications, such us fields of defense and aerospace to analyze the threats against tamper resistant electronics systems information technology. Also, in the domain of information technology they have been used to construe threats on computer systems and probable attacks to realize those threats.

Attack trees are constructed from the point of view of the adversary. thinking like an attacker is required for releasing a performing attack tree [6]. So firstly, it is not necessary to reflect about the ways to defend a system but to think about how to violate its security.

An attack tree is a tree wherein each node depicts an attack. the global goal of an attacker also named root node is located at the top of the tree. The root branches downwards, leafs (or sub-goals) represent attacks that can no longer be refined. There are various different types of attack trees like Vulnerabilities Tree [7], Protection Tree [8], Defense Tree [9], and Attack-Defense trees [10]. All of them have the same characteristics of attack tree. There are a few things that make them different.

978-1-5386-4248-1/18/$31.00 ©2018 IEEE

B. Attack Tree Construction

The process involved in constructing the attack tree aims to determine the sequence of events that can lead to the final event chosen. This analysis ends when all the potential causes correspond to elementary events [11]. The development of the attack tree follows the sequence in fig. 1.

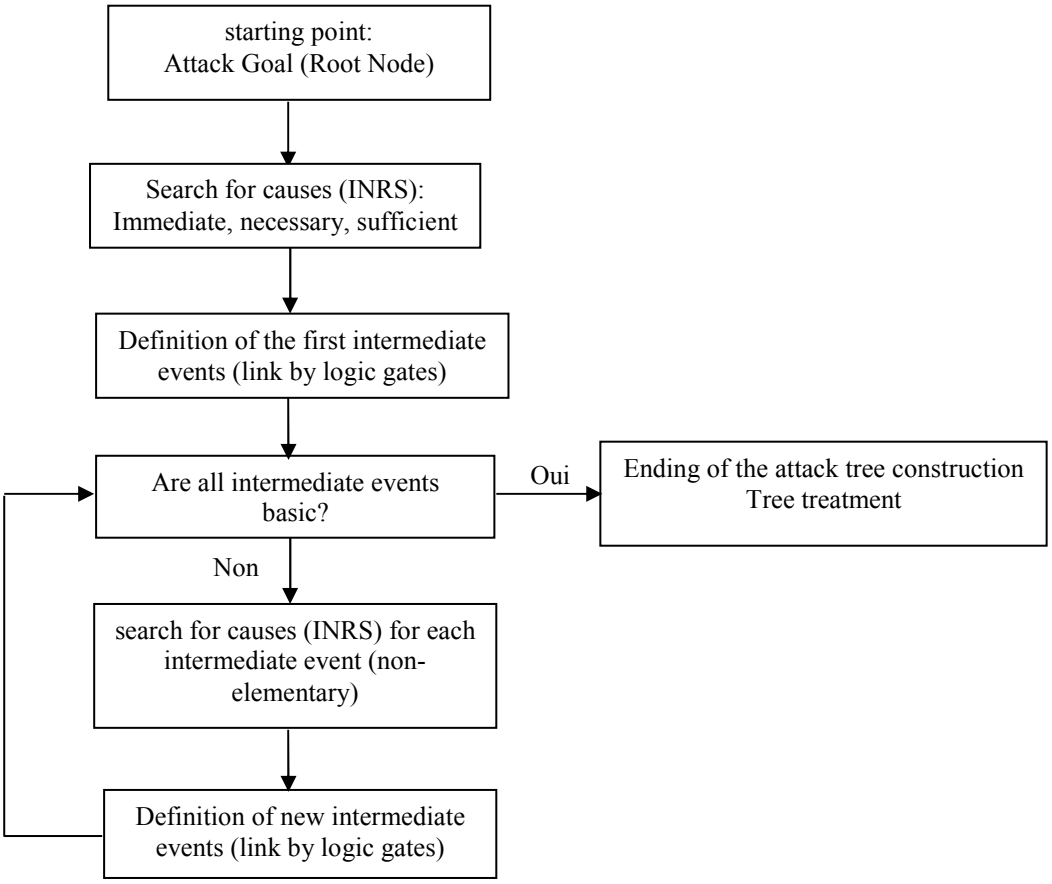

Figure 1: Approach for the development of an attack tree

The systematic research for the immediate, necessary and sufficient causes (INRS) is the basis of the construction of attack tree. This is the most delicate step and it is often useful to proceed with this construction within a multidisciplinary working group. In addition, the prior implementation of other methods of inductive risk analysis greatly facilitates the search of attacks for the development of the tree. In order to select the intermediate events, it is essential to proceed step by step, taking care to identify the direct and immediate causes of the attack goal and to ask whether these causes are necessary and sufficient. Otherwise, the resulting tree may be partially incomplete or even erroneous. Finally, it is necessary to respect certain additional rules during the construction of the tree namely:

- Check that the system is consistent, that is:
- Failure of all components causes system failure,
- The proper functioning of all its components leads to the proper functioning of the system,
- When the system is down, considering a new attack does not restore the system operation,
- When the system is operating properly, removing an event (attack) does not cause the system to fail. It may happen that an attack occurring on a component cancels the effects of an attack anterior and thus allows the operation of the system. In a non-coherent system, the second component must be assumed, in the analysis, in operation when the first attack occurs.
- Make sure that all the input events of a logical gate have been identified before analyzing their respective causes,
- Avoid connecting two logical gates directly,
- Just select anterior causes before the existence of the event.

Attack tree admit two sort of gates which is OR and AND gates. The OR gate are alternatives, it represents different ways to achieving the same goal. The AND gates represent different steps toward achieving the same goal.

To analyze the system, we select a particular event of the system as an attacker's goal, and then determine the immediate, necessary, and sufficient causes for the occurrence of this goal. It should be noted that these are not the basic causes of the goal but the immediate causes for the event.

These immediate, necessary, and sufficient causes of the goal are now treated as sub-goals and we proceed to determine their immediate, necessary, and sufficient causes. In this way we construct our attack tree model for the vehicular ad hoc network system, selecting availability of network issues as attacker's goals [12].

III. ATTACK DEFENSE TREE

Defense trees is an extension of attack tree have been introduced as a methodology for the analysis of attack/defense security scenarios. Attack defense trees allows an in-depth security analysis related to traditional attack tree, for the reason that interactions between attacker and defender are modeled in attack defense tree.

An attack defense tree has two kinds of nodes: attack and defense nodes.

There are two principal characteristics of attack defense tree which are: the representation of refinements and countermeasures.

Each node can have one or more children of the similar type representing a refinement into sub-goals of the node's goal. If a node does not have any children of the same type, it is called a non-refined node. Non-refined nodes represent basic actions. each node can as well have one children of the reverse type, showing a countermeasure.

thereby, an attack node can have various children which refine the attack and single children which defends versus attacks. In turn, defending children can have many children which refine the defense and single children that is an attack node and counters the defense [13].

IV. BUILDING ATTACK TREE AND ATTACK-DEFENSE TREE FOR VANET AVAILABILITY

A. Attack Tree Model for Availability of network for VANET

For building our attack tree, we achieve a stepwise refinement approach. The attacker's global goal in our tree is Availability of network which is denoted by G (see Fig.2).

Proceeding of the attack tree building is as follows:

- Determine the attacker's global goal G: Availability of network.
- Decompose the goal G into sub-goals: Black Hole (S1) is an attack where the network traffic is redirected, Denial of Service (S2), Malware & spam (S3). The attacker's goal can be achieved if any of the sub-objectives is achieved. This list might be expanded and some sub-goals could be added.
- Pursue the stepwise construct into different component. The Attack Tree is the final diagram of attack.

The black hole (S1) sub-goal can be occurred by joint two steps:

- Cheat the routing protocol (X1).
- Establish a forged route (X2).

In a black hole attack, a spiteful node cheats the routing protocol for having the shortest pathway to the target node. When the route is established between malicious and target node, attacker can drop traffic incoming or outgoing without denouncing the source that the data did not attain its destination or forward the packets to wherever it wants [14].

The second sub-goal is denial of Service (S2). A denial of service (DOS) attack is a type of attack designed to make the services or resources of a network unavailable for a temporary or indefinite time of a host connected to the Internet.

In order to get this sub-goal, it is requisite to perform:

- Channel jamming (S21), the objective of the attacker by channel jamming is to prohibit nodes to access network services. this task can arise through transmit dummy message (X3) in which an attacker sends multiple messages with a different fabricated source identity to the other vehicles. The basic goals of the attacker have reduced the efficiency and performance of the network by dispatching wrong messages and to impose other vehicles to leave the road for the favor of the attacker [15]. Channel jamming can also be achieved by sending high frequency signals (X4). In this task, the attacker sends request messages with oversized frequency, causing the crash the systems, then cannot send or receive messages on the network [16].
- Smurfing (X5). In the case of a Smurf denial of service (DoS) attack, when executing the ping tool, an ICMP echo request packet is sent to the target computer. the return IP address of the ping packet is established from the IP address of the target computer. The ping is sent to all broadcast IP address. Each computer responds to simulated ping packets and responds to the target computer, which is then saturated.
- Flooding (S22), which is designed to make a network or service unusable (disconnecting users from an Internet Relay Chat server) by flooding it with large amounts of traffic. this mission can be realized if two tasks are accomplished which is SYN flood (X6) or UDP flood (X7).

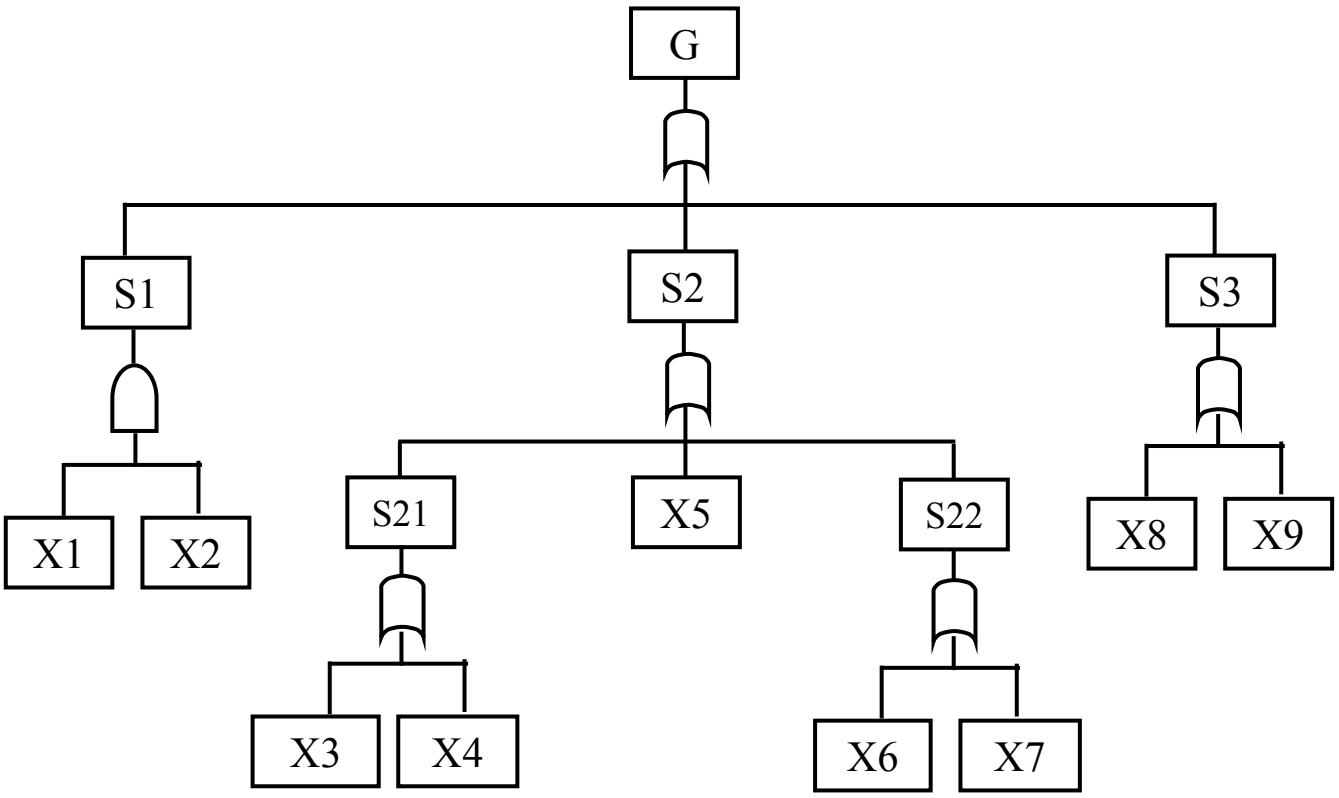

Figure 2: Attacks on Availability of VANET

The SYN flood is intended to make a network unavailable. This attack is applied in the context of a TCP (Transmission Control Protocol) and aims primarily to overwhelm the target server with many SYN requests (Synchronized), in order to not respond to legitimate SYN requests from other nodes. In the same way as for SYN flooding, in UDP flood, the attacker sends a large number of UDP requests to a node. Since UDP traffic has priority over TCP traffic, this type of attack can quickly disrupt and saturate traffic flowing through the network.

The final sub-goal is Malware and spam (S3).

Malicious software (Malware) is program created by hackers for the purpose of harming a computer system, collect sensitive information, or to access to private computer data.

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately.

To reach this sub-goal (S3), it is requisite to carry out:

- Introduce virus and worm (X8), by inserting a copy of itself into a reliable program and becoming part of it.
- Sending spam messages (X9). By sending junk messages, the attacker can consume the quota available through an email service and then preventing you from receiving legitimate messages.

B. Attack-Defense Tree Model for Availability of network

In this section we will build the attack-defense tree model for availability of network for VANETs (see Fig.3) based on the above attack tree model.

In order to deal with the attacks cited in the attack tree, we introduce some defense mechanisms who express the potential countermeasures which could be used to secure the system [16]. The attack-defense tree for VANETs availability is shown in Fig. 3.

To protect VANET against Black Hole attack, it is requisite to use packet sequence numbers in the packet header or introduce an intrusion detection system.

- By using packet sequence numbers in a packet header (D1), the destination can recognize any lost packet from the missing packet sequence number.
- IDS (D2) is a mechanism that listens to network traffic in a sneaky manner in order to identify abnormal or suspicious activities and thus to have a preventive action on the risks of intrusion. Sivaranjanadevi et al. [18] proposed an intrusion detection system that use support vector machine technique and Rough Set Theory to pick up black hole attacks in order to identify malicious vehicle.

The corresponding countermeasures to each leaf of DOS attack are:

- Suggest to the OBU to switch channel (D3), using frequency hopping technique or multiple transceiver (D4) to fight channel jamming [19].
- Ingress filtering (D5) can face to Smurf attack (S22). This countermeasure is employed to assure that incoming packets are really from the networks from which they pretend to come from. Network ingress filtering rejects the attacking packets on the basis of the forged source address.

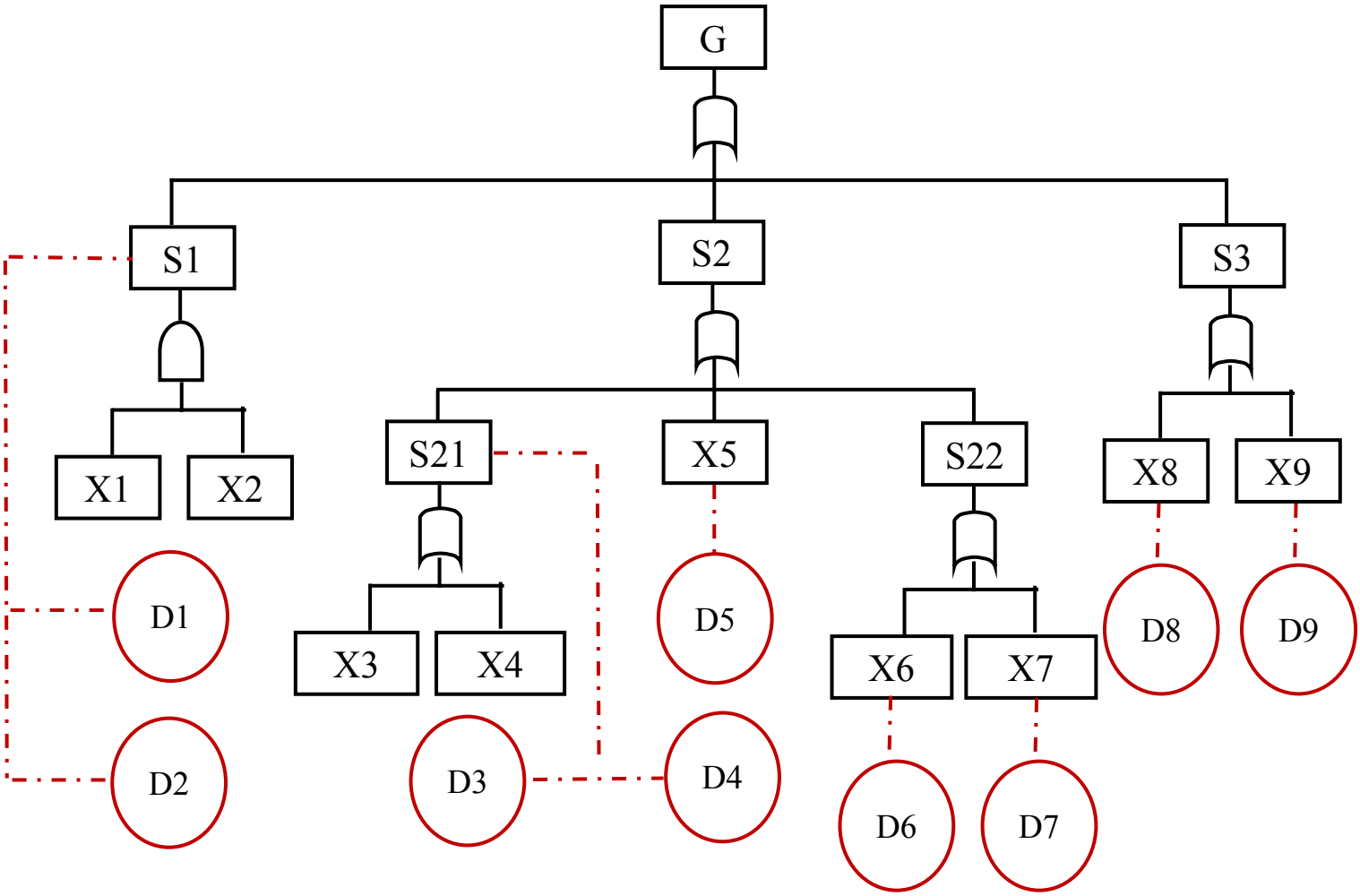

Figure 3: Attack-Defense tree for Availability of VANET

- To defend against SYN flood attacks (S231), it is necessary to use SYN cookies (D6), which are special values of the initial sequence numbers generated by a server (ISN: Initial Sequence Number) during a TCP connection request.
- UDP flood attack (S232) can be handled by installing firewalls (D7) at different positions in the network to filter out undesirable network traffic. thus, the target node does never receive or responds to the malicious UDP packets because the firewall stops them.

In order to guard the network versus Malware and spam (S3), anti-malware and anti-spamming must be used.

- introducing anti-malware malware (D8) in road side unit can protects systems against infections with many types of malwares.
- Blocking and mitigating the impact of illegal emails by using anti-spamming (D9).

V. Conclusion

Attack tree is a way to represents different possible combinations of events that describe the computer security threats launched by an attacker against a system.

In this paper, we analyze the threats that facing the availability of VANET from the system viewpoint. Moreover, we build an attack tree with availability of network as attack

goal for studying the attacker's behavior. We also proposed an attack–defense tree as a new model that represent vulnerabilities in the network and the possible solutions that a defender can employ to protect the availability of vehicular network.

In our future work, we will introduce a risk assessment in which we calculate the total probability of attaining attack goal based on the attack tree. According to the result, the defender can resolve which countermeasure might be adopted.

REFERENCES

[1] Mayada Abdelgadir, Rashid Saeed and Abuagla Babiker. Vehicular Ad-hoc Networks (VANETs) dynamic performance estimation routing model for city scenarios. In: International Conference on Information Science and Communications Technologies (ICISCT), IEEE, (2016).

[2] Pallavi A Targe and M P Satone. VANET based Real-Time Intelligent Transportation System. International Journal of Computer Applications 145(4), 34-38 (2016).

[3] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin and Aamir Hassan. Vehicular ad hoc networks (VANETS): status, results, and challenges. Telecommunication Systems. Springer, 217–241 (2010).

[4] Irshad Ahmed Sumra, Halabi Bin Hasbullah and Jamalul-lail bin AbManan. Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey. Book: Advances in Intelligent Systems and Computing. Springer. (2014).

[5] Sjouke Mauw and Martijn Oostdijk. Foundations of Attack Trees. In: Conference on Information Security and Cryptology, Springer, (2005).

[6] Amenaza and SecurITree. Attack Tree-based Threat Risk Analysis. Amenaza Technologies Limited. (2010).

[7] Stilianos Vidalis and Andy Jones. Using Vulnerability Trees for Decision Making in Threat Assessment. In: 2nd European Conference on Information Warfare. (2003).

[8] Yonggang Li, Yaohui Jin, Lemin Li and Longjiang Li. On Finding the Multicast Protection Tree Considering SRLG in WDM Optical Networks. Electronics and Telecommunications Research Institute. Wiley. (2006).

[9] Stefano Bistarelli, Marco Dall'Aglio and Pamela Peretti. Strategic Games on Defense Trees. Springer. (2006).

[10] Barbara Kordy, Sjouke Mauw, Saša Radomirovićand and Patrick Schweitzer. Foundations of Attack–Defense Trees. In: International Workshop on Formal Aspects in Security and Trust. Springer. (2016)

[11] Marlon Fraile, Margaret Ford, Olga Gadyatskaya, Rajesh Kumar, Mariëlle Stoelinga and Rolando Trujillo-Rasua. Using Attack-Defense Trees to Analyze Threats and Countermeasures in an ATM: A Case Study. In: IFIP Working Conference on The Practice of Enterprise Modeling, Spinger, (2016).

[12] Suguo Du and Haojin Zhu. Security Assessment via Attack Tree Model. book Springer Briefs in Computer Science, Springer,9-16 (2013).

[13] Barbara Kordy, Piotr Kordy, Sjouke Mauw, Patrick Schweitzer. ADTool: Security Analysis with Attack-Defense Trees. In: International Conference on Quantitative Evaluation of Systems, Springer, (2013).

[14] Vimal Bibhu, Kumar Roshan, Kumar Balwant Singh and Dhirendra Kumar Singh. Performance Analysis of Black Hole Attack in Vanet. International Journal Computer Network and Information Security, (2012).

[15] Halabi Hasbullah, Irshad Ahmed Soomro and Jamalul-lail Ab Manan. Denial of service (DOS) attack and its possible solution in VANET. International Journal of Electronics and Communication Engineering. (2010).

[16] Al-kahtani, Salman bin Abdulaziz and Al Kharj. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In: 6th International Conference on Signal Processing and Communication Systems (ICSPCS). (2012).

[17] Barbara Kordy, Sjouke Mauw, Saša Radomirovićand and Patrick Schweitzer. Attack–Defense Trees. Journal of Logic and Computation. 55–87(2012).

[18] P. Sivaranjanadevi, M. Geetanjali, S. Balaganesh and T. Poongothai. An Effective Intrusion System for Mobile Ad Hoc Networks using Rough Set Theory and Support Vector Machine. International Journal of Computer Applications. (2012).

[19] Karan Verma, Halabi Hasbullah and Ashok Kumar. Prevention of DoS Attacks in VANET. In: Wireless Personal Communications. (2013).