Journal of Mobile Multimedia, Vol. 12, No. 3&4 (2017) 213–224
© Rinton Press

WHEN GAME THEORY MEETS SECURITY AND PRIVACY RELATED RISK ASSESSMENT OF VEHICULAR NETWORKS (VANET)

SARA BAHAMOU
IA Laboratory, My Ismail University Meknes, Morocco
IRISA Laboratory, Institut Mines Telecom Atlantique, Rennes, France
sara.bahamou@imt-atlantique.fr

DRISS EL OUADGHIRI
IA Laboratory, My Ismail University
Meknes, Morocco
dmelouad@gmail.com

JEAN-MARIE BONNIN
IRISA Laboratory, IMT Atlantique
35510, Rennes, France
jean-marie.bonnin@irisa.fr

Vehicular ad-hoc networks faces numerous challenges, in particular Security and Privacy issues. Here, security assessment, risk evaluation and many other security features/ calculations are based generally on theoretical ideas, that may project in different level real life conditions. Hence, the existing of an important risk that these analysis may not work properly. We shouldn't forget that the important goal of VANET applications deployment is to reduce accident rate, which means the reduction of the human deaths and injuries number. Hence, our focus on the importance of strengthening the security aspect of different VANET applications and services, Which could be achieved by relying on security requirements. We found many research approaches covering a significant part of VANETs security and risk assessment challenges. This article is dedicated to the most crucial challenges in every security analysis methodology which is the study of different attack scenarios. These scenarios are generally in accordance with the most feared threats. So our goal here, is to determine the most probably attack scenario and how we can deploy the appropriate countermeasures in such a way some risks are acceptable. Therefore, our approach to VANET defense applies attack tree- defense tree for advanced vulnerabilities assessment and intrusion detection. Attack tree processing shows how attackers can penetrate a VANET, so by identifying critical vulnerabilities we can provide strategies for protecting the critical network assets. Thus, attack-tree leads us to the optimal intrusion detection and attack response. A strong link is existed between attacker and defender assets, which can be modeled by a mathematical analysis, called game theory analysis. This game approach has demonstrated the interaction in the attack-tree processing.

Keywords: Vehicular ad hoc networks Security and Privacy, location Privacy Risk Analysis, Attack Tree, Game Theory

1 Introduction

Serval research aims to develop wireless ad-hoc networks and their applications, in order to offer an efficient communication between different entities in Vehicular Ad-hoc Networks (VANETs). VANETs entities could be mobile or fixe with a deterministic properties or random such as: Roads infrastructure, bus, cars or trains, etc. Our work focus on vehicular networks (VANET) security, where the main objective is to provide road safety measures or information about vehicles speed and its location coordinates, which are transmitted between the vehicles with or without the deployment of the infrastructure. The communication between vehicles or Vehicle to Vehicle Communications (V2V) is made by a medium of inter-vehicle communication. The communication also enlist various road infrastructure equipments, with the intermediary of the vehicle communication to infrastructure (V2I). Also there are hybrid models obtained by the combination of V2V and V2I [1]. In this vehicular environment, communications are handled by specific entities embedded in the vehicles which are called: the On Board Units (OBU), by which vehicles are able to communicate with each other as well as Road Side Units (RSU)[1], that might be deployed every miles along the highways [1, 2, 3]. VANETs are deployed in order to support a large number of applications such as location based services, that generally demands the internet access from the vehicle. VANETs offers a huge number of applications, like Intelligent Transportation System (ITS), Intelligent Road Traffic Signaling System [4], Collision Avoiding Applications [5] and Vehicle Navigation System, this applications are basically used in order to provide road safety and infotainment services to the vehicles by providing them with collision alerts, warning messages and other location based informations. As being the most crucial part of the intelligent transportation systems, VANET has become, throughout years, more exposed to many attacks and security threats; due to its use of wireless based technologies as the core of its communications. The main objective of our research work is to improve the security level of exchanged data in these kind of networks. Our aims is to develop a general security architecture for vehicular communications in the ITS field. We can see the VANET networks as a new form of Mobile Ad-hoc NETwork (MANET). For our VANET system, game theory is implemented to analyze all the potential threats that could be executed by the attacker and the possible strategies of the defender to defend the system. Also the Nash Equilibrium concept is also used to define the stability state of the system, in order to build a strong defense mechanisms. For that we start via the next section by a general description of the main components of a general VANET game. Then we underline some benefits of game theory and challenges in the parameterization of that game.

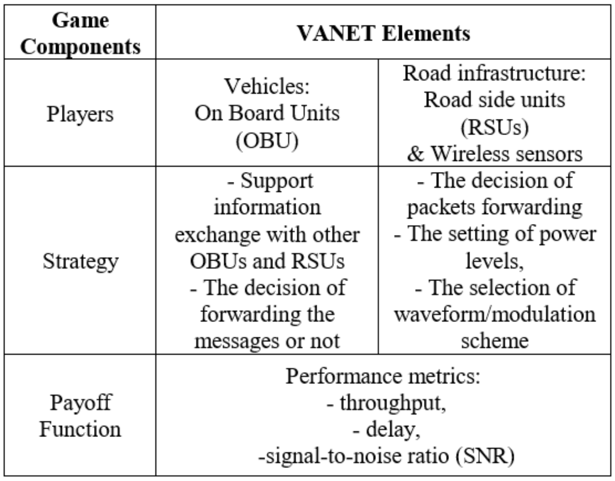
2 Modeling Vehicular Ad hoc Networks as a Game

In a VANET network, nodes could be considered as an independent decision makers, whose payoffs depends on other players actions. The following table 1 shows the general components of a VANET game.

Many advantages were provided by the game theory, such as tools to analyze distributed protocols for ad hoc networks. In [13], [14] and [15] we found the following common advantages:

- Game theory provides strong tools to study the existence and the convergence to a stable state when all the network nodes performs independently. Thus game theory offers a strict analysis of distributed protocols.

- Game theoretic analysis can provide a glimpse approaches for cross layer optimization.



Game Components	VANET Elements	
Players	Vehicles: On Board Units (OBU)	Road infrastructure: Road side units (RSUs) & Wireless sensors
Strategy	- Support information exchange with other OBUs and RSUs - The decision of forwarding the messages or not	- The decision of packets forwarding - The setting of power levels, - The selection of waveform/modulation scheme
Payoff Function	Performance metrics: - throughput, - delay, -signal-to-noise ratio (SNR)	

Table 1. VANET game components.

- The important use of the game theory to design of incentive schemes for ad hoc networks as presented in [16], [17] and [18], where incentive mechanisms proposed here to lead nodes to a constructive behavior.

Game theory analysis, help us to capture the cooperative and non-cooperative behavior of different components of a VANET system. Thus we can design the appropriate security architecture that provide incentives for individual components to contribute in the defense. Where by using game theory we can provide an important equilibria that converge to the optimal possible solution. In the following section we shows how these interactions between attacker and defender can be modeled in the vehicular networks. Besides, in the paper we highlight the trade-off existed between security and privacy. In any communicating system, we cannot talk about a secure system without ensuring its privacy. But nevertheless, in order to offer a secure system, such as a vehicular system, we need to have the access to some special information about the vehicles, such as the vehicle identity (ID), velocity, location, etc. This access can influence its privacy, because any attacker can also read, modify or even delete the transmitted information, which can cause many serious dangers. All this leads us to about the importance of ensuring the vehicular system privacy before applying different security mechanisms.

3 Privacy Games for VANET Networks

In VANETs, privacy concerns two main interests; content-oriented and context-oriented concerns. Content-oriented regards the privacy protection of collected or requested data. Contextual privacy concerns the contextual information, which includes the locations privacy of nodes and timing and pattern of the traffic flows. After studying the different aspect of the privacy in VANETs, we admit that the first step to be done is to ensure its context-oriented privacy. In our system model we focus on the node's location privacy of exchanged messages, which become the basis of our attack tree modeling[19].

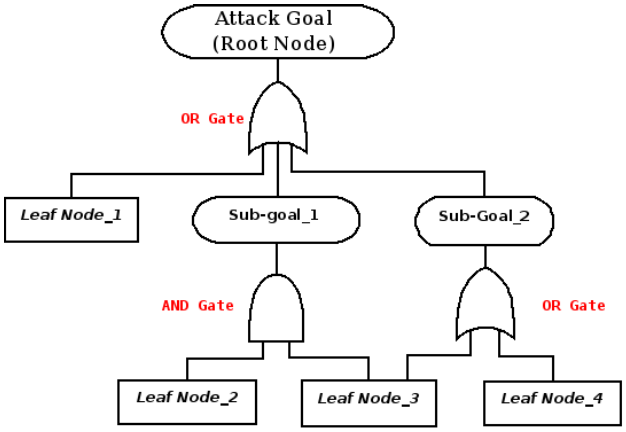


Fig. 1. A Basic Attack-Tree.

3.1 Building the Attack-countermeasures tree for VANET's Privacy

3.1.1 Attack- countermeasures tree construction

Attack trees helps to quantify security and privacy in term of losses caused by attacks [20] or defender's gain from applying such security mechanisms. The quantitative analysis leads to probabilistic risk analysis of the system. Like all mathematical tree models, attack trees are a diagrams where the root node is the goal of the attacker and leaf nodes are the potential attacks. Each leaf nodes are considered as sub goals, and their children are ways to achieve that sub goal. The attack goal (root) must be chosen carefully. Moreover, for complex systems, we can have many root nodes representing different goals. Nodes can be linked via Boolean operators in particular AND and OR gates [20, 21] (see Figure 2). OR gates are used to represent the different ways to achieving the same attack goal, while AND operator is used to depict different steps in achieving the attack goal.

We tries in [19] to cover the basis and foundations of attack tree modeling is. Similarly to the attack- countermeasures tree, where we start by defining the vehicular system model and its leakage which is in our case the node's location (or position) privacy [22, 23, 24]. Thus the attacker first goal here is the Disclosure of the Node's Position. Node here can be a vehicle, sensor deployed over the network or the vehicle's constructers (other authorities). So to achieve this goal, many possibilities could be imagined, for example an attacker can get the location of the nodes via the listening to the communications between nodes, because in VANETs most nodes broadcast clearly their locations with no encryption mechanisms. Or by inquiring directly the location from the target node. Or via the physical stealing of the vehicle. So its becomes easy now to define the intermediate causes of the attack goal. Each minimum combination of events at the level of the leaf node is known as an attack scenario. The purpose of establishing the attack tree is to define the most probable scenario that may occur in the VANET system. The full set of attack scenarios for an attack tree shows the different possibilities that are available to an attacker that has infinite resources, capabilities and motivations. Afterwards, for each sub-goal, we introduce countermeasures (or defense

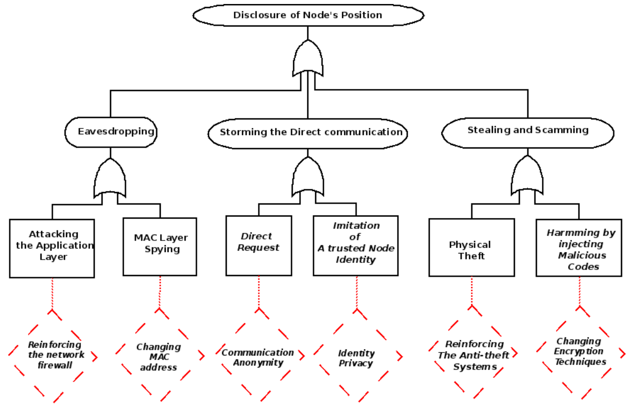
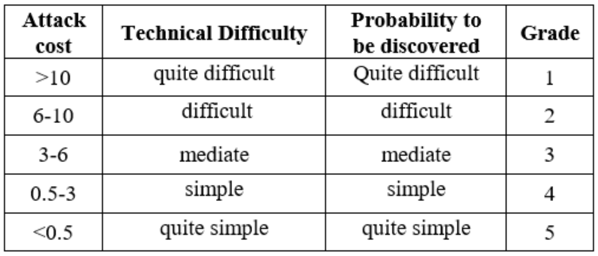

Disclosure of Node's Position
Eavesdropping
Storming the Direct communication
Stealing and Scamming
Attacking the Application Layer
MAC Layer Spying
Direct Request
Imitation of A trusted Node Identity
Physical Theft
Harmming by injecting Malicious Codes
Reinforcing the network firewall
Changing MAC address
Communication Anonymity
Identity Privacy
Reinforcing The Anti-theft Systems
Changing Encryption Techniques

Fig. 2. Attack-Defense Tree for location Privacy.



Attack cost	Technical Difficulty	Probability to be discovered	Grade
>10	quite difficult	Quite difficult	1
6-10	difficult	difficult	2
3-6	mediate	mediate	3
0.5-3	simple	simple	4
<0.5	quite simple	quite simple	5

Table 2. Grade Standards

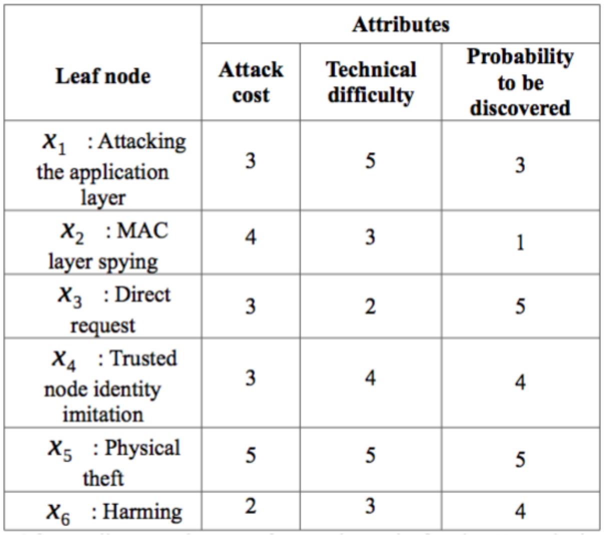
mechanisms) that can prevent each action, as we show in the following Figure 2.

From this figure, we take the example for the direct communication sub-goal, the attacker could try to impersonate someone else identity or make fake identity in order to find vulnerabilities in the VANET authentication mechanism. Attacker could also use its real own identity to communicate with the target node, where there is no rules that oblige that node to verify it. As we can highlight the fact that, the lake of the sensitivity about privacy is the main cause of this kind of attacks. Anonymity of the VANET should be ensured in the first time also enforcing the public key infrastructure (PKI) makes the network more robust against this kind of attacks.

3.1.2 Risk assessment and attack- countermeasures tree

For the risk assessments of our attack-countermeasures tree, we need to calculate the total probability of reaching the attacker main goal. So we need here to take into account many aspects, such as; the possibility to succeed, attack cost, technical difficulties and the probability that the attack could be discovered. The following table (Table 2) presents the grade standards related to this attributes [25].

The major challenge here, is to attribute values to each node in the attack tree. Because it's requires a knowledge of implementation details in the system, such as; protocols, hardware, operating systems and also the attack tools. So we tries to assign these values to leaf



Leaf node	Attributes		
	Attack cost	Technical difficulty	Probability to be discovered
x_1 : Attacking the application layer	3	5	3
x_2 : MAC layer spying	4	3	1
x_3 : Direct request	3	2	5
x_4 : Trusted node identity imitation	3	4	4
x_5 : Physical theft	5	5	5
x_6 : Harming	2	3	4

Table 3. Attributes for each leaf node.

nodes according to the metrics presented in [26]. So based on our attack tree, we assigned to each leaf node the following values, as listed in the table (Table 3).

After attributes assignment for attack tree leaf nodes. We calculate the occurrence probability of each leaf node, by using the following expression formula:

$$P_A = (w_1+u_1(\textit{attack coast}))+(w_2+u_2(\textit{technical difficulty}))+(w_3+u_3(\textit{discovering probability})) \tag{1}$$

Where $u_1(\textit{attack cost})$, $u_2(technical\ dificulty)$ and $u_3(\textit{discovering probability})$ are the utility functions of the attribute. w_1, w_2 and w_3 are the utilities corresponding weights: $w_1 = w_2 = w_3 = \frac{1}{3}$. So then we can calculate the total probability of reaching the attack goal, which is equal to 0.2336, by transferring the attack tree into a binary decision diagram (BDD) [29].

By the same way, we calculate the attack scenarios probabilities for the proposed attack tree, where we conclude that the attacker can get the target′s location privacy just by launching the attack x_3, thus to protect the system we should focus on this attack.

In addition, risk assessment is occurred also by quantifying the cost of attacks and the return on security investments for each attack tree scenario. We introduce here, economic factors in VANET location′s privacy analyzing, as presented previously this factors (mathematical indexes) are: the Return on Investment (ROI) [11] and Return on Attack (ROA) [12] factors. Each factor is considered as the utility functions for the system administrator and for the attacker, by viewing the scenario as a classical game with two player looking for different and usually opposite results. Thus, the attack- countermeasures tree is characterized by:

- Return On Investment (**ROI**) measures the return that a defender expects from a security investment over the costs for deploying a defense techniques. It is calculated with the formula:

$$ROI = \frac{(ALE \times RM) - CSI}{CSI} \tag{2}$$

  Where: **ALE** is the Annual expected Loss [28] caused by VANETs security threat; **RM** represents the Risk Mitigated by a countermeasure, and it$'$s represents the effectiveness of a countermeasure in mitigating the risk of loss deriving from exploiting a vulnerability. And **CSI** is the Cost of Security Investment, the cost that an enterprise sustains for implementing a given countermeasure.

- The Return On Attack (**ROA**) [11], measures the measures the gain that an attacker expects from a successful attack over the losses that he sustains due to the adoption of security measures by his target. ROA is defined as:

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

  Where **GI** represents the expected gain from a successful attack on the specified target and $cost_a$ is the cost sustained by the attacker to succeed, where $cost_{ac}$ is the additional cost brought by the countermeasure c adopted by the defender to mitigate the attack a.

In the next section we presents, how these measures are used as the utility functions of the VANET$'$s strategic game.

3.2 A VANET Attack-countermeasure Game

We show here, how game theoretic analysis [30] can be used to analyze the possible strategies of the VANET system administrator and of the attacker. So for our system use case, we consider a game which consist s of the following parts:

- 2 players: defender and attacker,

- A set of strategies S_a and S_d for each player. The set of defenders strategies S_d is the set of countermeasures techniques that he can introduce into the systems, and the set of attackers strategies S_a is the set of vulnerability that he can exploit.

- Utility function (or payoff) S_i for each player ($i = 1, 2$). The payoff functions are the Return on Investment (ROI) for the defender and the Return on Attack (ROA) for the attacker.

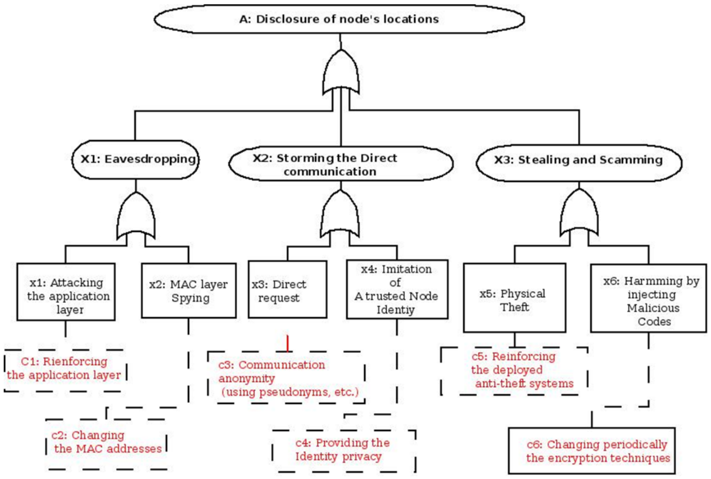
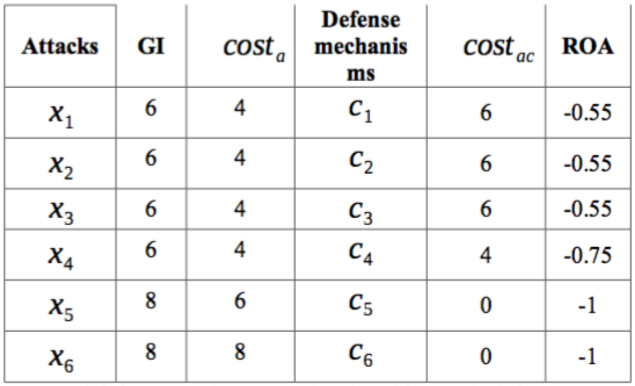

A: Disclosure of node's locations
X1: Eavesdropping
X2: Storming the Direct communication
X3: Stealing and Scamming
x1: Attacking the application layer
x2: MAC layer Spying
x3: Direct request
x4: Imitation of A trusted Node Identiy
x5: Physical Theft
x6: Harmming by injecting Malicious Codes
C1: Rienforcing the application layer
c2: Changing the MAC addresses
c3: Communication anonymity (using pseudonyms, etc.)
c4: Providing the Identity privacy
c5: Reinforcing the deployed anti-theft systems
c6: Changing periodically the encryption techniques

Fig. 3. Attack-Defense Tree for Location Privacy



Attacks	GI	$cost_a$	Defense mechanisms	$cost_{ac}$	ROA
x_1	6	4	c_1	6	-0.55
x_2	6	4	c_2	6	-0.55
x_3	6	4	c_3	6	-0.55
x_4	6	4	c_4	4	-0.75
x_5	8	6	c_5	0	-1
x_6	8	8	c_6	0	-1

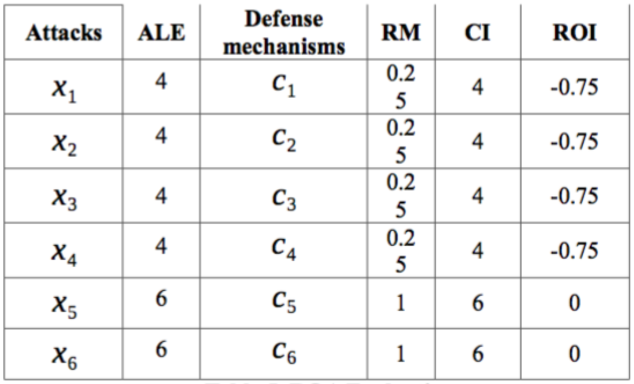
Table 4. ROA Evaluation

For our attack tree model, we consider the notations presented in the figure 3 for each node (leaf node).

Based on the expressions presented previously, the evaluation of ROA and of the ROI is given in the tables (Table 4 and Table 5)

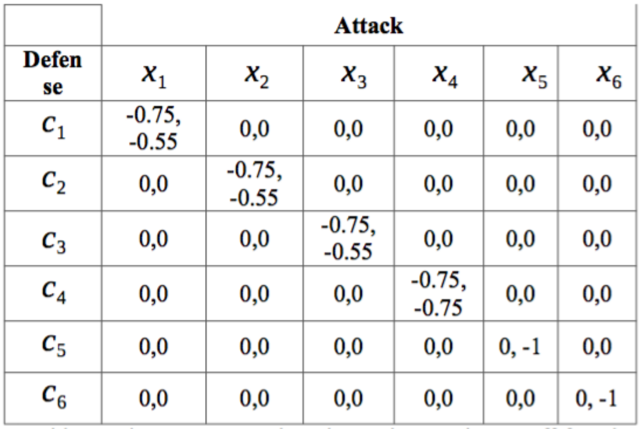
To model the strategic game related to this attack-defense tree, we consider the set of strategies S_d =$\{c_1, c_2, c_3, c_4, c_5, c_6\}$ and the attacker′s set of actions: S_a =$\{x_1, x_2, x_3, x_4, x_5, x_6\}$. We note here that the goal of each player here is to maximize their utility function. For our case, payoffs (utilities) function associated to a game strategy $(c_i, x_i)$are $u_d(c_i, x_i)$ for the defender, and u_a $(c_i, x_i)$for the attacker. Where: $ROI(c_i, x_i)$= u_d (c_i, x_i), and: $ROA(c_i, x_i)$= $\mathrm{u}_a(\mathrm{c}_i, x_i)$.
We get then, the utility game matrix show in the table 6.

In this matrix we suppose that players knows the payoff functions with each other, thus



Attacks	ALE	Defense mechanisms	RM	CI	ROI
x_1	4	c_1	0.25	4	-0.75
x_2	4	c_2	0.25	4	-0.75
x_3	4	c_3	0.25	4	-0.75
x_4	4	c_4	0.25	4	-0.75
x_5	6	c_5	1	6	0
x_6	6	c_6	1	6	0

Table 5. ROI Evaluation



	Attack					
Defense	x_1	x_2	x_3	x_4	x_5	x_6
c_1	-0.75, -0.55	0,0	0,0	0,0	0,0	0,0
c_2	0,0	-0.75, -0.55	0,0	0,0	0,0	0,0
c_3	0,0	0,0	-0.75, -0.55	0,0	0,0	0,0
c_4	0,0	0,0	0,0	-0.75, -0.75	0,0	0,0
c_5	0,0	0,0	0,0	0,0	0, -1	0,0
c_6	0,0	0,0	0,0	0,0	0,0	0, -1

Table 6. Game Strategy Utility Matrix

our game is a complete information game. Also we from the matrix we prove that, our game strategy leads to an equilibrium in the attack-defense tree. The *Nash Equilibrium* [30] state is approved in our model. Thus, the proposed countermeasures in the VANET system are the best response against the potential attacker strategies.

4 Attack-defense Games Improvement features

Besides the benefits given by applying the game theoretic analysis in the VANET system we should not ignore its important challenges of this analysis. The main areas of these challenges are:

- The rationality hypothesis: As game theories are founded on the fact that players act rationally, means that the player has an objective function. Each player tries to optimize (by maximizing or minimizing) given imposed constraints (by conditions in the game) on its choices of actions. Moreover, even if nodes in a VANET system can be programmed to act in a rational manner, the stable state of their rational behavior does not necessarily lead to socially optimal states. Thus, a perfect rationality hypothesis, does not reflect -in some cases- the observed behavior.

- The fact that a realistic VANET scenarios requires more complex models: Due to the dynamic and changed nature of the VANETs networks add many changes and modifications in the actions observed by vehicular and road nodes. Such modifications need to be modeled with a reasonable complex games of imperfect information. Additionally, modeling of wireless channel models and interactions between protocols at the different layers involves complex mathematical analysis.

- The choice of the utility function difficulty: It is quite clear, that it is hard to evaluate the way that VANET nodes will value the different levels of performance metrics, and what compromise they are prepared to make. The problem is aggravated by a shortage of analytical models that set each nodes available actions to higher layer metrics such as throughput.

Hence the importance of evolving this game theory studies, and go beyond Nash Equilibrium properties. VANET systems are a part of wireless systems, which have a strong capabilities of sensing their environments by using their cognitive capabilities. Our vehicular system have then the availability to detect its environment, here, the vehicular system defender can then detect the possible attackers interests. According to this, defender can optimize its defense mechanisms, related to the sensing results (we can imagine the same thing from the attacker point of view). The attack-defense game can be viewed here as a Stackelberg study [31] in which the attacker and the defender tries to find the optimize strategy before making their final decisions. We talk here about a game between a leader and followers, where the defender in our case study is the leader and the attacker techniques are the followers. In our current work we formulate the previous presented interaction between the leader and followers as a Stackelberg game [32], our goal here is to present a solution concept based on Stackelberg equilibrium, where the defender's goal is to maintain its balance in term of attack probabilities of the followers (attackers). The basics of Stackelberg game is that *the game is played sequentially such that the followers play knowing the decision of the leader. Moreover, the leader chooses its strategy knowing that the followers will play depending on their chosen strategy (best response). Thus the leader will choose a strategy and will communicate its decision to all the other users (followers) via a mediator. Followers will take into account the strategy played by the leader to decide their own strategies.* Current work describe more in details these analysis, where we tries to compare it to the Nash Equilibrium achieved in our attack-defense tree VANETs game.

5 Conclusion

Vehicular ad- hoc networks have emerged recently as a promising technology for next-generation ad-hoc networking. It provides wide variety of applications that cannot be supported directly by other ad-hoc networks. Security and risk assessments are a major concerns of this kind of networks. Via this paper we introduces the different methods to counter the much possible attack scenarios, by using the game theories principles. Applying the game theory methods may lead the vehicular system to several status, here we focus on the Nash Equilibrium case.

We conclude that detection of attackers behavior can depend on the defense mechanisms of the vehicular system. Thus the existence of a dynamic attack-defense tree, which can be developed and presented by using Stackelberg processing features. This process will be described in our future work.

Acknowledgements

We would thank the JMM committee members and reviewers for their remarks and opinions. The conference depends upon their care and competences. Their conscientiousness is much appreciated.

References

1. IEEE Standard for Message Sets for Vehicle/ Roadside Communications. 1455-1999, pp.i-130
2. Moustafa and Y. Zhang (Eds.). 2009. Vehicular Networks: Techniques, Standards and Applications. Auerbach publishers, Taylor and Francis Group.
3. E.B. Hamida, H. Noura, H. Znaidi: Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures. Electronics 2015, 4, 380−423.
4. N. S. Nafi and J.Y . Khan, A V ANET Based Intelligent Road Traffic Signaling System, IEEE T elecommunication Network and Applications Conference (ATNAC), Brisbane, QLD, pp. 1-6, 2012.
5. R. Eigner and G. Lutz, Collision Avoidance in VANETs−An Application for Ontological Context Models, in Proc. Of Sixth Annual IEEE Conference on Pervasive Computing and Communications (PERCOM08), Hong Kong, pp. 412−416, March 2008.
6. J. Eom, M. Park, S. Park, and T. Chung, A Framework of Defense System for Prevention of Insiders Malicious Behaviors, in Proceedings of the 13^{th} International Conference on Advanced Communication Technology, Korea, pp. 982−987, 2011.
7. R. Lu, X. Lin, and X. Shen, Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks, in INFOCOM 2010, San Diego, California, USA, March 2010.
8. S. Bistarelli, F.Fioravanti, and P.Peretti. Defense tree for economic evaluations of security investment. In 1st International Conference on Availability, Reliability and Security (ARES06), pages 416423, 2006.
9. D. Fudenberg and J. Tirole. Game Theory. MIT Press, 1991.
10. G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systemsl. NIST special publication 80030, NIST, National Institute of Standard Technology, July 2002.
11. W. Sonnenreich, J. Albanese, and B. Stout. Return On Security Investment (ROSI): A practical quantitative model. In Security in Information Systems, Proceedings of the 3rd International Workshop on Security in Information Systems, WOSIS 2005, pages 239252. INSTICC Press, 2005.
12. M. Cremonini and P. Martini. Evaluating information security investments from attackers perspective: the Return-On-Attack (ROA). In Fourth Work- shop on the Economics of Information Security, June 2005.
13. W. Di, Z. Dongxia, L. Sun, J. Liu and L. Juanjuan, A Game based routing algorithm for Congestion Control of multimedia transmission in VANETs, International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, pp. 1−6, Nov 2011.
14. D.B. Rawat, B.B. Bista and G. Yan, CoR− VANETs: Game Theoretic Approach for Channel and Rate Selection in Cognitive Radio VANETs. Seventh International Conference on Broadband Wireless Computing, Communication and Applications (BWCCA), Victoria, BC, pp: 94−99, Nov 2012.
15. J. Neel, J. Reed and R. Gilles, The role of game theory in the analysis of software radio networks;

SDR Forum Technical Conf., November 2002.

16. A. Urpi, M. Bonuccelli, and S. Giordano, Modeling cooperation in mobile ad hoc networks: a formal description of selfishness, Proc. of the 1^{st} Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, March 2003.
17. M. Felegyhazi, L. Buttyan, and J.-P. Hubaux,Nash equilibria of packet forwarding strategies in wireless ad hoc networks, to appear in IEEE Transactions on Mobile Computing.
18. P. Michiardi and R. Molva, A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile ad hoc networks,Proc. of the 1^{st} Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, March 2003.
19. M. H. Manshae et al., "Game theory meets network security and privacy," ACM Computing Surveys, Dec. 2011.
20. S. Du et al., "An attack-and-defence game for security assessment in vehicular ad hoc networks,"
21. S. Bahamou, D. El Ouadghiri and J-M. Bonnin, Vehicular Ad$-$hoc network Privacy Assessment Based on Attackdefense Tree. The tenth International workshop on communication technologies for vehicles (NETS4CARS, NETS4TRAINS and NETS4AIRCRAFT 2016), DonostiaSan Sebastian (Spain), June 6$-$7, 2016.
22. B. Schneier. Secrets and Lies: Digital Security in a Networked World. Wiley, 2000.
23. B. Schneier. Attack trees: Modeling security threats. Dr. Dobbs journal, December 1999.
24. J. Freudiger, M. Manshaei, J-P. Hubaux, Non-Cooperative Location Privacy: a game theoretic analysis, CCS$'$09, DC 2009.
25. S. Bistarelli, M. Dal$l'Ag$lio, P. Peretti, Strategic Games on Defense Trees, FAST 4691:1$-$15, 2007.
26. AR. Beresford; F. Stajano;Location Privacy in Pervasive Computing, Pervasive Computing. IEEE 2(1), 2003.
27. R. Rios, J. Lopez, Analysis of location privacy solutions in wireless sensor networks Privacy preservation in wireless sensor networks. Iet Communications, vol.5, pp. 2518$-$2532, 2011.
28. Ronal L. Krutz, Russell Dean Vines, and Edward M. Stroz. The CISSP Prep Guide:Mastering the Ten Domains of Computer Security. Wiley, August 2001.
29. Y. Sun, "A research on variable ordering methods of binary decision diagram". Shanghai Jiao Tong University, Shanghai, 2008.
30. R. Gibbons. A Primer in Game Theory. Pearson Higher Education, 1992.
31. C. Wang et al. Stackelberg game for spectrum reuse in the two-tier LTE femtocell network, 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, Shanghai, China, April 7-10, 2013,
32. A. Karouit et al. Hierarchical Slotted Wireless Random Channel Access with Power Control. Hindawi Publishing Corporation Mathematical Problems in Engineering, 2015,