An Attack Tree Based Comprehensive Framework for the Risk and Security Assessment of VANET using the Concepts of Game Theory and Fuzzy Logic

Sahil Garg
Department of Computer Science and Engineering
Chandigarh Engineering College
Landran, Mohali, India
garg.sahil1990@gmail.com

Gagangeet Singh Aujla
Department of Computer Science and Engineering
Chandigarh Engineering College
Landran, Mohali, India
cecm.cse.gagangeet@gmail.com

***Abstract*— VANET is a subclass of MANET that faces plenty of research challenges in terms of security. The existing risk and security analysis approach of VANET may not work well as it is purely based on the ideological beliefs, and it does not reflect any realistic conditions. In this research work, we have done the systematic study of the various algorithms which are used to find the inflection points of equilibrium that further reflects a trade-off between the attacker and the defender's gain or loss payoff for pursuing their pursuit. This paper explores and discusses the usage of game theory and fuzzy logic in analysis of the attack and defense equilibrium. After doing this research work we have also recommended the future directives for doing research in this area.**

***Index Terms*—Vehicular Adhoc Networks, Game theory, Fuzzy logic, Attack-Defense Tree**

I. INTRODUCTION

Vehicular Ad-hoc Network is a challenging and rapidly emerging class of Mobile Ad-hoc Network that enables vehicles to communicate with each other as well as with the roadside units. As VANET uses wireless medium as a mean of communication among the vehicles so it is always expected from it to support a large range of promising applications with high level of securities, hence, to support the wide range of road safety and comfort applications VANET has become an important component of Intelligent Transportation System. In 2003 U.S. Federal Communication Commission (FCC) has allocated 75 MHZ of Dedicated Short Range Spectrum (DSRC) for the use of Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. This overall DSRC communication architecture is drafted in the IEEE 1609 standard [1]. There are several characteristics of VANET that includes – decentralized infrastructure, high and predictable mobility, multihop topology, higher computation capability of nodes and unlimited transmission power of devices, but still VANETs are prone to attacks as there are many undercover agencies which are always being worked to make it more vulnerable to attacks.

In the earlier times VANET was only used for the emergency vehicles like ambulance, police vehicles, and fire brigades so that the vehicles within the range of 100-300 ft can communicate with each other, but its increasing demand has turned its use among all the vehicles to make the way safer. This concept has modified the definition of vehicles, as today's vehicles are known as "Computers on Wheels". VANET being the most important part of intelligent transportation system has become more vulnerable to attacks and due to its use of wireless based technology as a communication medium; it is always being much threatened by the security threats. There can be many reasons which put forward major inferences for a vulnerability to take serious action against the system. Financial or economic gain, revenge, ideological beliefs and intellectual challenge are some of the major aspects that make the attackers to hinder the VANET and disrupt its security. So due to the crucial security of VANET there is a need of stringent security requirements and for that it is solemnly required to study the infrastructure that VANET provides so to

doi:10.4304/jetwi.6.2.247-252

come across its security measures because even after the many advances still there are many challenges to undergo.

There are several applications of VANET like Intelligent Transportation System, Intelligent Road Traffic Signalling System [2], Collision Avoiding Applications [3] and Vehicle Navigation System that are typically used to provide road safety and infotainment services to the vehicles by providing them with collision alerts, warning messages and other location based information's. One of the major motivations of these applications is to reduce traffic accidents and human injuries, but still but these applications also have the rigid security requirements and to make these secure many security approaches on the basis of attack and defense tree solutions have come through but they do not have any realistic base. They have barely worked on the basis of their ideological belief and so suggested the different attacks and their corresponding defense mechanisms to make the VANET secure. So by keeping this in mind, we have proposed this research work in which we will use the concepts of game theory and fuzzy logic to do the risk and security assessment of VANET. We will further use the databases of International Monitoring Agencies that contains attack statistics data of some recent previous months to build the attack tree so that we can build our defense tree accordingly.

The rest of the paper is organized in the following way: in section II, we have discussed the game theoretical concepts to better understand the attack and defense strategies. In section III, we have reviewed the fuzzy logic concepts. In section IV, we have mentioned the related work accordingly. In section V, we have composed the problem formulation according to our analysis. In section VI, we have concluded the paper and so suggested the future work.

II. Game Theory

Game theory is a mathematical concept which uses the perceptions of rational decision makers to formulate the appropriate strategies that the entities (players) can adopt to win the game. There are several entities (players) in the game whose decisions are not fixed but can be influenced by the thought of decisions that their corresponding counterparts can take. A game can be classified according to the number of players in the game, there can be one-player game, two-player game or *n* players game (where *n* must be greater than '2').

According to Kant's perspective given in: "Choose only a strategy which, if you could will it to be chosen by all the players, would yield a better outcome from your point of view than any other".

There are three elements which all together, forms the complete game theory – the agent, the payoff function and the Nash equilibrium. The first element, the agent (player) need not be an individual person, it may be the team with many people but with common interests. The amount of satisfaction that the agents derive from their actions or events comprise the second element; the payoff function (or utility function). The third element of the game theory is the Nash equilibrium and it is the key concept of game theory. Nash Equilibrium can be termed as the set of strategies, called as action profile, in which there is only one strategy for each player. It also has the property that no player can do better by choosing an action different from its own, if the action of another player is known.

Let Act* is an action profile for some game G, P= $\{P_1, P_2, P_3..., P_n\}$ be the set of players and F is the set of payoff functions. It means that the game G can be defined as a triplet (P; Act*; F). Now if P_1 chooses the action Act*P_1 than the actions that can be chosen by the other players from the action set will be Act*-P_1 (-P_1 stands for except P_1).

As the concept of game theory is capable of judging the strategies of players involved in the game and we can also classify the security mechanism on the basis of two players, i.e. the attacker and the defender, so this concept is used in our research work to model the strategies of attacker's to attack and of the defender's to defend.

A. Applications of Game Theory Related To VANET

- The concept of game theory has earlier been used to analyze all the possible strategies of the attacker and the defender. This was done by implementing the game theoretical concepts on the attack-defense model. The concept was further used to calculate the Return on Investment (ROI) and Return on Attack (ROA) [4].
- The Nash equilibrium being the key concept of game theory has been used to determine the stability state of the players that were involved in the game. Furthermore, the concept was utilized to build the defense mechanism so to safeguard the VANET [5].
- The routing algorithm in collaboration with game theory had been evolved to control the congestion of multimedia transmission in VANET. Moreover, the payoff function had been projected to prove the presence and uniqueness of the Nash equilibrium [6].
- The game theory approach was used for making the channel and rate selection in cognitive radio VANET's. The conception was proved quite significant in achieving higher throughput of data rate for vehicular users [7].

III. Fuzzy Logic

By definition, Fuzzy Logic is an application of set theory in which Crisp and Non-Crisp boundary sets are analyzed for their degree of membership with respect to the numerical value understood in the linguistic terms.

Let U be the universal set and F be the fuzzy set of

U. So in fuzzy set F, each element can be mapped to [0, 1] by using the membership functions.

$$\mu F: U \rightarrow [0, 1]$$

And μF(u) can be interpreted as the degree of membership of element u in fuzzy set F for each u □ U.

Membership function in fuzzy logic represents the degree of truth in vaguely defined sets and also allows us to graphically represent a fuzzy set based on which trends, thresholds can be found, that can be used to take the critical decisions when multiple overlapping factors are influencing a particular process. For Example - Abnormal and Normal transmission of control message packets in VANET under adversity.

A. Applications of Fuzzy Logic Related To VANET

- Fuzzy logic has been used to implement the intelligent network intrusion detection system. The system uses the concepts of data mining that further combines the use of both Apriori and Kuok's Algorithm to produce the fuzzy rule set. Moreover, these rules were applied to the fuzzy inference engine to reveal the attacks in the network [8].
- The use of fuzzy logic was done to evaluate fuzzy sets using membership functions which are triangular in shape. By this application intrusion detection system was developed to detect the malicious behaviour of the vehicles and to identify the attacks.

IV. Related Work

Due to the vulnerable nature of VANET its security and privacy has become the most important prospect to research for. Moreover, in the context of VANET the interests of both the communities of researchers and academicians are hiking day by day.

In the research work described in the paper [4], the main focus was done on the comprehensive security analysis of the VANET. In doing this, the concept of the attack - defense game was used for doing the strategic analysis of both an attacker and a defender so that their attacking and defending mechanism can be studied in a better way. Furthermore, two utilities, i.e. Return on Investment (ROI) [4] and Return on Attack (ROA) [4] were introduced to measure the effectiveness of an attack and the cost incurred during the prevention of that attack. The concept of Nash Equilibrium was used to formulate the theorems for calculating the probabilities of an attack action and their corresponding countermeasures. On the whole, the tool that they made was a promising application which made the security evaluation of VANETs very effective.

To do the better risk assessment of VANET location privacy, the model was developed on the basis of various aspects like possibility to succeed, attack cost, technical difficulty and risk of being detected. Furthermore, an attack tree based approach was used to detect the possible attacking strategies of the attacker, to decide the countermeasures, and to determine the probability of reaching the attack goal. The drawback of this research work is that, this work is done purely on the basis of the theoretical conceptions and there is no realistic base of it [9].

The Voice Service Positioning Tool (VSPT) mechanism was formed to make the single hop beacon message secure during the transmission in VANET. For demonstrating this, two approaches were used. One was Time Efficient Stream Loss-Tolerant Authentication (TESLA) approach and another one was Elliptic Curve Digital Signature Algorithm Approach (ECDSA). TESLA was proved as an efficient alternative to signature based approach and is also immune to Denial of Service (DOS) attack, hence; it is being used for vehicle-to-vehicle communication. Moreover, it uses symmetric cryptographic approach rather than asymmetric cryptographic approach to make possible the delayed release of keys. Furthermore, ECDSA approach was used because of its efficient message authentication scheme and non-repudiation scheme [10].

There are many attacks [11] which can make the VANET prone to attacks. Denial of Service attack is one of them. This attack works to make the communication channel unavailable or inaccessible, so that the authentic nodes in the network could not access the network or its resources. In a DOS attack the unwanted load is enforced on the network intentionally so that the congestion in the network could be caused to disrupt the service. This attack affects the communication by making the network overloaded, by jamming the channel or by dropping the packets in between. Denial of Service attack takes more severe form when it occurs in the distributed form. In this distributed denial of service attacks, the attackers launch attacks from different locations so that the impact can be dispersed in the whole network. So to avoid all this and to make the communication channel secure three approaches were used, i.e. channel switching, technology switching and frequency hopping technique. Now, the decision that which approach is to be chosen is made by the processing unit which further suggests to the On-Board unit that is fitted on the vehicle so that it can adopt the appropriate approach and can make the channel secure [12].

V. Conclusion

In the previous work, the attack-defense trees have been made on the basis of the traditional and conventional attacks. However, with the passage of time the anatomy and variants of these attacks have changed and increased, and so has the defense mechanism. Moreover, no statistics and systematic methodology have been suggested for building the attack tree based on which the defense tree can be built. Hence, there is a need to build the tree structure based on the International Monitoring Agencies and Databases for such attacks which are prevailing

current in the context of VANET. Secondly, the previous work does not maintain the different probability states for each attack, although it does calculate the probabilities for payoff (attack cost vs. defense cost) but does not consider various probabilities related to factors like skill of the attacker and defense environmental factors of the defender. Moreover, there are multiple states which are either partially observable or non-observable. These are also not considered properly. The current concept of Nash Equilibrium discussed in the previous paper starts by assuming that strategies of all the players are given. It doesn't promote "entities, current skill set, technologies ecosystems" to a strategy. The idea of Nash equilibrium in the previous work also considers that the player of a multi-player game observes the strategies of all other players and then chooses the strategy that is best for him, given what they are doing. In other words, it freezes their behavior, assuming they will do the same thing whatever he does. Hence, we suggest that the state transition table must also be incorporated with multiple factors based on latest tree developed from the descriptive statistics of the International Monitoring Agencies and Databases. Above all, a case study must be done using the parameters shown in the table below.

Case study can be used to do the detailed investigation and understanding of an attack-defense game. Therefore, for doing a case study it becomes desirable to study the detailed payoff values for both an attacker and a defender. Hence, to calculate these factors we have suggested some case study parameters. Table I. Shown below illustrates the case study parameters according to both attacker's and defender's point of view.

TABLE I.

CASE STUDY PARAMETERS

Attacker's Point of View	**Defender's Point of View**
Expected Gain	Expected Loss
Return on Attack	Return on Investment
The risk of being detected	The risk of being attacked
Cost of Investment	Cost of Investment

An attacker on the one hand tries to maximize his gain by minimizing the risk and investment cost he had to sustain due to countermeasures adopted, whereas, the defender on the other hand tries to maximize his return by minimizing the loss and investment cost he sustains on the defense mechanisms. The attacker always tries to minimize the risk of being detected, whereas defender on the other hand tries to minimize the risk of being attacked. We believe that if both the players that are involved in the game (an attacker and a defender) are able to put the hold over these parameters then their performance can be maximized. Moreover, these case study parameters may be used to analyze the actual behavior of an attacker and a defender in the simulated environment.

VI. RECCOMENDATIONS AND FUTURE DIRECTIONS

Based on the research and analysis done from previous and contemporary work, we suggest the following steps:-

Fig. 1 shows the block diagram in which we have suggested some steps to by which the risk and security analysis of VANETs can be done. Step 1 begins with the construction of an attack tree and its corresponding defense tree. To build the tree, that we have suggested, descriptive statistical data is needed, which can be collected from the databases of International Monitoring Agencies. Furthermore, to check the equilibrium of that attack and defense tree in the VANET environment, simulation can be done. Moreover, for checking the ground truth and validity of an attack-defense tree that we have suggested, a case study can be done and for it initially, some case study parameters are needed to be initialized. In this paper we have suggested some case–study parameters as shown in Table I. After this, the nodes are made to communicate with each other so that the attack could be introduced. The corresponding defense mechanism is then enforced to detect an attack. Finally, after the detection of an attack, the Nash equilibrium can be analyzed on the basis of effectiveness and mitigation of the this attack and defense mechanism.

Furthermore, we suggest that the people can contribute in this area by conducting the assessment of their assets. This can be done by using vulnerabilities scoring systems like Common Vulnerability Scoring System (CVSS).

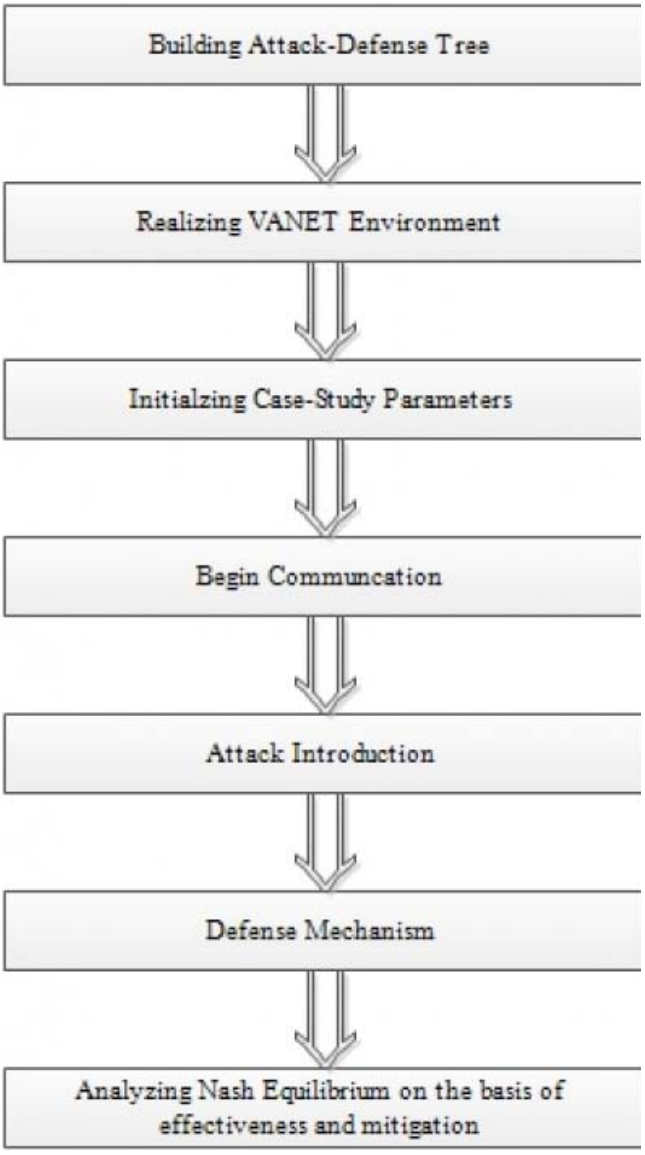

Figure 1. Block Diagram of our Research Methodology

REFERENCES

[1] J.B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," *in Proc. of the IEEE*, vol. 99, no. 7, pp. 1162-1182, 2011.

[2] N.S. Nafi and J.Y. Khan, "A VANET Based Intelligent Road Traffic Signaling System," *IEEE Telecommunication Network and Applications Conference (ATNAC)*, Brisbane, QLD, pp. 1-6, 2012.

[3] 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 (PERCOM'08)*, Hong Kong, pp. 412-416, March 2008.

[4] S. Du, X. Li, J. Du and H. Zhu, "An attack and-defense game for security assessment in vehicular ad hoc networks," *Springer Science + Business Media*, LLC 2012.

[5] M. Prabhakar, J.N. Singh and G. Mahadevan, "Defensive Mechanism for VANET security in game theoretic approach using heuristic based ant colony optimization," *International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, pp. 1-7, Jan 2013.

[6] 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.

[7] 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.

[8] A.E. Semary, J Edmonds, J.G. Pino and M. Papa, "Applying Data Mining of Fuzzy Association Rules to Network Intrusion Detection," *In Proc. of the IEEE Information Assurance Workshop*, United States Military Academy, West Point, NY, pp. 100-107, June 2006.

[9] D. Ren, S. Du and H. Zhu, "A novel attack tree based risk assessment approach for location privacy preservation in the VANETs," *In Proc. Of International Conference on Communications (IEEE ICC'11)*, Kyoto, pp. 1-5, June 2011.

[10] C. Lyu, D. Gu, X. Zhang, S. Sun and Y. Tang, "Efficient, Fast and Scalable Authentication for VANETs," *IEEE Wireless Communications and Networking Conference (WCNC)*, Shanghai, pp. 1768-1773, April 2013.

[11] I.A. Sumra, I. Ahmad, H. Hasbullah and J.L. bin Ab Manan, "Classes of Attacks in VANET," *Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, Riyadh, pp. 1-5, April 2011.

[12] H. Hasbullah, I.A. Soomro and J.A. Manan, "Denial of Service (DOS) Attack and its Possible Solutions in VANET," *World Academy of Science, Engineering and Technology*, pp. 411-415, 2010.

Sahil Garg (22-12-1990), Ambala, Haryana, India.

He received the B.Tech degree in Computer Science and Engineering from Maharishi Markandeshwar University, Mullana, Ambala, India, in 2012. He is currently an M.Tech student in the Department of Computer Science and Engineering in Chandigarh Engineering College, Landran, Mohali, Punjab, India.

His research interests include Security and Privacy Based Risk Assessment of Vehicular Adhoc Network, Game Theory and other areas of Wireless Network Security.

Gagangeet Singh Aujla (15-07-1982), Kapurthala, Punjab, India.

He received the B.Tech degree in Computer Science and Engineering from Punjab technical University, Jalandhar, Punjab, India, in 2003, and the M.Tech degree from Punjab Technical University, Jalandhar, Punjab, India, in 2012.

He is currently an Associate Professor in Department of Computer Science and Engineering at Chandigarh Engineering College, Landran, Mohali, Punjab, India. His current research interests include Vehicular Adhoc Networks, Wireless Body Area Networks, Cryptography and Wireless Communication. He is a lifetime member of Indian Society of Technical Education and a senior member of Computer Society of India. He currently serves as the reviewer in International Journal of Security and Network Communication, Wiley Publications.