Peer-to-Peer Netw. Appl. (2014) 7:215–228
DOI 10.1007/s12083-012-0127-9

An attack-and-defence game for security assessment in vehicular ad hoc networks

Suguo Du · Xiaolong Li · Junbo Du · Haojin Zhu

Received: 21 December 2011 / Accepted: 13 February 2012 / Published online: 8 March 2012

Abstract Recently, there is an increasing interest in Security and Privacy issues in Vehicular ad hoc networks (or VANETs). However, the existing security solutions mainly focus on the preventive solutions while lack a comprehensive security analysis. The existing risk analysis solutions may not work well to evaluate the security threats in vehicular networks since they fail to consider the attack and defense costs and gains, and thus cannot appropriately model the mutual interaction between the attacker and defender. In this study, we consider both of the rational attacker and defender who decide whether to launch an attack or adopt a countermeasure based on its adversary's strategy to maximize its own attack and defense benefits. To achieve this goal, we firstly adopt the attack-defense tree to model the attacker's potential attack strategies and the defender's corresponding countermeasures. To take the attack and defense costs into consideration, we introduce *Return On Attack* and *Return on Investment* to represent the potential gain from launching an attack or adopting a countermeasure in vehicular networks. We further investigate the potential strategies of the defender and the attacker by modeling it as an attack-defense game. We then give a detailed analysis on its Nash Equilibrium. The rationality of the proposed game-theoretical model is well illustrated and demonstrated by extensive analysis in a detailed case study.

Keywords Attack tree · Game theory · Vehicular ad hoc networks · Security and privacy

S. Du · X. Li · J. Du · H. Zhu (✉)
Shanghai Jiao Tong University,
Shanghai, People's Republic of China
e-mail: zhu-hj@cs.sjtu.edu.cn

S. Du
e-mail: sgdu@sjtu.edu.cn

X. Li
e-mail: ymingchen_123@sjtu.edu.cn

J. Du
e-mail: djb1107@sjtu.edu.cn

1 Introduction

Vehicular ad hoc networks (or VANETs) are self-organized networks designed for communication among vehicles [1]. In VANETs, each vehicle is equipped with an On Board Unit, by which vehicles are able to communicate with each other as well as Road Side Units (or RSUs). VANETs are expected to support a wide range of promising applications such as location based services. For example, Internet access has become a part of our daily life and there is a growing demand for accessing the Internet or information centers from vehicles. In VANETs, the RSUs can be deployed every few miles along the highway for users to download maps, traffic data and multimedia files. Vehicles can use RSUs to report real time traffic information and request location-based services such as finding restaurants, gas stations, or available parking space [2]. Therefore, as a typical application of Machine-to-Machine (M2M) communications, VANETs are expected to play an important role in the real Market of M2M communications.

In the past several years, there are quite a few studies on how to realize efficient data routing/forwarding in

vehicular networks [3]. However, vehicular networks have brought new security challenges due to their mobile and infrastructure-less nature. For example, 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, which is referred to as privacy related threats. Further, a malicious vehicle could impersonate an legitimate user to disseminate bogus traffic information, which may mislead other vehicles and compromise the normal functionality of VANETs. Therefore, VANETs security and privacy is regarded as one of major challenges for vehicular communications.

The existing research on VANETs security and privacy mainly focuses on the preventive techniques. From a system point of view, it lacks a comprehensive yet well-defined security evaluation to allow the system administrator to identify the most critical security threats and thus determine the appropriate defense strategy, which are more than important for the overall success of VANETs deployment. The existing risk analysis schemes include attack tree, attack graph or defense tree based solutions. However, there are serval research challenges which make the existing security analysis solutions cannot work well for security and privacy evaluation in VANETs. Firstly, for VANETs security, the defense strategy is directly correlated to the attack strategy and vice versa, which means that the security evaluation should consider both of attack and the defense side rather than any single one. Secondly, most of the existing security solutions only consider how to prevent an attack while fail to consider the costs and gains of the attacker and the defender. In reality, a rational attacker or defender may try to maximize its attack or defense benefits in stead of blindly launching an attack or adopting a countermeasure. Lastly, but no less importantly, how to model the mutual interaction between the attacker and defender remains a great challenge for VANETs security evaluation.

In contrast with the existing approaches, we consider both of the rational attacker and defender which decide whether to launch an attack or adopt a countermeasure based on its adversary's strategy to maximize its own attack and defense benefits. To achieve this goal, we firstly adopt the attack-defense tree to model the attacker's potential attack strategy and the defender's corresponding countermeasure. To take the attack and defense cost into consideration, we introduces two novel concepts: *Return On Attack (ROA)* and *Return on Investment (ROI)* to represent the potential gain from launching an attack or adopting a countermeasure. We further investigate the potential strategies of the defender and the attacker by using a game-theoretic analysis. In the newly defined attack-defense game, each rational participant may tend to get the maximum utility by maximizing ROI or ROA, which depends on the different utility attack/defense strategy and the associated attack/defense cost.

To the best of our knowledge, this paper is the first to consider the attack/defense cost in the game-theoretic analysis of the attack-defense tree. The contributions of this work are summarized as follows:

- We adopt the attack-defense tree based risk analysis model to describe the potential attack/defense strategy of the attacker and the defender. The built attack-defense tree gives a comprehensive review on the reported security solutions.
- We introduce ROA and ROI to evaluate the gains of the attacker and the defender from an attack and the corresponding countermeasure.
- We introduce a novel attack-defense game to model the interact between the attacker and the defender, both of which may try to maximize its benefit. We model the attack-defense game as a static game and give a detailed analysis on its Nash Equilibrium.
- The proposed attack-defense game is well demonstrated and illustrated by the detailed analysis in the case study.

This paper is organized as follows. The attack-defense tree model for VANETs security analysis is given in Section 2. In Section 3, a novel attack-defense game between the attacker and the defender is introduced and the Nash Equilibrium is analyzed. In Section 4, the case study is given to demonstrate and illustrate the attack-defense game. We conclude this paper in Section 5.

2 Related work

VANETs security and privacy is gaining an increased interest from both of industry and academia. In this study, we mainly focus on how to protect the messages from being modified and how to preserve users' location privacy.

False message injection from outsider attacker is one of major security threats in VANETs. To provide the authentication and integrity checking for the broadcasted message, IEEE 1609.2 standard has proposed to have a Public Key Infrastructure (PKI) for key management. Each vehicle has a pair of ECDSA keys: a

private signing key and a public verification key. The verification key is certified by a certificate authority (CA). Each sent message will append a signed signature to provide message authentication, which could prevent the outsider attackers from injecting bogus messages [4].

However, the insider false message injection attacker cannot directly be addressed by the public key based solutions since the attackers could compromise a legitimate user and then exploit its private key to launch the attacks. To address the insider false message injection attack, there are two problems need to be addressed: how to detect a false message sent by a legitimate identity and how to revoke this legitimate but misbehaving node. For the first problem, one of the potential approaching is local voting approach which allows multiple vehicles to cross check a target message in VANETs [5]. For the second problem, VANETs could revoke a misbehaving node by revoking its public/private key pairs. That is, revocation decision making may be the result of a collaborative, systemic or a unilateral decision process [6]. In collaborative schemes, nodes accuse other nodes of misbehaving by casting negative votes against them. If a predetermined threshold of negative votes are cast, then the offending node is considered revoked [7–10]. By contrast, systemic revocation decision could be made by contacting a centralized CA. In the unilateral decision process, a notion of suicide has recently been extended for use in ad hoc networks where a node, upon detecting some malicious behavior, can instigate a suicide-bombing on a (perceived) malicious node. A node commits suicide by broadcasting a signed instruction to revoke both its own key and the key of the misbehaving node [11–15].

To protect privacy and prevent location tracking, a VANETs-enabled vehicle can obtain multiple certified key pairs with non-overlapping periods of validity and change its public key periodically (e.g., every five minutes) [16]. Note that the attacker could also launch the privacy related attack by tracking the long-term identifiers, such as MAC (Medium Access Control) addresses, IP address, or physical layer information. Therefore, the corresponding pseudonyms on different layers could be used to enhance the location privacy. To avoid the spatial-temporal correlation, the mixzone based approach is introduced to enhance the location preserving by using the collaboration of multiple users. In addition, group signature based approach is another way to improve the location privacy [17].

In summary, there are quite a few threats and the corresponding protection solutions proposed for VANETs. In the next section, we will give a more detailed threat analysis by using an attack-defense tree based model.

3 Attack-defense tree model For VANETs security

3.1 System model

Communications in VANETs are divided into two parts: vehicle to infrastructure and vehicle to vehicle. The followings are some assumptions about the network [7]:

- Each vehicle has its own communication equipment OBU (On Board Unit), which enables the vehicles to communicate with others as well as the Road Side Units (RSUs).
- It is assumed that there is a trusted third party called Certificate Authority, like transportation authority within the network to take charge of the network's security and privacy issues. Each vehicle becomes a legitimate node of the network until it registers at CA.
- The CA disseminates each node with a single identity as well as a set of pseudonyms after it verified the validity of the node's identity.
- A node changes its pseudonym at certain intervals for the privacy preservation. Expired pseudonym is directly removed from the vehicle's storage media and CA is responsible for the issuance of new pseudonyms if a node uses up all of its predownload pseudonyms.
- Each node automatically broadcasts its location, velocity and other special information to its neighbors at fixed intervals.
- Vehicles have enough power to install and run personal firewall or other antivirus software to protect it from malicious programs like worms and viruses spread among wireless network.

3.2 Modeling the attack-defense tree for securing vehicular networks

3.2.1 Introduction to attack-defence tree model

In this paper, we adopt attack tree approach to model the behavior of the attackers in VANETs system and the effect of exploits. In general, attack trees offer a goal-oriented perspective that facilitates the expression of multi-stage attacks [14]. Attack trees in their simplest form assert subgoals for achieving the goal set forth by an attack node. Attack nodes can be grouped into AND or OR sequences to capture conjunctive and disjunctive attack conditions, respectively. Nodes can be weighted to reflect the likelihood of successfully mounting an

attack. We further propose to utilize the the attack-defense tree model to express the potential countermeasures which could be used to mitigate the system. The difference between an attack tree and an attack-defense tree is that the front only represents the attack strategies that attackers can launch, while the latter includes the set of countermeasures which can mitigate the possible damages produced by the attackers [18].

Figure 1 illustrates the structure of an attack-defense tree. There are two parts in an attack-defense tree. The square nodes represent the attack goals or actions which form the attack-tree part; the circle nodes represent the corresponding countermeasures of each attack goal or action. The top of the attack tree is associated with the asset of the system under consideration, which represents the attacker's final objective. The atomic attack (or leaf node) in the attack tree can lead the attacker to (partially) damage the asset by exploiting a single vulnerability. The sub-goal nodes (or Non-leaf nodes)can be of two different types under two kinds of gates: or-nodes (under or-gates) and and-nodes (under and-gates). Sub-goals associated with or-nodes are achieved as long as any of its child nodes is achieved, while and-nodes represent the sub-goals which require all of its child nodes to be completed.

3.2.2 Building attack-defense tree for VANETs security

In this section we will build the attack-defense tree model for VANETs security. In VANETs system, we set *Compromise the Security or Privacy* of VANETs as attack tree root, which is denoted as A. Two sub-goals of A are *Compromise Communication Security* and *Compromise Location Privacy*, which are denoted as AS and AP, respectively. In other words, an attacker could achieve the attack objective A by compromising the communication security (or the left sub-goal) or location privacy of the vehicles (or the right sub-goal). The attack-defense tree for VANETs security and privacy is shown in Fig. 2.

In the left sub-tree, there are three possible ways to achieve sub-goal AS, *Outsider False Data Injection* (AS_1), *Insider False Data Injection* (AS_2) and *Denial of Service* (AS_3). To achieve AS_1, the attacker must take two actions: to impersonate a legitimate vehicle(*Masquerad- ing*) denoted by AS_{11} and to disseminate *Bogus Information* denoted by AS_{12} (e.g., misleading traffic information). The countermeasure corresponding to this attack is *PKI & Signature* (C_1), which means that the security authority could prevent the outsider attackers from distributing unauthorized messages by requiring each vehicle to provide the public key signature for each sending message. Similarly, to obtain the sub-goal "insider false data injection (AS_2)", it is necessary for the attacker to perform two attack steps *Stealing Identity* (AS_{21}) and *Bogus Information* (AS_{22}), in which an attacker could compromise a legitimate node's secret key and disseminate the unauthentic information by using the compromised secret key. To thwart insider attack AS_2, the security authority could cross check the information under the collaboration of multiple nodes and revoke the public key of a misbehaving vehicle. Therefore, these defense strategies compose the countermeasures of *Cross Check* (C_2), *Cooperation* (C_3) and *Revocation* (C_4). Further, the *Denial of Service Attack* (AS_3) could be achieved by *Channel Jamming* (AS_{31}), which cannot be easily addressed in a cost-effective way.

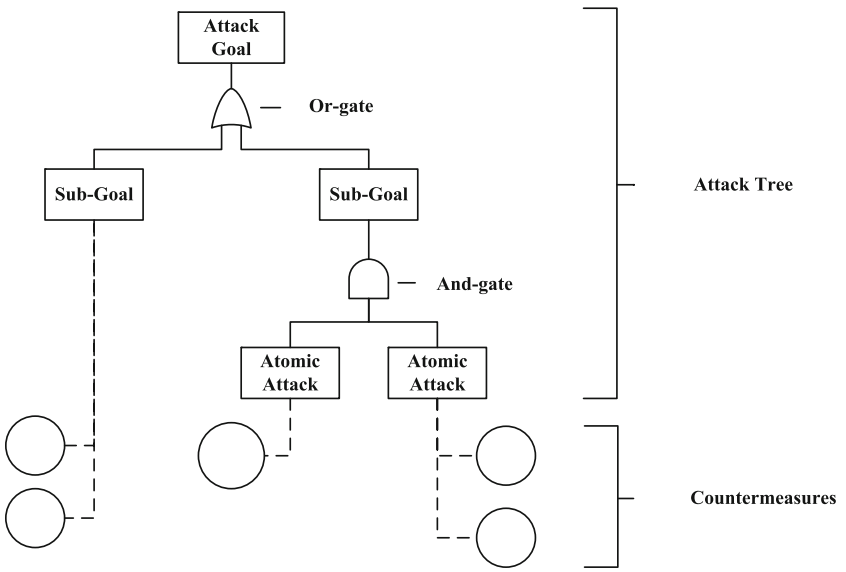


Fig. 1 An example of attack-defense tree

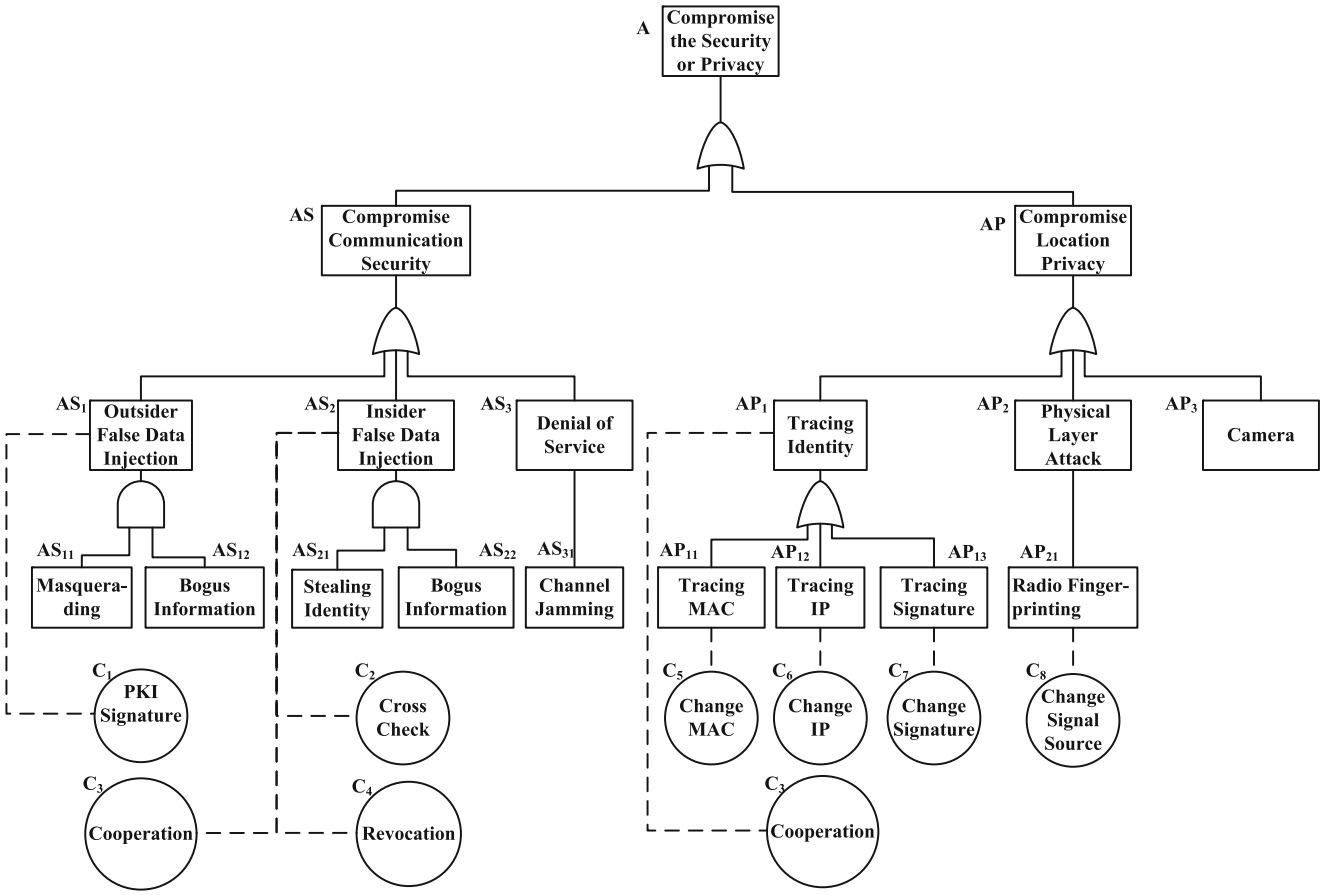


Fig. 2 The attack-defense tree model for VANETs security and privacy

In the right sub-tree, there are also three possible ways to achieve sub-goal *AP*, *Tracing Identity* (AP_1), *Physical Layer Attack* (AP_2) and *Camera* (AP_3). To achieve AP_1, the attacker may select one of three actions: *Tracing MAC* (AP_{11}), *Tracing IP* (AP_{12}) and *Tracing Signature* (AP_{13}). The corresponding countermeasures for the defender are *Change MAC* (C_5), *Change IP* (C_6) and *Change Signature* (C_7), respectively. Another countermeasure corresponding to AP_1 is *Cooperation* (C_3), with which C_5, C_6 or C_7 are more effective. To achieve the physical attack AP_2, the attack must use *Radio Fingerprinting* (AP_{21}). *Change Signal Source* (C_8) such as radio transmitters that randomize fingerprints is a countermeasure to AP_{21}. In addition, the *Camera* (AP_3) is a thorny attack so that there is no countermeasure to mitigate AP_3 effectively.

3.2.3 Introduction of ROI and ROA for attack-defense tree

In this work, we consider economic factors in VANETs security analysis by introducing Return on Investment (ROI) and Return on Attack (ROA). In the attack-defense tree, there are two types of costs: cost of attack and security investment cost [18]. We firstly define *Return on Investment* for the countermeasures of defenders. In particular, ROI is introduced to measure the return that a defender expects from a security or privacy investment over the costs he sustains for countermeasures. It is defined as follows:

$$ROI = \frac{ALE \times RM - CI}{CI} \tag{1}$$

where ALE denotes the *Annual Expected Loss* caused by VANETs security threat; RM represents the *Risk Mitigation* induced by the countermeasure; CI denotes the *Cost of Investment* which defines the cost that the defender pays for implementing a given countermeasure.

If we use $R_D = ALE/CI$ to denote the gain-cost ratio for defenders, the ROI in Eq. 1 can be expressed by R_D and RM as follows:

$$ROI = R_D \times RM - 1 \tag{2}$$

We will give more analysis on different alternatives of ROI with the change of R_D and RM in case

Table 1 Evaluation of ROI

Attack	ALE	Countermeasures	RM	CI	ROI
AS_1	4	C_1	1	2	1
		$C_2, \cdots, C_8$	0	–	−1
AS_2	10	C_2	0.25	4	−0.375
		C_3	0.5	8	−0.375
		C_4	0.25	4	−0.375
		$C_1, C_5, \cdots, C_8$	0	–	−1
AS_3	8	$C_1, \cdots, C_8$	0	–	−1
AP_{11}	4	C_3	0.75	8	−0.625
		C_5	0.25	4	−0.75
		$C_1, C_2, C_4, C_6, C_7, C_8$	0	–	−1
AP_{12}	4	C_3	0.75	8	−0.625
		C_6	0.25	4	−0.75
		$C_1, C_2, C_4, C_5, C_7, C_8$	0	–	−1
AP_{13}	4	C_3	0.75	8	−0.625
		C_7	0.25	4	−0.75
		C_1,C_2,C_4, C_5, C_6, C_8	0	–	−1
AP_2	6	C_8	1	6	0
		$C_1, \cdots, C_7$	0	–	−1
AP_3	8	$C_1, \cdots, C_8$	0	–	−1

study section. We further define the *Return On Attack* (ROA), which is used to measure the gain that an attacker expects from a successful attack over the losses that he sustains due to the adoption of security or privacy measures by his target. ROA is defined as follows:

$$ROA = \frac{GI \times (1 - RM) - (Cost_A + Cost_{AC})}{Cost_A + Cost_{AC}} \tag{3}$$

where GI represents the expected gain from a successful attack on the specified target; $Cost_A$ is the cost sustained by the attacker to launch an attack, and $Cost_{AC}$ represents the additional cost brought by the countermeasure C adopted by the defender to mitigate the attack.

Similar with the definition of R_D, we let $R_A = GI/(Cost_A + Cost_{AC})$ denote the gain-cost ratio for attackers. Consequently ROA in Eq. 3 is reduced as follows:

$$ROA = R_A \times (1 - RM) - 1 \tag{4}$$

Since ROA is a function of R_A and RM, we will discuss the different impacts on ROA caused by R_A and RM in later case study section.

From the definitions of ROI and ROA, the values of them are relative and they represent the return of the

Table 2 Evaluation of ROA

Attack	GI	$Cost_a$	Countermeasures	$Cost_{ac}$	ROA
AS_1	4	4	C_1	0	−1
			$C_2, \cdots, C_8$	0	0
AS_2	4	10	C_2	4	−0.786
			C_3	8	−0.889
			C_4	4	−0.786
			$C_1, C_5, \cdots, C_8$	0	−0.6
AS_3	2	6	$C_1, \cdots, C_8$	0	−0.667
AP_{11}	6	4	C_3	8	−0.875
			C_5	6	−0.55
			$C_1, C_2, C_4, C_6, C_7, C_8$	0	0.5
AP_{12}	6	4	C_3	8	−0.875
			C_6	6	−0.55
			$C_1, C_2, C_4, C_5, C_7, C_8$	0	0.5
AP_{13}	6	4	C_3	8	−0.875
			C_7	6	−0.55
			$C_1, C_2, C_4, C_5, C_6, C_8$	0	0.5
AP_2	8	6	C_8	0	−1
			$C_1, \cdots, C_7$	0	0.333
AP_3	8	10	$C_1, \cdots, C_8$	0	−0.2

costs. In our case, according to the attack-defense tree and the possible difficulties of acting countermeasures and attacks, we use a set of levels 0, 2, 4, 6, 8, 10 as the specific values of ALE, CI, GI, $Cost_A$ and $Cost_{AC}$, by which obtaining the final values of the gain and cost is possible. Since RM is a risk measurement, we will choose 0, 0.25, 0.5, 0.75, 1 as the specific values of RM to represent the effectiveness of each countermeasure. A higher value of RM indicates a more effective countermeasure. Thus, we can evaluate the ROI and ROA for all the countermeasures according to the data in Tables 1 and 2 respectively [19].

In Table 1, it should be noticed that the reason of choosing the subgoals AS_1, AS_2 instead of atomic attacks AS_{11}, AS_{12}, AS_{21}, AS_{22} for attackers in the Attack column which is related to the logical gate type of the attack subgoals. Due to the 'AND' logical type of AS_1, AS_2 shown in Fig. 2, the attacker won't achieve any gain by only taking one single attack of AS_{11}, AS_{12}, AS_{21}, AS_{22}.

In the RM column, zero values indicate that the countermeasure cannot mitigate the attack. For example, countermeasure $C_2, \ldots, C_8$ cannot mitigate attack AS_1, the corresponding RM is 0. The dash "–" in the column of CI means that the CI of the countermeasure do not impact the result of the corresponding ROI in Table 1. In addition, when a countermeasure cannot mitigate an attack ($RM = 0$), in this case, $ROI = -1$ in Table 1 and $ROA = (GI - Cost_A)/Cost_A$ in Table 2.

From the above, we can obtain the values of ROI and ROA between each pair of countermeasure and attack, which constitute the utility matrix for the attack-defense game in the next section.

4 A VANETs attack-defense game

In the previous section, we have introduced *Return on Attack (ROA)* to measure the effectiveness of attacks in terms of attack cost and *Return on Investment (ROI)* to evaluate the investment on a security countermeasure with regard to a specific attack. On one side the VANETs security administrator wants to protect the security of the vehicular networks by adopting countermeasures to thwart the attacks; on the other side, the attacker wants to exploit the vulnerabilities and obtain some profit by attacking the vehicular networks. By using ROI and ROA to represent the utility of the defender and the attacker, both of the defender and the attacker may tend to get the maximum utility by maximizing ROI or ROA, respectively. However, they cannot maximum their utility at the same time because one's action that aims to increase its own benefits will reduce its adversary's utility. Therefore, in this paper, we investigate the possible strategies of the security administrator and of the attacker by using a game-theoretic analysis. We consider rational participants that maximize their payoff function, which depends on the different utility attack/defense strategy and the associated attack/defense cost [20].

4.1 Game model

In this section we analyze the possible strategies of the system defender and of the attacker by using an attack-defense game model for VANETs security and privacy. Game theory allows modeling situations of conflict and, hence, predicting the behavior of the participants. We model the attack-defense game as a *static game* in which each participant take action when another's action is unknown. It is reasonable since in our VANETs security attack-defense system, both defender and attacker don't know each other's strategies when they take actions. We also suppose that the participants are rational in our model. This model assumption keeps our analysis tractable while solving the Nash Equilibrium solution of the game. The game $\mathcal{G}$ is defined as a triplet $(\mathcal{O}; \mathcal{S}; \mathcal{U})$, where $\mathcal{O}$ is a set of players, $\mathcal{S}$ is a set of strategies and $\mathcal{U}$ is a set of payoff functions.

- **Players**: The set of $\mathcal{O} = \{O_i\}$ includes a defender O_1 and an attacker O_2, referring to Def and Att respectively. Each player has no idea about which action his adversary has chosen (e.g., as soon as the attacker has decided to perform the insider false data injection (AS_2), the defender can't receive any information about it so that the game is static.).
- **Strategy**: Each player has a set of strategies $S_k (k = 1, 2:$ all countermeasures $C_i \in S_1$ and all attacks $A_j \in S_2$). According to our attack-defense tree model for VANETs security and privacy, the countermeasures which the defender can select are $\{C_i | i = 1, ..., 8\}$; the attacks which the attacker can select are $\{A_j | j = 1, ..., 8\}$, or $\{AS_1, AS_2, AS_3, AP_{11}, AP_{12}, AP_{13}, AP_2, AP_3\}$ respectively.
- **Payoff function**: The utility functions(or payoff) are defined as: $u_1(C_i, A_j) = ROI(C_i, A_j); u_2(C_i, A_j) = ROA(C_i, A_j)$.

We show the utility matrix of the attack-defense game in Table 3. We suppose the players know the utility (payoff) functions with each other completely, thus our game is a *complete information game*. It is noticed that knowing the adversary's utility doesn't give a clue to the adversary's action strategies. For example, the defender knows that the cost or the gain to launch an location privacy related attack. However, he has no

Table 3 The utility matrix of attack-defense game

	Attack		
Defense	A_1	$\cdots$	A_8
C_1	$ROI(C_1, A_1), ROA(C_1, A_1)$	$\cdots$	$ROI(C_1, A_8), ROA(C_1, A_8)$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
C_8	$ROI(C_8, A_1), ROA(C_8, A_1)$	$\cdots$	$ROI(C_8, A_8), ROA(C_8, A_8)$

idea about which specific attack action (e.g., tracing the identity, physical layer tracing, or even use camera) will be adopted by the attacker.

4.2 Equilibrium concepts

In this section, we introduce a few game-theoretic concepts that will help us get an insight into the strategies of participants. In our complete information attack-defense game, a *pure strategy* for player k is (C_m, A_n), $C_m \in S_1$ and $A_n \in S_2$, which means that under certain conditions the strategies of the attacker and of the defender converges to a pair of best action profile. This is to say that the defender cannot do better by choosing an action different from C_m, given that the attacker adopt A_n, and vice versa. In this case we say that our attack-defense game admits a Nash Equilibrium.

Definition 1 (Nash Equilibrium under pure strategy) In the attack-defense game, the combination of strategy (C_m, A_n) with $C_m \in S_1$ and $A_n \in S_2$ is a Nash Equilibrium if and only if, for each player k, the action C_m or A_n is the best response to the other player:

$$u_1(C_m, A_n) \geq u_1(C_i, A_n) \ \ for\ any\ C_i \in S_1$$

$$u_2(C_m, A_n) \geq u_2(C_m, A_j) \ \ for\ any\ A_j \in S_2$$

However, in the VANETs system, the pure strategies seldom happens since (C_m, A_n) means that the defender selects C_m as the only countermeasure and the attacker selects A_n as the only attack in the attack-defense game. Both sides of players wouldn't take this strategy in a long-term process in the VANETs security and privacy system. In a word, both defender and attacker will select actions with a certain probability distribution which compose a mixed strategy. The below is the definition of a mixed strategy.

Definition 2 A **mixed strategy** for the attack-defense game is a strategy of selecting countermeasures with a probability distribution $P_1 = (P_{C_1}, \cdots, P_{C_8})$, where $0 \leq P_{C_i}$ and $\sum_{i=1}^{8} P_{C_i} = 1$ for defenders or $P_2 = (P_{A_1}, \cdots, P_{A_8})$, where $0 \leq P_{A_j}$ and $\sum_{i=1}^{8} P_{A_i} = 1$ for attackers. If player Def believes that player Att will play the strategies S_2 with probability $P_2 = (P_{A_1}, \cdots, P_{A_8})$, the expected payoff for player Def obtained with the pure strategy C_i is:

$$\sum_{j=1}^{8} P_{A_j} ROI(C_i, A_j)$$

If player Att believes that player Def will play the strategies S_1 with probability $P_1 = (P_{C_1}, \cdots, P_{C_8})$, the expected payoff for player Att obtained with the pure strategy A_j is:

$$\sum_{i=1}^{8} P_{C_i} ROA(C_i, A_j)$$

Definition 3 (Nash Equilibrium under mixed strategies) If the players Def and Att play respectively the strategies S_{P_1} with probability $P_1 = (P_{C_1}, \cdots, P_{C_8})$, and S_{P_2} with probability $P_2 = (P_{A_1}, \cdots, P_{A_8})$, the expected payoffs for the players are computed as follows:

$$u_1(S_{P_1}, S_{P_2}) = \sum_{i=1}^{8} \sum_{j=1}^{8} P_{C_i} P_{A_j} ROI(C_i, A_j)$$

$$u_2(S_{P_1}, S_{P_2}) = \sum_{i=1}^{8} \sum_{j=1}^{8} P_{C_i} P_{A_j} ROA(C_i, A_j)$$

The mixed strategy $(S_{P_1^*}, S_{P_2^*})$ is a Nash Equilibrium only if the mixed strategy for each player is the best response to the mixed strategy of the other player:

$$u_1(S_{P_1^*}, S_{P_2^*}) \geq u_1(S_{P_1}, S_{P_2^*}) \ \ for\ any\ S_{P_1}$$

$$u_2(S_{P_1^*}, S_{P_2^*}) \geq u_2(S_{P_1^*}, S_{P_2}) \ \ for\ any\ S_{P_2}$$

From the above two definitions, we can achieve the conditions of the Nash Equilibrium of mixed strategy $(S_{P_1^*}, S_{P_2^*})$:

$$\max \sum_{i=1}^{8} \sum_{j=1}^{8} P_{C_i} P_{A_j}^* ROI(C_i, A_j)$$

$$= \sum_{i=1}^{8} \sum_{j=1}^{8} P_{C_i}^* P_{A_j}^* ROI(C_i, A_j) \quad (5)$$

$$\max \sum_{i=1}^{8}\sum_{j=1}^{8} P^*_{C_i} P_{A_j} ROA(C_i, A_j)$$

$$= \sum_{i=1}^{8}\sum_{j=1}^{8} P^*_{C_i} P^*_{A_j} ROA(C_i, A_j) \quad (6)$$

where $P^*_{C_i} \in P^*_1, i = 1, 2, \cdots, 8$; $P^*_{A_j} \in P^*_2$, $j = 1, 2, \cdots, 8$. However, it is a challenge to obtain the probabilities of the countermeasure and attack actions. This is because that we have to solve two groups of unknown probabilities by optimizing two payoff functions at the same time. To address this issue, based on the assumption that every participant is rational, we conclude the following Theorem 1, which provides a simplified solution to obtain the probabilities of countermeasure and the attack actions.

Theorem 1 *If $(S_{P^*_1}, S_{P^*_2})$ is the Nash Equilibrium of mixed strategies for the attack-defense game; p denotes the number of countermeasures ($C_{i_k}, k = 1, ..., p$) taken by the defender with non-zero probabilities; q denotes the number of attacks ($A_{j_k}, k = 1, ..., q$) launched by attacker with non-zero probabilities, then for any countermeasure C_{i_k} with probability $P_{C_{i_k}}$, the expected payoff of all attacks ($u_{A_{j_k}}, k = 1, ..., q$) are equivalent for the attacker, vice versa.*

$$\sum_{k=1}^{p} P_{C_{i_k}} ROA(C_{i_k}, A_{j_1}) = \sum_{k=1}^{p} P_{C_{i_k}} ROA(C_{i_k}, A_{j_2})$$

$$= \cdots = \sum_{k=1}^{p} P_{C_{i_k}} ROA(C_{i_k}, A_{j_q}) \quad (7)$$

$$\sum_{k=1}^{q} P_{A_{j_k}} ROI(C_{i_1}, A_{j_k}) = \sum_{k=1}^{q} P_{A_{j_k}} ROI(C_{i_2}, A_{j_k})$$

$$= \cdots = \sum_{k=1}^{q} P_{A_{j_k}} ROI(C_{i_p}, A_{j_k}) \quad (8)$$

Proof

Case I Without loss of generality, we assume that the expected payoff $u_{A_{j_1}} = \sum_{k=1}^{p} P_{C_{i_k}} ROA(C_{i_k}, A_{j_1})$ is less than the other expected payoffs in the attack-defense game. It indicates that with the probability of P^*_1 the expected payoff of A_{j_1} is lower than that of other attack actions. Therefore, the attacker will not select A_{j_1} at all which leads $P_{A_{j_1}} = 0$. This is contradictive with the assumption of $P_{A_{j_1}}$ greater than 0.

Case II Without loss of generality, we assume that $u_{A_{j_1}}$ is greater than the other expected payoffs in the attack-defense game. It means that with the countermeasures' probabilities of P^*_1 the expected payoff of A_{j_1} is higher than that of other attack actions. Therefore the attacker must select only A_{j_1} which leads $P_{A_j} = 1$. Under this condition, the defender must choose countermeasures with the max ROI related to A_{j_1} while set the probabilities of the other countermeasures as zero. This is contradictive with the assumption of p non-zero probabilities of countermeasures. □

We can achieve the Nash Equilibrium of mixed strategy from Theorem 1. However, the previous conclusion cannot reflect the impact of the cost and gain change of different actions on the chosen strategies of the participants (or Nash Equilibrium in the Attack-Defense Game). This is especially important for VANETs, which are typically a dynamic network with the frequently changed network architecture. Thus, a specific action may lead to a different cost as well as the gain under different environment setting. In the follows, we take the malicious node revocation as an example to show the change of costs and gains in different cases.

- **Case 1: A Low Defense Cost with A High Defense Gain** In the case of presence of the network infrastructure (e.g., Road Side Unit), a node could easily revoke a malicious node by contacting the security authority via vehicle to RSU communications and the security authority could broadcast a revocation message within the whole network to revoke the target malicious node, which incurs a low defense cost and high defense gain.
- **Case 2: A Moderate Defense Cost with A Moderate Defense Gain** In a case of of no infrastructure but the presence of sufficient number of legitimate user, the different vehicles could collaborate to revoke a malicious node, which leads a moderate defense cost (e.g., transmission of coordinate messages among the different collaborative nodes) as well as a moderate defense gain (e.g., local revocation of this malicious node rather than global revocation) with a certain successful rate (e.g., revocation failure if no enough voting numbers).
- **Case 3: A High Defense Cost with A Low Defense Gain** In a case of even no enough collaboration nodes, a legitimate user can still revoke a node by launching a suicide revocation, which incurs a high defense cost (e.g., also revoking its own public/private key) with a low defense gain (e.g., a

limited number of transmission range of revocation message in a sparse network).

From the above example, it is obvious that the cost and gain of the defense could have a significant change in different scenarios, which has a direct impact on the strategy choosing of the attacker and the defense. In the follows, we use Theorem 2 to model the impact of the change of the gains and the costs on the Nash Equilibrium.

Theorem 2 *If the gain or the cost incurred by a specific attack takes change and this change leads to an increased utility of the attacker (e.g., a higher R_A or lower RM), the defender will perform the countermeasures corresponding to this attack with a higher probability. Conversely, if the gain or the cost incurred by a specific countermeasure takes change and this change leads to an increased utility of the defender (e.g., a higher R_D or higher RM), the attacker will perform the attacks regarding to this countermeasure with a lower probability.*

Proof Without loss of generality, we suppose for a specific attack A_{j_1}, $C_{i_k}(k = 1, \cdots, r)$ are the countermeasures which can mitigate A_{j_1}; $C_{i_k}(k = r+1, \cdots, p)$ are the countermeasures which cannot mitigate A_{j_1}. For $C_{i_k}(k = r+1, \cdots, p)$, their $ROA(C_{i_k}, A_{j_1})$s are equivalent, denoted by $ROA(A_{j_1})$ and we conclude that $ROA(A_{j_1})$ is greater than any $ROA(C_{i_k}, A_{j_1})(k = 1, \cdots, r)$ from the Eq. 3. The expected payoff of A_{j_1} is:

$$u_{A_{j_1}} = \sum_{k=1}^{r} P_{C_{i_k}} ROA(C_{i_k}, A_{j_1}) + \sum_{k=r+1}^{p} P_{C_{i_k}} ROA(A_{j_1})$$

$$= ROA(A_{j_1}) + \sum_{k=1}^{r} P_{C_{i_k}} [ROA(C_{i_k}, A_{j_1}) - ROA(A_{j_1})]$$

If $R_{A_{j_1}}$ is increased(or RM is decreased), consequently $u_{A_{j_1}}$ will be increased. To keep the Eq. 7 in Theorem 1, the defender has to increase $P_{C_{i_k}}(k = 1, \cdots, r)$.

We also suppose for a specific countermeasure C_{i_1}, $A_{j_k}(k = 1, \cdots, r)$ are the attacks which can be mitigated by C_{i_1}; $A_{j_k}(k = r+1, \cdots, q)$ are the attacks which cannot be mitigated by C_{i_1}. For $A_{j_k}(k = r+1, \cdots, q)$, their $ROI(C_{i_1}, A_{j_k})$s are equivalent to -1, and we conclude that -1 is great than any $ROI(C_{i_1}, A_{j_k})(k = 1, \cdots, r)$ from the Eq. 1. The expected payoff of C_{i_1} is:

$$u_{C_{i_1}} = \sum_{k=1}^{r} P_{A_{j_k}} ROI(C_{i_1}, A_{j_k}) + \sum_{k=r+1}^{q} P_{A_{j_k}} (-1)$$

$$= \sum_{k=1}^{r} P_{A_{j_k}} [ROI(C_{i_1}, A_{j_k}) + 1] - 1$$

If $R_{D_{i_1}}$ is increased(or RM is increased), consequently $u_{C_{i_1}}$ will be increased. To keep the Eq. 8 in Theorem 1, the attacker has to decrease $P_{A_{j_k}}(k = 1, \cdots, r)$. □

Theorem 2 shows that in the attack-defense game, if the attacker can get more payoffs from an attack or use this attack more easily than other, the defender must choose the countermeasures related to this attack with a higher priority to avoid the failure of the defense; if the defender can effectively mitigate an attack, the attacker must decrease the possibility of launching this attack, or even give up using this attack.

5 Security analysis of attack-defense game: a case study

In this section, we investigate an attack-defense game to illustrate the Theorems 1 and 2 by using the specific attack-defense tree for VANETs security and privacy presented in Section 2. For this specific case study, the detailed payoff values of attacker and defender are given in Table 4. In particular, Tables 1 and 2 summarize all the factors to calculate the payoff of defender (ROI) and payoff of attacker (ROA), respectively.

Table 4 The utility matrix of the attack-defense game

	AS_1	AS_2	AS_3	AP_{11}	AP_{12}	AP_{13}	AP_2	AP_3
C_1	1, −1	−1, −0.6	−1, −0.667	−1, 0.5	−1, 0.5	−1, 0.5	−1, 0.333	−1, −0.2
C_2	−1, 0	−0.375, −0.786	−1, −0.667	−1, 0.5	−1, 0.5	−1, 0.5	−1, 0.333	−1, −0.2
C_3	−1, 0	−0.375, −0.889	−1, −0.667	−0.625, −0.875	−0.625, −0.875	−0.625, −0.875	−1, 0.333	−1, −0.2
C_4	−1, 0	−0.375, −0.786	−1, −0.667	−1, 0.5	−1, 0.5	−1, 0.5	−1, 0.333	−1, −0.2
C_5	−1, 0	−1, −0.6	−1, −0.667	−0.75, −0.55	−1, 0.5	−1, 0.5	−1, 0.333	−1, −0.2
C_6	−1, 0	−1, −0.6	−1, −0.667	−1, 0.5	−0.75, −0.55	−1, 0.5	−1, 0.333	−1, −0.2
C_7	−1, 0	−1, −0.6	−1, −0.667	−1, 0.5	−1, 0.5	−0.75, −0.55	−1, 0.333	−1, −0.2
C_8	−1, 0	−1, −0.6	−1, −0.667	−1, 0.5	−1, 0.5	−1, 0.5	0, −1	−1, −0.2

Table 5 Reduction of attack-defense game

	AS_1	AP_1	AP_2	AP_3
C_1	$1, -1$	$-1, 0.5$	$-1, 0.333$	$-1, -0.2$
C_3	$-1, 0$	$-0.625, -0.875$	$-1, 0.333$	$-1, -0.2$
C_8	$-1, 0$	$-1, 0.5$	$0, -1$	$-1, -0.2$

Before we solve the Nash Equilibrium of this Attack-defence game, it is useful to introduce the concept of *Dominated Strategy* to simplify the process of solving final solutions. A dominated strategy means that its'payoff is less than any other strategy's payoffs under the same strategy of the adversary in the attack-defense game.

From Table 4, we observe that the attacks of AS_2 or AS_3 are dominated strategies for attackers. The countermeasures of C_2, C_4, C_5, C_6 and C_7 are dominated strategies for defenders. The reduction solutions are shown in Table 5. This is a mixed strategy for both defender and attacker. The probabilities of choosing attacks of AS_2 or AS_3 are zeros for attackers. Similarly probabilities of choosing countermeasures of C_2, C_4, C_5, C_6 and C_7 are zeros for defenders. From Theorem 1, for any countermeasure i with probability P_{Ci}, the expected payoff of the attacker in any attack are equivalent, vice versa, we therefore get the equations as follows:

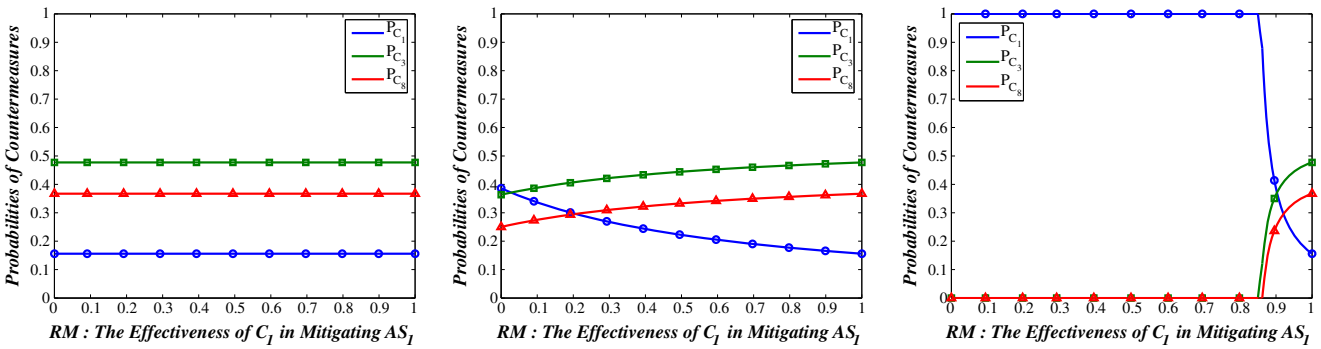
$$\begin{aligned}(-1)P_{C_1} &= 0.5(P_{C_1} + P_{C_8}) + (-0.875)P_{C_3} \\ &= 0.333(P_{C_1} + P_{C_3}) + (-1)P_{C_8}\end{aligned} \tag{9}$$

$$\begin{aligned}P_{AS_1} &+ (-1)(P_{AP_{11}} + P_{AP_{12}} + P_{AP_{13}} + P_{AP_2} + P_{AP_3}) \\ &= (-1)(P_{AS_1} + P_{AP_2} + P_{AP_3}) \\ &\quad + (-0.625)(P_{AP_{11}} + P_{AP_{12}} + P_{AP_{13}}) \\ &= (-1)(P_{AS_1} + P_{AP_{11}} + P_{AP_{12}} + P_{AP_{13}} + P_{AP_3})\end{aligned} \tag{10}$$

From above equations, we can obtain the two groups of probabilities of mixed strategies for the attacker and defender: $P_{AS_1} = 3/25$, $P_{AP_1} = 16/25$, $P_{AP_2} = 6/25$, $P_{AP_3} = 0$; and $P_{C_1} = 17/109$, $P_{C_3} = 52/109$, $P_{C_8} = 40/109$. Here, $P_{AP_3} = 0$ indicates that the attack AP_3 is also a dominated strategy for attackers. Until now we have obtained the Nash Equilibrium of this attack-defense game. That is for the attacker taking the attacks of AS_1, AP_1 and AP_2 with the probabilities of 3/25, 16/25 and 3/25 respectively; for the defender choosing the countermeasures of C_1, C_3, and C_8 with the probabilities of 17/109, 52/109 and 40/109 respectively.

According to the final Equilibrium results, we find that the defender will adopt the countermeasure C_3 with the highest probability of 52/109; the attacker will choose the attack AP_1 with the highest probability of 16/25. These solutions indicate that in our considered VANETs security scenario, the defender will cooperate with the other vehicles (countermeasure C_3) as far as possible to mitigate the attacks of tracing identity (AP_1, including AP_{11}, AP_{12} and AP_{13}), and vice versa. In fact, due to the high costs of stealing identity to utilize insider false data (AS_2) and using the camera to impinge privacy (AP_3), the attacker has to give up these two attacks in this attack-defense game (the probabilities of AS_2 and AP_3 are zeroes in the Nash Equilibrium).

Figure 3 illustrate how the attack gain-cost ratio (R_A)and effectiveness of defense strategies (RM) affect the result of Nash Equilibrium of mixed strategies. In case 1: $R_A = 0$ indicate that the attacker won't have any gain (or failure attack) by launching the specific attack AS_1. For example, a attacker may be malicious who seeks no personal benefits from the attacks but aims to disrupt the VANETs security. Since in our game, the utilities of both sides are known by each participant, the defender chooses a low probability ($P_{C_1} = 0.15$) of countermeasure C_1. Under this

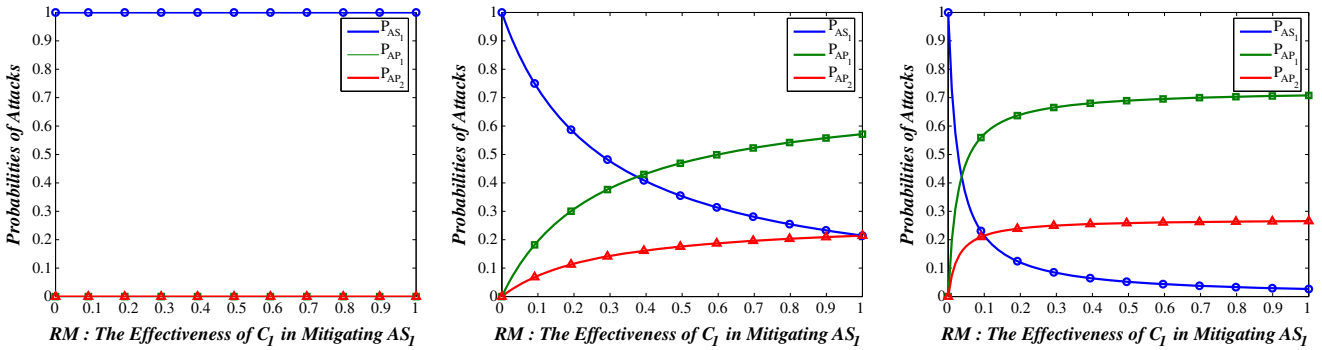


(a) Case 1 $R_A = 0$: A Low Attack Gain with A High Attack Cost

(b) Case 2 $R_A = 1$: The Attack Gain Equals Attack Cost

(c) Case 3 $R_A = 10$: A High Attack Gain with A Low Attack Cost

Fig. 3 Probabilities of countermeasures with the changes of R_A and RM of Nash equilibrium



(a) Case 1 $R_D = 0$: A Low Attack Gain with A High Attack Cost

(b) Case 2 $R_D = 1$: The Defense Gain Equals Defense Cost

(c) Case 3 $R_D = 10$: A High Attack Gain with A Low Attack Cost

Fig. 4 Probabilities of attacks with the changes of R_D and RM of Nash equilibrium

circumstance, the probabilities of countermeasures C_1, C_3 and C_8 keep no changing whatever RM is low or high. This is reasonable since this attack won't affect the security of VANETs system with $R_A = 0$.

In case 2: $R_A = 1$ means that the attacker increased his gain by launching the attack AS_1 comparing with that in case 1. Under this condition, the probability of countermeasure C_1 although is decreasing with the more effective countermeasure C_1 (RM increasing), it is increased ($P_{C_1} > 0.15$)comparing with that in case 1 when the attacker have no gain($P_{C_1} = 0.15$). This has shown the result of Theorem 2: a higher gain of attacker, a higher probability of corresponding countermeasure in Nash Equilibrium of mixed strategies.

In case 3: $R_A = 10$ means a high gain-cost ratio for the attacker. Under this condition the defender will choose countermeasure C_1 with probability of 1 as long as RM is less than 0.85. However as RM tends to 1 (i.e., countermeasure C_1 is 100% effective) the probability of C_1 decreases to 0.15. Due to the relationship of $P_{C_1} + P_{C_3} + P_{C_8} = 1$, the probabilities of countermeasures of C_3 and C_8 are zeros when RM is less than 0.85. Both of them increase when RM is greater than 0.85. This result explains that when the countermeasure C_1 is very effective (RM close to 1), the attacker will choose other attacks AP_1 or AP_2 with higher probabilities which lead the defender to choosing the corresponding countermeasures C_3 and C_8 with higher probabilities.

Figure 4 illustrate the impacts on probabilities of attacks brought by changes of defender's gain-coast ration R_D and effectiveness of countermeasures RM. In case 1: $R_D = 0$ means that the defender have no gain (or failure defense) by using countermeasure C_1. The attacker will launch the attack AS_1 of probability 1 since defender's low utility will lead a low probability of countermeasure C_1.

In case 2: $R_D = 1$ means that the defender increased his gain comparing with that in case 1. The probability of attack AP_1 decreases with the growing of RM and it is lower than that in case 1 when defender has a lower gain. This has shown the result of Theorem 2: a higher gain of defender, a lower probability of the corresponding attack in Nash Equilibrium of mixed strategies. In case 3, under the condition of a higher gain of defender ($R_D = 10$), the probability of attack AP_1 is even lower than that in case 2.

6 Conclusions

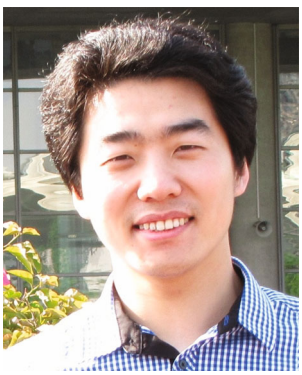
In this paper, we present a novel security assessment approach for the security and privacy issues in vehicular ad hoc networks. In particular, an attack-defense tree based risk analysis is given to identify the potential threats and related countermeasures in VANETs security. Further, we consider the costs and gains of the attacks and the countermeasures by introducing two utility functions: ROA and ROI. To model the interact of the attacker and defender, we introduce a game-theoretical analysis, or attack-defense game, in which each participant tends to get the maximum utility by maximizing ROI or ROA, which depends on the different attack/defense strategy and the associated attack/defense cost. In a practical case study, we show how our approach can be used to evaluate effectiveness and economic profitability of countermeasures as well as their deterrent effect on attackers, thus providing decision makers with a useful tool for performing better evaluation of VANETs security investments during the risk management process.

Acknowledgements This research was supported by National Natural Science Foundation of China (Grant No.61003218, 70971086), and Doctoral Fund of Ministry of Education of China (Grant No.20100073120065).

References

1. Lin X, Lu R, Zhang C, Zhu H, Ho P-H, Shen X (2008) Security in vehicular Ad Hoc networks. IEEE Commun Mag 46(4):88–95
2. Zhu H, Lu R, Lin X, Shen X (2009) Security in service-oriented vehicular networks. IEEE Wirel Commun Mag 16(4):16–22
3. Lin X, Lu R, Liang X, Shen X (2011) STAP: a social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs. In: Proc. IEEE INFOCOM'11. Shanghai, China, 10–15 April 2011
4. Hsiao H, Studer A, Chen C, Perrig A, Bai F, Bellur B, Lyer A (2011) Flooding-resilient broadcast authentication for vanets. In: Proc. ACM MOBICOM'11
5. Han Q, Du S, Ren D, Zhu H (2010) SAS: a secure data aggregation scheme in vehicular sensing networks. In: International Conference on Communications (IEEE ICC'10). Cape Town, South Africa, 23–27 May 2010
6. Reidt S, Srivatsa M, Balfe S (2009) The Fable of the bees: incentivizing robust revocation decision making in ad hoc networks. In: Proc. ACM CCS'09
7. Raya M, Hubaux J-P (2007) Securing vehicular ad hoc networks. JCS-SASN
8. Hoeper K, Gong G (2006) Bootstrapping security in mobile Ad Hoc networks using identity-based schemes with key revocation. Technical Report CACR 2006-04, Centre for Applied Cryptographic Research (CACR) at the University of Waterloo, Canada
9. Matt BJ (2004) Toward hierarchical identity-based cryptography for tactical networks. In: Proceedings of the 2004 Military Communications conference (MILCOM 2003), IEEE Computer Society, pp 727–735
10. Zhang Y, Liu W, Lou W, Fang Y, Kwon Y (2005) AC-PKI: anonymous and certificateless public key infrastructure for mobile ad hoc networks. In: Proceedings of the International Conference on Communications (ICC 2005). IEEE Computer Society, pp 3515–3519
11. Luo J, Hubaux J-P, Eugster PT (2005) DICTATE: distributed certification authority with probabilistic freshness for Ad Hoc networks. IEEE TDSC 2(4):311–323
12. Clulow J, Moore T (2006) Suicide for the common good: a new strategy for credential revocation in self-organizing systems. ACM SIGOPS Operating Systems Review 40(3):18–21
13. Anderson R, Moore T, Clulow J, Nagaraja S (2007) New strategies for revocation in Ad-Hoc networks. In: Proceedings of the 4th European workshop on security and privacy in ad hoc and sensor networks (ESAS 2007). Springer, pp 232–246
14. Moore T, Raya M, Clulow J, Papadimitratos P, Anderson R, Hubaux J-P (2008) Fast exclusion of errant devices from vehicular networks. In: Proceedings of the 5th conference on sensor, mesh and ad hoc communications and networks (SECON 2008), pp 135–143
15. Raya M, Hossein Manshaei M, Felegyhazi M, Hubaux J-P (2008) Revocation games in ephemeral networks. In: Proceedings of the 15th ACM conference on computer and communications security. ACM, pp 199–210
16. Freudiger J, Manshaei M, Hubaux J-P, Parkes DC (2009) On non-cooperative location privacy: a game-theoretic analysis. CCS'09, 2009
17. Beresford AR, Stajano F (2003) Location privacy in pervasive computing. Pervasive computing. IEEE 2(1):46–55
18. Bistarelli S, Dall'Aglio M, Peretti P (2007) Strategic games on defense trees. FAST 4691:1–15
19. Ren D, Du S, Zhu H (2011) A novel attack tree based risk assessment approach for location privacy preservation in the VANETs. In: Proc. of ICC 2011
20. Kordy B, Mauw S, Melissen M, Schweitzer P (2010) Attack-defense trees and two-player binary zero-sum extensive form games are equivalent. GameSec 6442:245–256

Suguo Du received the BSc degree in Applied Mathematics from Ocean University of Qingdao, China, in 1993, the MSc degree in Mathematics from Nanyang Technological University, Singapore, in 1998, and the PhD degree in Control Theory and Applications Centre from Coventry University, U.K., in 2002. She is currently an Associate Professor of Management Science Department in Antai College of Economics & Management, Shanghai Jiao Tong University, China. Her current research interests include Risk and Reliability Assessment, Fault Tree Analysis using Binary Decision Diagrams, Fault Detection for nonlinear system and Wireless Network Security Management.



Xiaolong Li received the B.Eng. degree in communication engineering from Nanjing University of Posts and Telecommunications,

Nanjing, China, in 2009. He is currently a M.Sc. candidate in the Department of Management Science, Antai College of Economics and Management, Shanghai Jiao Tong University, Shanghai, China. His research interests include risk and reliability assessment, network security assessment and other areas of system and management science.

Junbo Du received the B.Eng.Mgt degree in Department of Management Science from Shanghai University, Shanghai, China, in 2010. He is currently a M.Sc. candidate in the Department of Management Science, Antai College of Economics and Management, Shanghai Jiao Tong University, Shanghai, China. His research interests include risk and reliability assessment and other areas of system and management science

Haojin Zhu received his B.Sc. degree (2002) from Wuhan University (China), his M.Sc.(2005) degree from Shanghai Jiao Tong University (China), both in computer science and the Ph.D. in Electrical and Computer Engineering from the University of Waterloo (Canada), in 2009. He is currently an Associate Professor with Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His current research interests include wireless network security and distributed system security. He is a co-recipient of best paper awards of IEEE ICC 2007 - Computer and Communications Security Symposium and Chinacom 2008- Wireless Communication Symposium. He served as Guest Editor for IEEE Networks and Associate Editor for KSII Transactions on Internet and Information Systems. He currently serves as the Technical Program Committee for international conferences such as INFOCOM, GLOBECOM, ICC, WCNC and etc. He is a member of IEEE.