

## Chapter 2

# Security Assessment via Attack Tree Model

**Abstract** Even though emerging as a promising approach to increase road safety, efficiency and convenience, Vehicular Ad hoc Networks (VANETs) pose many new research challenges, especially on the aspect of location privacy. The existing literatures focus on preventive techniques to achieve location privacy protection, however the location privacy risk assessment receives less attention. In this chapter, we introduce a novel risk assessment method to evaluate the security risk of VANETs privacy based on attack tree.

### 2.1 Introduction of Privacy Protecting in VANETs

Vehicular ad hoc networks [24] (or VANETs) are self-organized networks designed for communication among vehicles. In VANET, each vehicle is equipped with an On Board Unit, by which vehicles are able to communicate wireless with each other as well as Road Side Units. VANETs are expected to support a wide range of promising applications such as location based services. However, the broadcast nature of the wireless medium allows an adversary to eavesdrop on the communications containing node identifiers, and to estimate the locations of the communicating nodes with an accuracy that is sufficient for tracking the nodes. For example, in [25], it is reported that the adversary can even approximately derive the drivers family address and their workplaces with the collection of location traces every day. Due to these reasons, location privacy threat [26] has been well recognized as one of the major security threats for VANETs and has attracted a lot of interest recently.

The existing research on VANET privacy mainly focuses on the preventive techniques including: pseudonym [27] based approaches, group signature [28] based techniques or mix-zone [26, 29, 30] based approach. The basic idea of the preventive techniques is introducing the privacy protection techniques to prevent the compromise of user location privacy. However, the preventive schemes may face the challenges that it can only address the expected security vulnerabilities while have nothing to do with the unexpected privacy threats. Furthermore, from a system point of view, a comprehensive yet well-defined security evaluation enables the system administrator to identify the most critical security threats and attack strategies, which are more than important for the overall success of VANET deployment. Even though some reported studies also investigate the possible security vulnerabilities, they fail to give a quantity risk analysis from a system point of view.

In this study, we propose a novel risk assessment approach for location privacy preserving in VANETs based on the attack tree based approach. Attack tree based risk analysis leverages tree based method to model and analysis the risk of the system and identify the possible attacking strategies the adversaries may launch. With the help of the attack tree model, it is convenient to analyze the capability of the attack source and estimate the degree or the impact a certain threat might bring to the system. Due to these features, in this chapter, we take advantage of attack tree based approach to identify the possible threats. And we further calculate the total probability of reaching attack goal on the basis of the attack tree. According to the quantitative result, the decision maker of the system can decide which protection measure should be adopted.

The reminders of this chapter are organized as follows: in Sect. 2.2, we introduce the attack tree method and present how to build the attack tree. In Sect. 2.3, we assign values to leaf nodes and calculate the systems risk. In Sect. 2.4, to estimate the most likely way an attacker may choose, we carry out an analysis of attack scenarios on the basis of attack tree. At last, in Sect. 2.5, we summarize the conclusion .

## 2.2 Attack Tree Model for VENET Privacy

An attack tree [31] can be simply described as an analytical technique, whereby an undesired state of the system is specified, and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur [32]. There are two basic types of attack tree gates: the OR-gate and the AND-gate. The OR-gate is used to show that the output event occurs only if one or more of the input events occur. The AND-gate shows that the output attack occurs only if all the input attacks occur. 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 proceed down the tree continually, until ultimately we reach the limit of resolution of our tree, that is leaf node (atomic attack) of an attack tree.

In VANET system, we choose "leakage of location privacy", which is denoted by  $G$ , as the attack goal. Now we proceed with a step-by-step analysis of the attack goal. The intermediate causes of the goal are: direct communication, eavesdropping, stealing and illegal disclosure, which are respectively marked with  $M_1$ ,  $M_2$ ,  $M_3$ , and  $M_4$ . The mission objective can be achieved if any of the four components is reached. Now we identify the four intermediate causes as sub-goals, and it is necessary to determine their immediate cause or causes separately.

There are two possibilities for direct communication ( $M_1$ ).

“Inquiry ( $X_1$ )”: an attacker communicates with a target node with real identity of itself, and then inquiries the node’s location privacy. This way applies only when a node has low sensitivity on its privacy.

“Cheating ( $M_5$ )”: an attacker impersonates as someone else that the target node trusts, and gets privacy of the target node by communicating with it. Since nodes which have close relationship with a target node such as friends, colleagues or service providers are supposed to be reliable for most nodes, this kind of attack succeeds with higher opportunity.

Therefore, the sub-goal “direct communication ( $M_1$ )” can arise from two events, “inquiry ( $X_1$ )” or “cheating ( $M_5$ )”. Now we are ready to seek out the immediate causes for the new sub-goal “cheating ( $M_5$ )”, which appears as intersection of two events: “finding vulnerabilities in the systems authentication mechanism  $X_2$ ” and “making fake identity  $X_3$ ”.

We now continue the analysis by focusing our attention on event “eavesdropping ( $M_2$ )”. To get a node’s privacy by “eavesdropping ( $M_2$ )”, it is necessary to carry out “physical layer eavesdropping ( $M_6$ )”, or “MAC layer eavesdropping ( $M_7$ )”, or “application layer eavesdropping ( $M_8$ )”. We identified  $M_6$ ,  $M_7$ , and  $M_8$  as intermediates which will be analyzed as below.

Physical layer eavesdropping ( $M_6$ ): This mission can be achieved if two tasks were accomplished in a row: “dismantle wiretap-proof device  $X_4$ ” and “installing wiretap device  $M_{11}$ ”. There are three ways for an attacker to successfully “installing wiretap device  $M_{11}$ ”: “being a service provider for cars  $X_5$ ”, or “disrupting the cars anti-theft system  $X_6$ ”, or “making use of the owners carelessness  $X_7$ ”.

MAC layer eavesdropping ( $M_7$ ): The attack “MAC layer eavesdropping ( $M_7$ )” can be launched through two joint atomic attacks: “protocol vulnerability analysis  $X_8$ ” and “resetting its own configuration  $X_9$ ”.

Application layer eavesdropping ( $M_8$ ): In application layer, an attacker can choose from two aspects to eavesdrop: “eavesdropping pseudonyms  $M_{12}$ ” or “running eavesdropping software  $M_{13}$ ”. Each of the two is further decomposed into sub-components. For “eavesdropping pseudonyms  $M_{12}$ ”, it is essential for an attacker to “obtaining signal receiver  $X_{10}$ ” and “analyzing the adopted pseudonym mechanisms weaknesses  $X_{11}$ ”. While for “running eavesdropping software  $M_{13}$ ”, after “breaking the networks firewall  $X_{12}$ ” an attacker needs to “being familiar with wireless networks weak security feature  $X_{13}$ ” and then compromise the target node by planting eavesdropping program.

Sub-components of “stealing  $M_3$ ” include “physical theft  $M_9$ ” and “malicious node theft  $M_{10}$ ”. These two sub-components are represented by a logical OR relationship in the attack tree construction, for any occurrence of the two possible events which may result in the happening of “stealing  $M_3$ ”. In the attack “physical theft  $M_9$ ”, three steps must be taken: “stealing the car  $M_{14}$ ”, “disrupting the function of removing data from remote control  $X_{15}$ ” and “deciphering encrypted file  $X_{14}$ ”. When an attacker steals a car, he can adopt the same approaches as in “installing wiretap device  $M_{11}$ ”. “malicious node theft  $M_{10}$ ” refers to an attack using malicious program to steal privacy stored in the vehicles storage media. It requires an attacker to “deciphering encrypted file  $X_{14}$ ” as well as “breaking the networks firewall  $X_{12}$ ”.

As far as the last intermediate cause of the attack goal “illegal disclosure  $M_4$ ” is concerned, it is decomposed into a logical OR relationship of two atomic attacks: “purchasing privacy information from third party  $X_{16}$ ” or “leakage from official department  $X_{17}$ ”. Third parties such as location service providers, employees collect large information about nodes privacy, so it is possible that these trusted third parties might sell their collected privacy for commercial profit. For the convenience of management, official management department could also leak nodes privacy accidentally.

According to the analysis above, we built the attack tree model which is presented in Fig. 2.1. Notations of gates and leaf nodes in the attack tree are listed in Table 2.1.

### 2.3 Risk Assessment

For the limitation of resources, an attacker has to take into account of many aspects including the possibility to succeed, attack cost, technique difficulty, risk of being detected and so on. In this work, we calculate the total probability of reaching the attack goal by assigning leaf nodes three attributes: attack cost, technical difficulty and discovering difficulty, which are denoted as  $c_L$ ,  $d_L$  and  $s_L$  respectively. The grade level standards are given in Table 2.2. The values of  $c_L$ ,  $d_L$  and  $s_L$  depend on the following rules.

An attacker could launch an attack on any layer of the system. The higher the attacked layer is, the more difficult for the attacker, and the lower the probability of success. In this condition, we can sort those layers according to the difficulty of compromise in the following order: application layer > transmission layer > routing layer > MAC layer > physical layer.

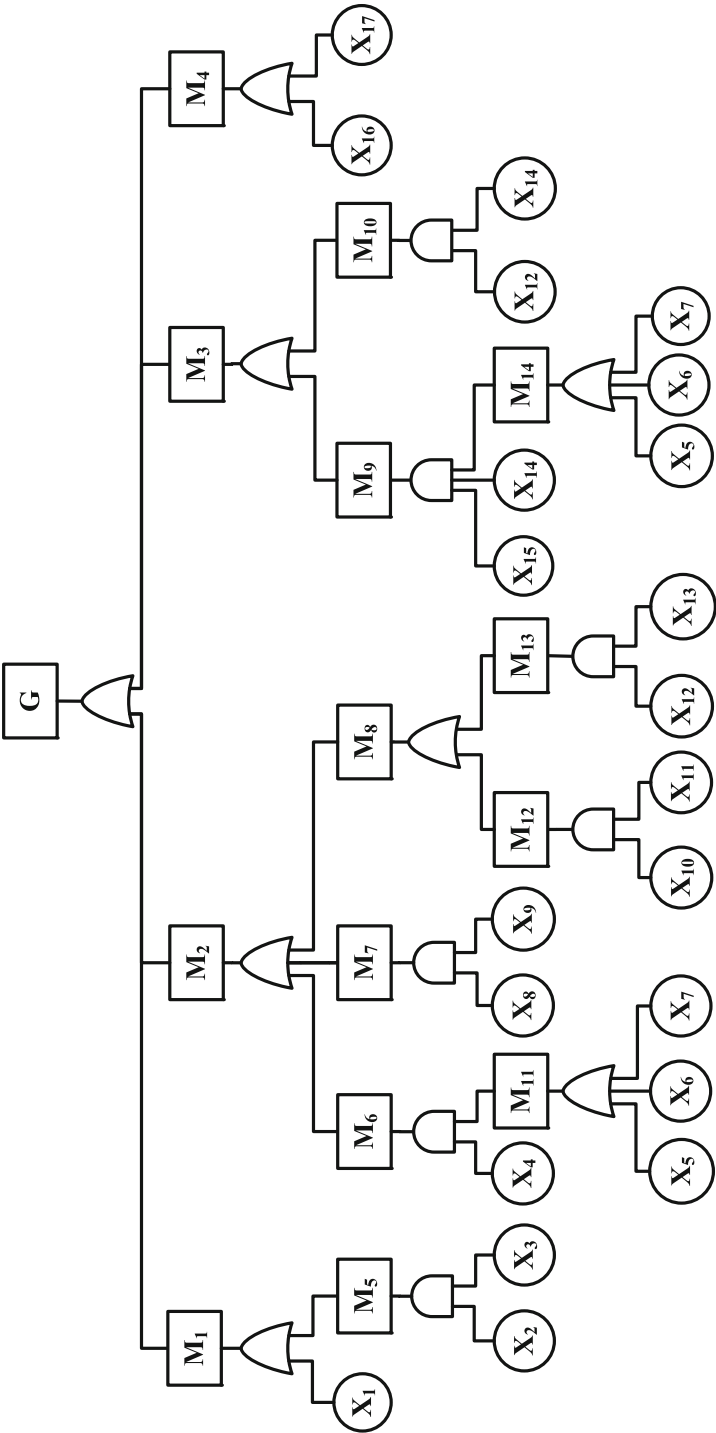
Cost of physical vehicle and labor assistant is higher compared with that of analyzing protocol or mechanisms vulnerabilities. Powerful nodes, for instance traffic offices or service providers, are capable of taking more protecting behaviors, so these nodes are more difficult to be compromised than common nodes.

The multi-attribute utility theory [34] is adopted to transfer these three attributes into attackers utility value, which is the occurrence probability of a leaf node. The following is a formula we applied to calculate the utility of each leaf node:

$$P_L = w_1 \times u(c_L) + w_2 \times u(d_L) + w_3 \times u(s_L)$$

Where  $u(c_L)$ ,  $u(d_L)$ ,  $u(s_L)$  represent the utility functions of  $c_L$ ,  $d_L$  and  $s_L$ , and their values fall into the interval of  $[0, 1]$ ;  $w_1$ ,  $w_2$ ,  $w_3$  are the weights of the utilities, where  $w_1 + w_2 + w_3 = 1$ .

For the convenience of calculation, we define that  $w_1 = w_2 = w_3 = 1/3$ . The specific assignment of each nodes attribute requires knowledge of implementation details of the system in question including protocols, hardware, operating system as well as attack software and tools. Since the main focus of this chapter is proposing a new evaluation method, we assign the value to each leaf node, which is listed in Table 2.3. In order to get the occurrence probability of each leaf node, we also



**Fig. 2.1** Attack tree model for VANETs location privacy

**Table 2.1** Notations and meanings of gates and leaf nodes

Notations	Meaning	Notations	Meaning
$G$	Leakage of location privacy	$X_2$	Finding vulnerabilities in the authentication mechanism
$M_1$	Direct communication	$X_3$	Making fake identity
$M_2$	Eavesdropping	$X_4$	Dismantling wiretap-proof device
$M_3$	Stealing	$X_5$	Being a service provider for cars
$M_4$	Illegal disclosure	$X_6$	Disrupting a cars anti-theft system
$M_5$	Cheating	$X_7$	Making use of the owners carelessness
$M_6$	Physical layer eavesdropping	$X_8$	Protocol vulnerability analysis
$M_7$	MAC layer eavesdropping	$X_9$	Resetting its own configuration
$M_8$	Application layer eavesdropping	$X_{10}$	Obtaining signal receiver
$M_9$	Physical theft	$X_{11}$	Analyzing the adopted pseudonym mechanisms weakness
$M_{10}$	Malicious code theft	$X_{12}$	Breaking the networks firewall
$M_{11}$	Installing wiretap tool	$X_{13}$	Being familiar with wireless networks weak security feature
$M_{12}$	Eavesdropping pseudonyms	$X_{14}$	Deciphering the encrypted file
$M_{13}$	Running eavesdropping software	$X_{15}$	Disrupting the function of removing data from remote control
$M_{14}$	Stealing the car	$X_{16}$	Purchasing privacy from third party
$X_1$	Inquiry	$X_{17}$	Leakage from official department

**Table 2.2** Grade standard

Attack cost/Ten Thousands		Technical difficulty		Discovering difficulty	
$c_L$	Grade	$d_L$	Grade	$s_L$	Grade
$> 10$	5	Quite difficult	5	Quite difficult	1
6–10	4	Difficult	4	Difficult	2
3–6	3	Mediate	3	Mediate	3
0.5–3	2	Simple	2	Simple	4
$< 0.5$	1	Quite simple	1	Quite simple	5

need to determine the utility function. Since all the three attributes are inversely proportional to their respective utility value, we suppose that the three utility functions  $u(c_L) = u(d_L) = u(s_L) = u(x) = c/x$  (where, the value of parameter  $c$  is set as 0.2 in this book for illustration). Then the occurrence probability of each leaf node can be calculated (see the rightmost column in Table 2.3) by using the utility functions combined with the attribute values assigned to leaf nodes.

So as to calculate the total probability of reaching the attack goal, the attack tree is transferred to a BDD [33] (Binary Decision Diagram). We get that the total probability of reaching the attack goal is 0.239. From analysis of structure importance degree, three atomic attacks “inquiry ( $X_1$ )”, “purchase privacy from third party ( $X_{16}$ )” and “leakage from official department ( $X_{17}$ )” take main responsibility for the occurrence of the attack goal.

**Table 2.3** Attribute values for leaf nodes

Leaf node	Attribute			Occurrence probability
	Attack cost	Technical difficulty	Discovering difficulty	
$X_1$	3	2	5	0.069
$X_2$	3	4	2	0.072
$X_3$	2	1	4	0.117
$X_4$	1	2	2	0.133
$X_5$	5	1	5	0.093
$X_6$	2	3	4	0.072
$X_7$	1	2	3	0.122
$X_8$	3	3	1	0.111
$X_9$	4	2	1	0.117
$X_{10}$	2	4	2	0.083
$X_{11}$	3	4	3	0.061
$X_{12}$	2	3	2	0.089
$X_{13}$	2	5	1	0.113
$X_{14}$	1	2	4	0.117
$X_{15}$	4	5	5	0.043
$X_{16}$	4	4	3	0.056
$X_{17}$	5	2	5	0.060

## 2.4 Attack Scenarios

An attack scenario [34] is a set of leaf nodes, in which only the occurrence of all the leaf nodes could reach the attack goal, that is to say the goal will not be realized if one of the leaf nodes does not occur. An attack scenario is the real attack way that an attacker considers. Once the attack scenarios have been known, we could calculate their probabilities of occurrence, and then compare them to find out the attack scenario that the malicious may launch most likely. Suppose an attack scenario is denoted as:

$$S_i = (X_{i_1}, X_{i_2}, \dots, X_{i_n})$$

Then the probability of an attack scenario is:

$$P(S_i) = P(X_{i_1}) \times P(X_{i_2}) \times \dots \times P(X_{i_n}) \quad (2.1)$$

We adopt Boolean algebra method to get all the attack scenarios for our attack tree. It can be seen that there are fourteen attack scenarios to achieve the attack goal, and they respectively are  $\{X_1\}$ ,  $\{X_2, X_3\}$ ,  $\{X_4, X_5\}$ ,  $\{X_4, X_6\}$ ,  $\{X_4, X_7\}$ ,  $\{X_8, X_9\}$ ,  $\{X_{10}, X_{11}\}$ ,  $\{X_{12}, X_{13}\}$ ,  $\{X_5, X_{14}, X_{15}\}$ ,  $\{X_6, X_{14}, X_{15}\}$ ,  $\{X_7, X_{14}, X_{15}\}$ ,  $\{X_{12}, X_{14}\}$ ,  $\{X_{16}\}$ ,  $\{X_{17}\}$ . In the first scenario  $\{X_1\}$ , it means an attacker can get the targets privacy by just launching the atomic attack  $X_1$ , while in the second scenario  $\{X_2, X_3\}$ , an attacker requires to compromise the systems authentication mechanism  $X_2$  as well as making fake identity  $X_3$ . From the Eq. 2.1, we calculate probabilities of occurrence for attack sequences which are listed in Table 2.4.

**Table 2.4** Probabilities of attack sequences

Attack sequence	Probability
$S_1$	0.0690
$S_2$	0.0084
$S_3$	0.0123
$S_4$	0.0096
$S_5$	0.0162
$S_6$	0.0130
$S_7$	0.0051
$S_8$	0.0101
$S_9$	0.0005
$S_{10}$	0.0004
$S_{11}$	0.0006
$S_{12}$	0.0104
$S_{13}$	0.0560
$S_{14}$	0.0600

From the Table 2.4, we find that the attack scenario  $S_1$  is the most likely happened attack method, so to protect the system from attack, it is necessary to first keep close eyes on it and take correspondent location protection measures.

## 2.5 Summary

Location privacy in VANETs is getting more concerns of the world. However, the study on the risk assessment of location privacy in the system has received less attention. In this chapter, we present an attack tree based security assessment methodology to quantify the risk of location privacy in VANETs from the systems perspective. We further build an attack tree with the leakage of location privacy information as attack goal. Also the total possibility of reaching attack goal is calculated on the basis of the attack tree. At last, according to the attack scenario analysis, we find out the most likely path that an attacker may use. In the next chapter, we will introduce an attack-defense tree method for VANETs security and privacy assessment, by which the system's defense strategies can be analyzed.





<http://www.springer.com/978-1-4614-9356-3>

Security Assessment in Vehicular Networks

Du, S.; Zhu, H.

2013, XI, 49 p. 9 illus., Softcover

ISBN: 978-1-4614-9356-3