Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Invade and Shun: Game-Theory-Based Analysis on Interactions among Nodes in MANETs

Pooja Nayak S[*]
Computer Science and Engineering
India

Abstract- In mobile ad hoc networks, nodes have the inherent ability to move. Aside from conducting attacks to maximize their utility and cooperating with regular nodes to deceive them, malicious nodes get better payoffs with the ability to move. In this paper, we propose a game theoretic framework to analyze the strategy profiles for regular and malicious nodes. We model the situation as a dynamic Bayesian signaling game and analyze and present the underlining connection between nodes' best combination of actions and the cost and gain of the individual strategy.

Regular nodes consistently update their beliefs based on the opponents' behavior, while malicious nodes evaluate their risk of being caught to decide when to flee. Some possible countermeasures for regular nodes that can impact malicious nodes' decisions are presented as well. An extensive analysis and simulation study shows that the proposed equilibrium strategy profile outperforms other pure or mixed strategies and proves the importance of restricting malicious nodes' advantages brought by the flee option.

Keywords— Bayesian signaling game, game theory, mobile ad hoc networks (MANETs), mobility, reputation systems, sequential rationality, uncertainty..

I. INTRODUCTION

THE COLLABORATION between the participants is the foundation for mobile ad hoc networks (MANETs) to achieve the desired functionalities. The topologies in MANETs change dynamically because of node movement. Nodes in MANETs usually have no predefined trust between each other. Moreover, all nodes tend to maximize their own *utility* (also referred to as *payoff*) in activities. Among existing research, different mechanisms (e.g., reputation systems, virtual currency, and barter economy) have been developed to stimulate cooperation and mitigate nodes' selfish behavior. Aside from regular nodes' selfish behavior, malicious nodes also exist in the network. The common objective of malicious nodes is maximizing the damage to the network while avoiding being caught. Their utility comes from activities that disrupt the operation of the network and waste the resources of regular nodes. comply with the sequential rationality requirement; 3) we study the equilibrium strategy profiles for both parties based on the belief and expected payoff and reveal the connection between nodes' best response and the cost and gain of each individual strategy; and 4) we present several countermeasures to restrict the flee strategy.

II. RELATED WORKS

The incentives for nodes to cooperate are analyzed and presented in [1]–[3]. However, in these works, malicious nodes are modeled as never cooperative, without any further sophistication, since their main focus was discouraging selfish nodes.

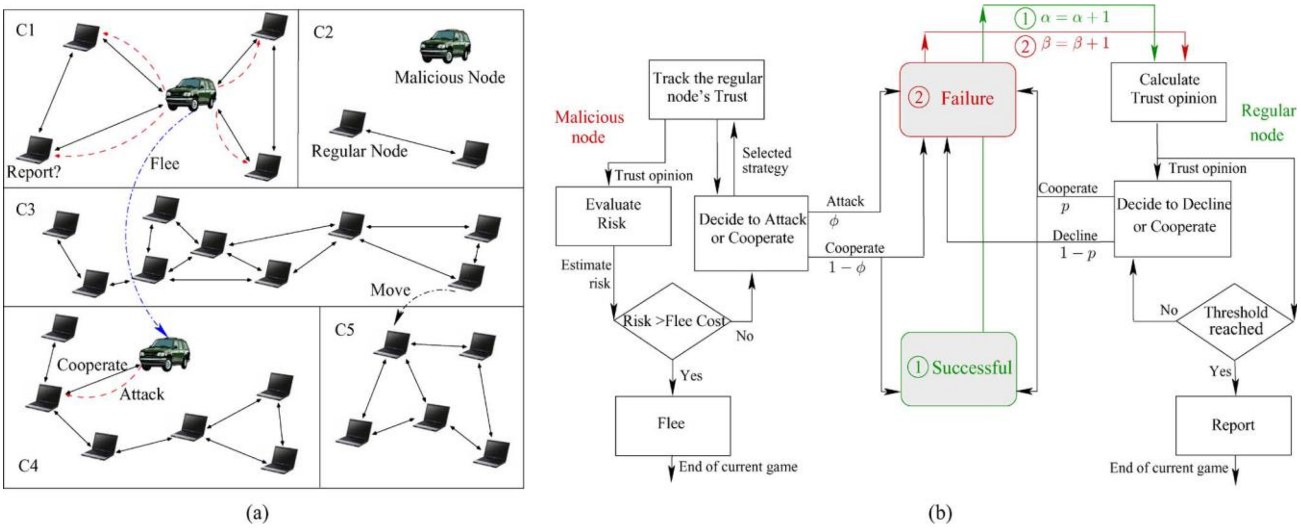


Fig. 1. Wrestling between regular and malicious nodes in MANETs. (a) Example scenario. (b) Decision process.

There is no degree of selfishness that can approximate the behavior of malicious nodes. In this paper, we model the malicious nodes with their own utility functions, which are different from regular nodes. In other words, we assume that malicious nodes are also rational concerning their goals. Some recent works have studied the incentives for malicious nodes and modeled their behavior more rationally.

Cluster:

A *cluster* denotes a logical region of a MANET where nodes are highly connected with each other. The grid in Fig. 1 indicates a cluster. A MANET can always be divided into clusters. Nodes can dynamically leave or join a cluster during their movement. We assume that an authentication method exists and that the identity is bounded with the physical node which cannot be changed or faked during the node's stay in the cluster. When a node first joins a cluster, other nodes in the cluster authenticate the node and set their belief toward the newcomer to the initial value. When a malicious node *flees* (*F*) into a cluster that it has never visited before, nodes in that cluster will treat it as a newcomer. This is because a node's behavior cannot be tracked and the identity binding cannot be monitored outside the cluster.

In essence, the flee strategy leads to a reputation reset. When a regular node decides to *report* (*R*) one of its neighbors as a malicious node, it broadcasts the report in its current cluster. If the report is considered to be true, the malicious node being reported will be punished. Otherwise, the reporting node's accountability will be affected for the false alarm.

Decision Process:

Fig. 1(b) shows the general decision process of regular and malicious nodes. The regular node obtains feedback from the neighbor monitoring and evaluates the belief and sufficiency of evidence toward the opponent based on α and β. It follows a threshold policy to decide whether to report. If not, the regular node chooses C with a probability p, which is calculated based on its belief. The malicious node also evaluates the risk of being caught. It follows its rule to decide whether to flee. If not, the malicious node chooses A with a probability φ. The key issues in this decision process are the decision rules for both parties and the action profiles reflected by p and φ.We analyze theMANET to find the optimal decision rules and action profiles by using the dynamic Bayesian game framework.

Bayesian Signaling Game:

The regular/malicious node game in this paper is a multistage dynamic Bayesian signalling game. *Bayesian games* are the combination of game theory and probability theory that allow taking incomplete information into account. In Bayesian games, each player is allowed to have some private information that affects the progress of the game. Others are assumed to have beliefs about the private information. Players choose their actions during the game according to their beliefs and private information. *Signaling games* are one specific category of Bayesian games. There are two kinds of players in signaling games: senders and receivers. The sender's type is its private information. Based on its own type, the sender chooses to send a message from a set of possible messages. The receiver observes the message but not the type of sender.

Stage games:

Stage games are simple games played at individual time slots. The objective of both regular and malicious nodes is to maximize their expected payoff, which implies that both players are *rational*. The Nash equilibrium for a single stage game given nodes' current beliefs is called *Bayesian Nash equilibrium* (BNE)[3]. For a multistage game, the notion of *sequential rationality* means that a player's strategy should be the best response to others' strategies according to its prediction, and it is what determines the optimality of the subsequent play. Through analysis, we aim to find the *perfect Bayesian equilibrium* (PBE) of this game. PBE is a refinement of BNE. PBE requires that players form beliefs about the opponents' types, update the beliefs, and take the best response actions using these beliefs.

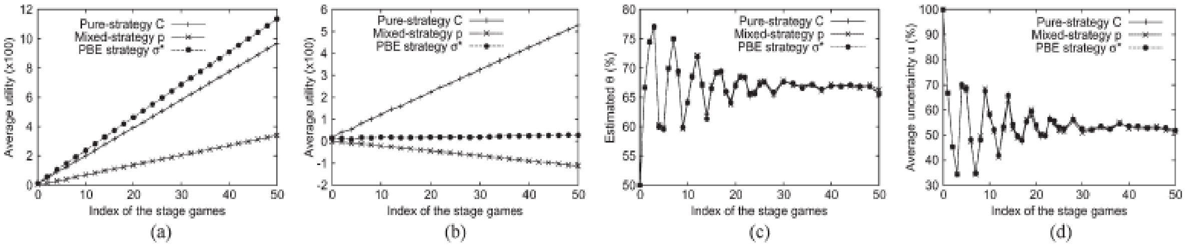
III. PROPOSED SYSTEM

The wrestling between the regular and malicious node is modeled as a dynamic Bayesian game. In this game, nodes observe the result of each round of communication. Each node's type, regular or malicious, is its own private information. The nodes neighbor's actual type is the incomplete information in the game. Each node should form beliefs toward neighbors and update the beliefs according to the neighbors' actions as the game evolves. Both regular and malicious nodes' best are guided by threats about certain reactions from other players. Such threats are dependent on their current beliefs. The regular node sets a reputation threshold and judges other nodes' types based on the evaluated belief and this threshold. The malicious node continuously evaluates the risk, which is decided by the possibility that a regular node would choose to report responses under current conditions. On the basis of the risk and expected fleeing cost, the malicious node makes a decision on fleeing.

The advantages of the proposed system are as follows:

- A Bayesian game framework is formulated to study the strategy of regular and malicious nodes in MANETs.
- Decision rules is proposed for regular nodes to report and malicious nodes to flee, which comply with the sequential rationality requirement.
- The equilibrium strategy profiles for both parties is studied based on the belief and expected payoff and reveal the connection between node's best response and the cost and gain of each individual strategy
- Several countermeasures are presented to restrict the flee strategy.

IV. RESULT ANALYSIS



- A polynomial trend line is used to understand the graphical representation.
- Fig-(a) and Fig-(b). Trend line is almost similar, but a slight deviation on average speed at 5, 6, 7 seconds. Which represents that almost all the normal node and malicious node poses the same behavior with respect to mobility in mobile adhoc network topology, which will provoke the application very difficult situation to distinguish between the normal and attack nodes.
- Fig-© represents encounter of attack nodes with regular nodes. The graph represents very uneven variation proving difficult to predict the encountering strategy of attack nodes in the MANET environment.
- Fig-(d) represents cooperation instances of attack nodes and regular nodes. Comparison proves that malicious nodes tries to duplicate the similar behavior of the regular node. The observation is carried out in 60 second interval. In case of continuing for another cycle of observation, it can be observed that attack nodes have higher tendency of cooperation at the end of each simulation, which indirectly proves the detrimental strategy of infection by the malicious nodes.

V. CONCLUSION

A dynamic Bayesian game framework is used to analyze the wrestling between regular and malicious nodes in mobile networks. The regular node forms belief, chooses the probability to cooperate with its opponent based on its belief, and follows a rational decision rule to report. The malicious node keeps evaluating the risk of being caught and exploits its flee strategy to avoid punishment. The PBE is analysed in this game and emphasize the advantages that malicious nodes would gain from the flee strategy. The future work will focus on multiattacker collusion in the regular/malicious node game and particularly interested in the scenario where attackers can come together in a locality to conduct sophisticated attacks.

REFERENCES

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

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

[4] 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.

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

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

[7] R. Axelrod and W. Hamilton, “The evolution of cooperation,” *Science*, vol. 211, no. 4489, pp. 1390–1396, Mar. 1981.

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

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