# An Expatiate Game-Theory Based Analysis On Multiattacker Scenario In MANETS

Venkateswarlu.B[#1], Venugopal.S[*2]

[#1]*M.Tech Student, Department of CSE, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India*
[*2]*Assistant Professor, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India*

**Abstract--Nodes in Mobile Ad Hoc Network (MANET) have mobility which causes the network vulnerable to attacks. Malicious nodes can attack MANET for utility and other gains as they have ability to move. Regular node sin the network has certain strategies towards their functionality and security. In the same fashion, malicious nodes must be having their own strategies to make attacks on the network. It is important to analyze the profiles of both kinds of nodes. Recently Li et al. proposed a framework that analyzes interactions among the nodes in Mobile Ad Hoc Network in order to secure the network from malicious access. Their solution is based on game theory. Regular nodes update their security aspects based on the malicious nodes and their behavior. In the same manner the malicious nodes also think about the risk of being caught. They also think about when to flee to avoid the risk. In this paper we practically implement the proposed game theory. We built a prototype application to simulate the MANET scenario that analyzes interactions among the nodes. The empirical results revealed that the proposed framework is useful.**

**Keywords– MANET, game theory, attack, flee, security**

## I. INTRODUCTION

MANET is the network with nodes that can move from one place to another place. This kind of network is formed on demand and the nodes are automatically configured without any fixed network infrastructure. Collaboration among the nodes is the main feature of this network which is widely used in the real world. This network is handy in case of natural calamities, emergencies and other such scenarios where normal communications are disrupted. The nodes in MANET try to maximize their utilities while making communications with other nodes in the network. There needs to be cooperation among the nodes for successful communication. The nodes can be made to participate genuinely using certain techniques known as reputation systems, barter economy, and virtual currency. All the nodes are supposed participate in regular communications. However, some nodes behave selfishly and do not cooperate with other nodes. Such nodes may even drop packets. Maximizing the damage caused to the network is the common objective of malicious nodes while the genuine nodes have good intentions.

Reducing the impact of malicious nodes is the need of the hour. To do so regular nodes are to monitor their neighbors and evaluate them continuously. Nodes much have trust level so as to achieve efficient participation in the network. There are some criteria that can differentiate the node from other nodes. When any node in the network is not participating genuinely that node might have been compromised or we can call it a selfish node. The selfish behavior can also be attributed to the lack of resources to the node sin MANET. There are intelligent malicious nodes that choose to cooperate frequently in order to deceive regular nodes. Such nodes also have the habit of attack and flee thus avoiding consequences of malicious activities. Malicious nodes have an optimal strategy to cooperate regular nods in order to deceive them. Game theory analysis is used between the regular and malicious nodes in order to find the attack and flee nature of malicious nodes may help them to avoid risks. To model the game theory analysis we used dynamic Bayesian game in this paper. When the network is in full swing, regular and malicious nodes behavior is analyzed and observations say that the beliefs of the regular nodes influence their behavior towards the activities of the malicious nodes. Fleeing decision is made by malicious node after assessing risk in terms of flee and its cost.

In this paper we make simulations to demonstrate the flee strategy and also bring forth number of countermeasures that can prevent the problems. The remainder of this paper is structured as follows. Section II reviews literature pertaining to security in MANET and game theoretic analysis. Section III provides information about the proposed work. Section IV presents the results of experiments while section V concludes the paper.

## II. RELATED WORKS

Nodes in the MANET work in coordination with each other. When there is some sort of incentive for the cooperation, the nodes can perform well and the whole network works fine. The incentives play an important role in brings about cooperation among the nodes in MANET [1], [2] and [3]. Malicious nodes are not modeled as cooperative nodes in these works. But in reality nodes may be selfish in order to avoid participation in communication so as to save their energy levels. Therefore in this paper we model malicious nodes with their own functions that are different from that of regular nodes. Malicious nodes conceal their intentions while the regular nodes have their own beliefs and based on them they behave towards other regular nodes and opponents. Incentive based approaches are explored in [4] and [5] while game theory is a tool which is very powerful to study interactions among the selfish and regular nodes in the MANET [6], [7], [8]. Wireless ad hoc networks are also studied using the game theory explored in [9] and [10]. There is some peculiar behavior among selfishnodes also. They frequently cooperate with regular nodes and behave like regular nodes. They are not easy to detect and handle. To overcome this problem game theory is studied in [11] and [10]. Mixed strategy is followed in [11] in order to prevent jamming attacks. For energy efficiency Bayesian game is studied in [11] which made use of game theory [12] for analyzing various scenarios pertaining to communications among nodes. In this paper reputation system [13], [14], [15], [16] is used to simulate the MANET and study the nodes using game theory. Many reputation systems came into existence as explored in [17], [18] and [19]. A modified game theory known as tit-for-tat is followed in [20] for cooperative communications.

## III. PROPOSED FRAMEWORK FOR GAME THEORITIC ANALYSIS

We studied the problem of analyzing the interactions of malicious and regular nodes in MANET. The nodes in MANET need cooperative communication. The clustered nature of MANET with regular nodes and malicious nodes is represented in figure 1. There is wrestling between regular nodes and malicious nodes. It also shows the decision making process of regular nodes based on the beliefs and interactions from regular and malicious nodes.

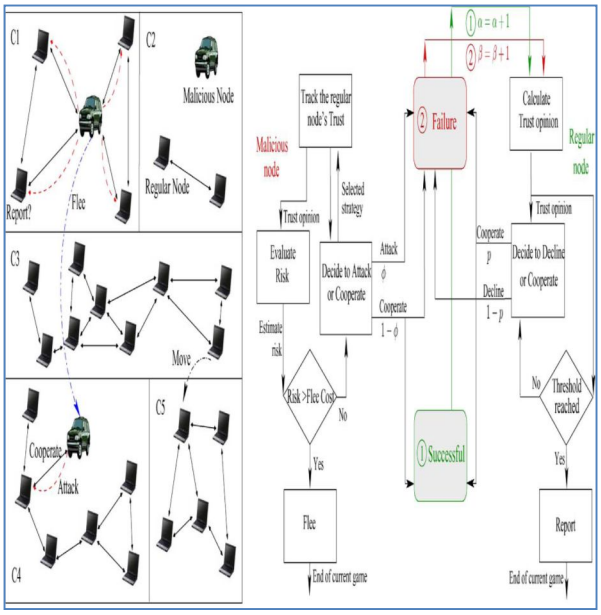


Figure 1 – MANET scenario and the decision process (excerpt from [21])

As can be seen in figure 1, it is evident that the MANET is divided into clusters. The nodes are of two types. The model is taken from [21] for the game theory implementation. The malicious nodes cooperate in communication frequently to deceive regular nodes. Malicious node evaluates the risk of attack in terms of being caught. If the risk cost is greater than flee cost, it prefers to flee otherwise it prefers to cooperate or attack. The attack is not successful because the framework evaluates trust communications. The cooperation is successful as the nodes are deceived. With regard to regular node, it evaluates the trust of nodes and also verifies its beliefs to decide whether to cooperate with malicious nodes or decline the requests.

### Game Specification

In the game i is the player who act as sender. However, the sender could be either malicious node or regular node. The receiver is the j which is always a regular node. Each player has strategy space. For instance {C, D, R} and {A, C, F} are the strategy spaces of sender and receiver respectively. The payoffs for the strategy spaces in the game such as CDR and ACF are presented in table 1.

| | C | D | R |
|---|---|---|---|
| A | $(G_A-C_A,-G_A-C_C)$ | $(-C_A,0)$ | $(-G_R-C_A,G_R-C_R)$ |
| C | $(-C_C,-G_C,-C_C)$ | $(-C_C,0)$ | $(-G_R-C_C,G_R-C_R)$ |
| F | $(G_A-C_A,-G_A-C_C)$ | $(-C_F,0)$ | $(-C_F-C_R)$ |
| | C | D | R |
| C | $(G_C,-C_C$, same) | $(-C_C,0)$ | $(-C_C,-L_F-C_R)$ |
| D | $(0,-C_C,)$ | (0,0) | $(0,-L_F-C_R)$ |
| R | $(-L_F-C_R,-C_C)$ | $(-L_F-C_R,0)$ | $(-L_F-C_R$, same) |

Table 1 –Payoffs for the players in the game(excerpt from [21])

As can be seen in payoffs table, except for D all strategies incur cost. Here the cost is nothing but energyconsumed or spent. In this game node j has to get updations to its beliefs as the game is being evaluated. The trust belief rule is as follows.

$$\alpha / (\alpha+\beta)$$

The total uncertainty is computed as follows.

$$u = \frac{12.\alpha.\beta}{(\alpha+\beta)^2.(\alpha+\beta+1)}$$

| | |
|---|---|
| $C_A/C_C/C_F/C_R$ | Cost for attack/cooperate/flee/report |
| $G_A/G_C/G_R$ | Gain for attack/cooperate/report |
| α | The number of detected cooperations |
| β | The number of detected attacks or declines |
| θ | The probability that a node is a malicious node |
| φ | The probability that a node malicious node attacks |
| P | The probability that a regular node cooperates |

Table 2 Notations

**Algorithms Used**

Algorithms are used by the players to have their respective strategies. For instance PBE strategy of regular and malicious players isevaluated using the following algorithms.

**Algorithm 1** Player j's PBE strategy

1: while θ. (1-u) < T do
2: if $\theta \le (G_C-C_C) / (G_C+G_A)$ then
3: Choose C with p=1;
4: else
5: Choose C with $p = (C_A-C_C) / G_A$;
6: end if;
7: Updated α, β, get θ and calculate u;
8: end while
9: Report node i as a malicious node;

Listing 1 –Algorithm for receiver's PBE strategy
This algorithm is used to compute and update the beliefs of player *j* in the game. Its PBE strategy is based on the criteria specified.

**Algorithm 2** Malicious type player i's PBE strategy

1: while $E_i(F) < \max\{ E_i(A), E_i(C)\}$ do
2: if $\theta \le (G_C-C_C) / (G_C+G_A)$ then
3: Choose A with φ = 1;
4: else
5: Choose A with $\varphi = (G_C-C_C) / ((G_C+G_A) . \theta)$;
6: end if;
7: Track j's θ, estimate risk of being caught and $E_i(F)$;
8: end while
9: Flee to a remote area and attack again;

Listing 2 – Algorithm for PBE strategy of malicious player
This algorithm is used to compute and update the beliefs of player *i* in the game. Its PBE strategy is based on the criteria specified.

## IV. EXPERIMENTAL RESUTLS

We made experiments in terms of average utility, PBE strategy, pure strategy, mixed strategy, index of stage games, hit and run, flee, and never flee.

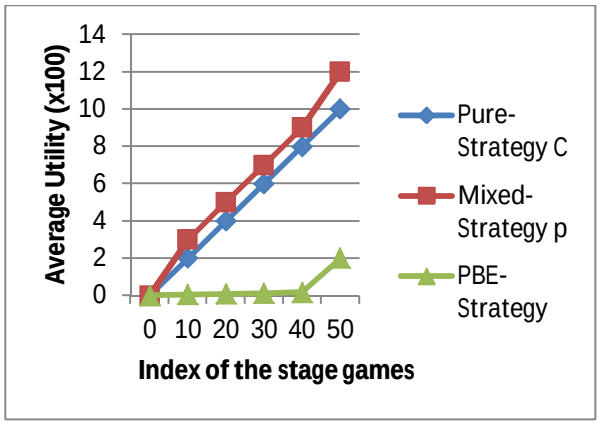


Fig. 2 –Utility of regular node

As can be seen in figure 2, when malicious nodes use their PBE strategy, the regular nodes follow their strategy according to their beliefs. The utility of regular nodes in various strategies is presented here. As can be seen in results, the strategy of regular node out performs the rest.

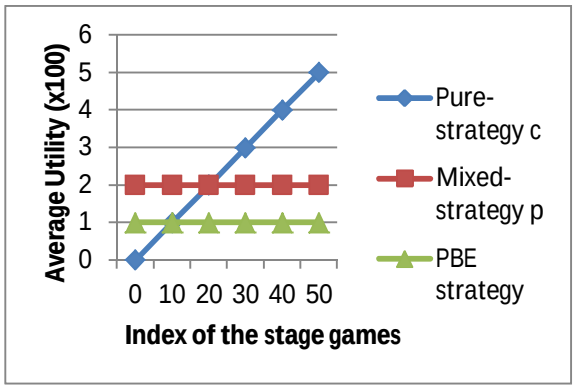


Fig. 3 – Utility of malicious node

As can be seen in figure 3, when malicious nodes use their PBE strategy, the regular nodes follow their strategy according to their beliefs. The utility of regular nodes in various strategies is presented here. As can be seen in results, the strategy of regular node out performs the rest.

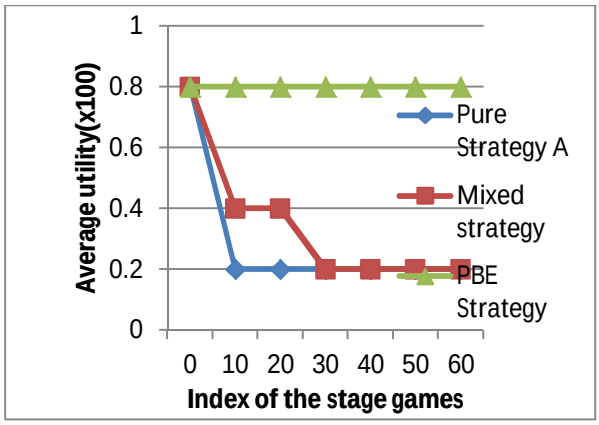


Fig. 4 – Utility of malicious nodes

As can be seen in figure 4, when malicious nodes use their PBE strategy, the regular nodes follow their strategy according to their beliefs. The utility of regular nodes in various strategies is presented here. As can be seen in results, the strategy of regular node out performs the rest.

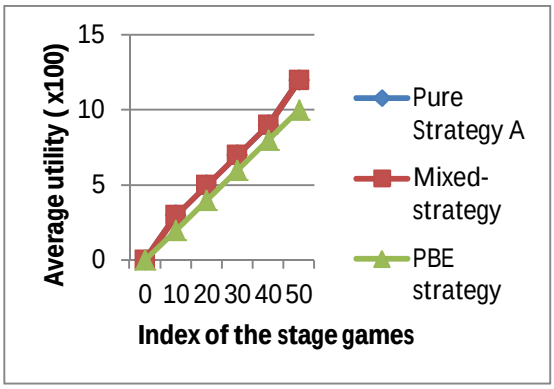


Fig. 5 – Utility of regular nodes

As can be seen in figure 5, when malicious nodes use their PBE strategy, the regular nodes follow their strategy according to their beliefs. The utility of regular nodes in various strategies is presented here. As can be seen in results, the strategy of regular node out performs the rest.

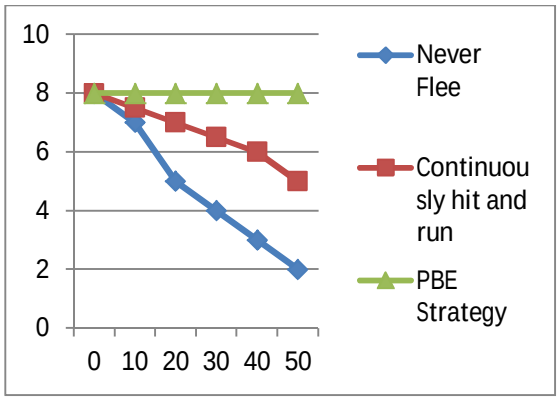


Fig. 6 – Utility of regular nodes (Flee strategy comparison)

As can be seen in figure 6, when malicious nodes use their flee strategy, the regular nodes follow their strategy according to their beliefs. The utility of regular nodes in various strategies is presented here. As can be seen in results, the strategy of regular node out performs the rest.

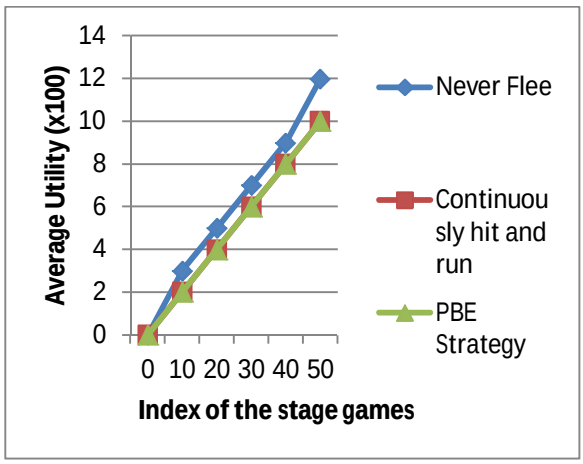


Fig. 7 – Utility of regular nodes (Flee strategy comparison)

As can be seen in figure 7, when malicious nodes use their flee strategy, the regular nodes follow their strategy according to their beliefs. The utility of regular nodes in various strategies is presented here. As can be seen in results, the strategy of regular node out performs the rest.

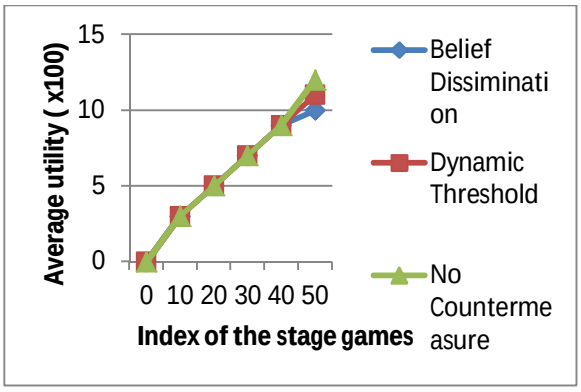


Fig. 8 – Utility of regular nodes (Counter measure comparison)

As can be seen in figure 7, when malicious nodes use their flee strategy, the regular nodes follow their strategy according to their beliefs. The utility of regular nodes in various strategies is presented here. As can be seen in results, the strategy of regular node out performs the rest.

## V. CONCLUSION

In this paper we studied the problem of analyzing interactions among nodes in MANET. The intention of this study is to know the strategic profile of both genuine nodes and malicious nodes. This will help in protecting network from malicious nodes. To achieve this we implement Bayesian game theory framework that analyzes the behavior of regular and malicious nodes. The regular node has certain beliefs. When it is involved in communication, its cooperation to other nodes depends on its beliefs. It may cooperate its opponent also based on its belief. In the same fashion, malicious nodes also have their own strategic profiles. They keep evaluating the risk of being caught and how to flee to avoid risk. This paper analyzes the strategic profiles of two nodes and finds how the flee strategy is advantageous to malicious nodes. The simulations reveal that the application is useful in making security decisions.

## REFERENCES

[1] M. Felegyhazi, J. Hubaux, and L. Buttyan, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," *IEEE Trans. MobileComput.*, vol. 5, no. 5, pp. 463–476, May 2006.

[2] L. Buttyan and J. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM Mobile Netw. Appl.*, vol. 8, no. 5, pp. 579– 592, Oct. 2003.

[3] A. Blanc, Y. Liu, and A. Vahdat, "Designing incentives for peer-to-peer routing," in *Proc. IEEE INFOCOM*, 2005, pp. 374–385.

[4] G. Theodorakopoulos and J. Baras, "Malicious users in unstructured networks," in *Proc. IEEE INFOCOM*, 2007, pp. 884–891.

[5] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives and strategies," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 1, pp. 78–118, Feb. 2005.

[6] S. Sarkar, E. Altman, R. El-Azouzi, and Y. Hayel, "Information concealing games," in *Proc. IEEE INFOCOM*, 2008, pp. 2119–2127.

[7] S. Ng and W. Seah, "Game-theoretic model for collaborative protocols in selfish, tariff-free, multihop wireless networks," in *Proc. IEEEINFOCOM*, 2008, pp. 216–220.

[8] P. Nuggehalli, M. Sarkar, K. Kulkarni, and R. Rao, "A game-theoretic analysis of QoS in wireless MAC," in *Proc. IEEE INFOCOM*, 2008, pp. 1903–1911.

[9] L. Chen and J. Leneutre, "Selfishness, not always a nightmare: Modeling selfish MAC behaviors in wireless mobile ad hoc networks," in *Proc.IEEE ICDCS*, 2007, p. 16.

[10] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "SPREAD: Foiling smart jammers using multi-layer agility," in *Proc. IEEE INFOCOM*, 2007, pp. 2536–2540.

[11] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. ACM GameNets*, 2006, p. 4.

[12] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA: MIT Press, 1991.

[13] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Stanford Univ. Press, Stanford, CA, Tech. Rep. (CoRR cs.NI/0307012), 2003.

[14] S. Buchegger and J. Boudec, "Performance analysis of the confidant protocol," in *Proc. ACM MobiHoc*, 2002, pp. 226–236.

[15] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc.Commun. Multimedia Secur.*, 2002, pp. 107–121.

[16] S. Buchegger and J. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in *Proc. 2nd Workshop Econ. Peer-to-PeerSyst.*, 2004, pp. 403–410.

[17] F. Li, A. Srinivasan, M. Lu, and J. Wu, "Uncertainty mitigation for utility-oriented routing in MANETs," in *Proc. IEEE GLOBECOM*, 2007, pp. 427–431.

[18] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, Mar. 2007.

[19] F. Li and J. Wu, "Mobility reduces uncertainty in MANETs," in *Proc. IEEE INFOCOM*, 2007, pp. 1946–1954.

[20] V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. Rao, "Cooperation in wireless ad hoc networks," in *Proc. IEEE INFOCOM*, 2003, pp. 808–817.

[21] Feng Li, Yinying Yang, and Jie Wu, "Attack and Flee: Game-Theory-Based Analysis on
Interactions Among Nodes in MANETs". IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, VOL. 40, NO. 3, JUNE 2010.

## AUTHORS

**Venkateswarlu Bollapalli** has completed B.Tech (I.T) from R.V.R.& J.C. College of Engineering and Pursuing M.Tech (C.S.E) in QIS College of Engineering and Technology, JNTUK, Ongole, Andhra Pradesh, India. His main research interest includes information security and Computer Ad-Hoc networks.

**Sadineni Venugopal** is working as an Assistant Professor in QIS College of Engineering and Technology, JNTUk, Ongole, Andhra Pradesh, India. He has completed M.Tech from Andhra University. His main research interest includes Cloud Computing and Computer Ad-Hoc networks.