Global Journal of Computational Intelligence Research.
ISSN 2249-0000 Volume 3, Number 1 (2013), pp. 1-10

http://www.ripublication.com/gjcir.htm

A Strategic Analysis on Multi Attacker Collusion in MANETs

D. Ravikumar[1], Dr O. Srinivasa Rao[2] and Dr MHM Krishna Prasad[3]

[1]Dept. of IT, JNTUK UCEV, Vizianagaram, A.P., 535 003, India
[2]Assistant Professor & Head, Dept. of CSE, JNTUK UCEV, Vizianagaram, AP, 535 003, India
[3]Associate Professor & Head, Dept. of I. T, JNTUK UCEV, Vizianagaram, AP, 535 003, India
[1]e-mail: dasariravee@gmail.com [2]e-mail: osr_phd@yahoo.com
[3]e-mail: krishnaprasad.mhm@gmail.com

Abstract

The cooperation between the nodes in MANETs is crucial in rendering services successfully without depending on any fixed network topology. The main challenge in mobile ad-hoc networks is their self-organized and distributed nature. In order to achieve the desired functionalities and to address the problem of node mobility the cooperation between participants of ad-hoc networks is required. Collaboration is productive if all participants operate in honest and cooperative manner. Cooperation among players in ad-hoc network has been enhanced by designing several strategies. The vague behavior of the malicious nodes can be modeled using Bayesian game approach. In this paper, we aimed on multi attacker collusion in the regular and malicious player game and modeled a multistage dynamic Bayesian signaling game to find the optimal strategy of the players. We adopted a separate routing protocol which is used to eliminate duplicate packets and digital signatures along the path ensure secured communication.

Keywords: Bayesian signaling game, mobility, reputation, game theory, mobile ad hoc networks, mobility, reputation systems.

Introduction

Ad-hoc networks are self-organized, infrastructure free systems thus providing

an open environment with no existing authority to set trust related constraints. Not all the nodes exhibit normal behavior some of them may be malicious. Apart from being selfish, malicious nodes intentionally aims at harming the network operations. A malicious node can mount attacks to either compromise individual nodes or degrade the performance of the overall network. The operation of ad-hoc networks relies on the contribution of participating nodes. Several strategies were proposed to incite cooperation among the nodes based upon various parameters.

The cooperation among nodes have been enhanced by approaches like incentive based system, barter system and tit-for-tat. The malicious nodes always tend to attack other nodes and alter the data or waste the resources whereas regular nodes maintain normal network operations. We can consider this as a wrestling scenario between the two players. The problem of malicious nodes can be addressed by using game theory approach. The vague behavior of the malicious nodes can be modeled effectively using game theory.

We consider the scenario between the two players as a game. During the game we usually intend to know the strategy of other player. But we always land up in half knowledge about the other player i.e., the strategy of the opposite player is not completely known. At the time of playing we keep monitoring other player in order to design the strategy to follow, it is known as static neighbor monitoring. The malicious node always tends to attack and flees to a new location in order to avoid punishment. So it flees to the other network and starts a new phase with clean history. The regular node cannot report unless it reaches the threshold value of disbelief. Normal players aim to focus their resources on cooperating with regular nodes and do not accept the requests from suspicious neighbors and reports when a neighbor is considered to be malicious.

Both regular and malicious nodes' best responses to the challenges encountered are guided by threats about certain reactions from other players. Such threats are dependent on their current beliefs. In [1] the regular node sets a reputation threshold and other nodes' are judged based on the evaluated belief and this threshold. This analysis may be on self assessment or on second hand reputation basis. The malicious node continuously evaluates the risk of being caught, which is decided by the possibility that a regular node would choose to report under current conditions.

On evaluating the risk and expected fleeing cost, the malicious node decides to flee or not. The Bayesian strategy works for single attacker problems i.e., when we find a single attacker along a path. The same approach may not work effectively when multiple attackers collude to exploit the network resources. The colluded attackers drop the packets and do not update their neighbor statistics. They conceal their behavior from the neighbors to maximum extent and disrupt the network operations. The neighboring nodes may not assess the loss of data at an early stage.

By using the path signature approach during the communication at node level we can address the problems that arise due to this collusion attack. The

contributions of this paper are as follows: 1) we simulate the multi stage game for multiple and single attacker scenarios of regular nodes to report and malicious nodes to flee 2) we use path signature by applying cryptographic techniques at node level and analyze how they are used effectively to encounter multi player collusion attack. Instead of using the traditional approaches like reputation based system, we have used path signature concept and node level security in order to achieve maximum utility and to address the problem of multi attacker collusion.

II. Related work

The Bayesian strategy of the game theory is used to efficiently encounter single attacker and multiple individual attackers. In general those attackers will not cooperate with each other so the strategy of every attacker is independent of each other. The payoff for players to cooperate are analyzed and presented in [1]–[3]. The malicious players are structured as never cooperative, since their main motive is to discourage players which are abnormal. As we know that the good players' behavior [5] is simple, and it cannot assume the possibility that an attacker can choose different attacking techniques toward different strategies depending upon the requirement [10]. The attitude of malicious players cannot be approximated by any degree of measurement. In this paper, we have modeled the malicious players with their own functions of utility, which will be different from regular players. In other sense, we will assume that malicious players are also rational concerning their goals.

The malicious player's behavioral strategies are simulated depending on their payoffs. We model the situation as multi stage game and identify its impact on the network topology. We consider malicious players, making the malicious and regular players' game in this paper more and more interesting. Game theory [6] is a powerful tool in modeling interactions among self-interested players and to predict their choice of strategies [7]–[10]. The wireless ad hoc networks [7]–[10] are more often studied using game theory because of the fuzzy strategies followed by the players [10]. The PBE strategy is not effective in the multi collusion attacker model, for this we have used path signature method which addresses security problem at node level in order to ensure trusted communication.

III. Basic model and assumptions

Somehow the single attacker model may not create serious threats in the data transmission, so this will give flexible and even at times equal probability to attack or flee. Not all the times it is possible to predict the strategy of the attacker based on the probability constraints. In order to overcome these limitations there is a need to introduce sophisticated technique to effectively encounter multi attacker collusion.

To specify the collusion attacker we need to consider conditional probability as well as likelihood of the player's strategy. According to the conditional probability we can verify the strategy of a player for given class where class indicates the evidence already accumulated and the representation is given by P(x|c). In the above representation (x) specifies strategy of current player and (c) represents the total strategies in the game. Likelihood specifies the behavior of a given class. In this paper we are applying condition probability and likelihood between players i.e., to what extent the level of support coming from other player.

Based on this assumption we can divide the players into two groups 1) one group specifies high transmission error rate and 2) other group specifies high packet delivery ratio. Based on the probability in the error transmission group we can also say that those players are playing the game with cooperation. This will be treated as collusion attacker with respect to the high transmission error group. To achieve this we need to monitor and record the activities of each player throughout the game. If the player is a new comer in the game then there is a need to find the likelihood of the player. Likelihood calculation involves behavioral analysis of the player so that there is a need to verify the players approach against the available strategy.

Apart from the pure probability theory there is a need to provide cryptographic solution for path security. We need to incorporate digital signature for the strategy of every player as well as digital signature for the control packets. Every time we are reading route request and route reply we need to verify the signature of those packets. This is very much useful when the attackers try to introduce wormhole attack in the given path.

- Watchdog strategy: By exploring the nature of broadcast intercommunication in wireless network, players will track the outgoing packets from one-hop neighbors through passive observation. But, a player will be able to differentiate whether a failure in communication is caused by its opposite players' attack or decline.

Therefore, by detailed observation we can classify a given move as either a detected cooperation or a detected attack/decline. The corresponding discrete variable namely (α) for detected cooperation and (β) for detected attack/decline, will be incremented. This mechanism is called Watchdog strategy. In practical the detection process has many challenges in MANETs. First, the malicious player can disguise itself. Second, the unreliability of the wireless channel brings more uncertainity to the observing process. The scheme which ignores the noise in the observation may not be practical in the actual wireless intercommunication. We assume that the bugs in the observation will occur with low probability or else it would be impossible to distinguish a malicious player by neighbor monitoring. By this we update the belief and disbelief parameters from time to time.

- Player strategy: We analyze the nodes in MANET to find the best

decision rules and action by using the dynamic Bayesian game framework in the process of regular and malicious player game scenario. The regular player obtains feedback from its neighbors by observing and calculates the belief and sufficiency of evidence toward the opposite player based on α and β values. It follows threshold rules to decide whether to report or not. If not the regular player will choose C with a probability p, which is calculated based on its belief. The malicious player calculates the risk of being caught. It evaluates the risk and decides whether to flee or not depending on the threshold. The malicious player chooses to attack with a probability ϕ if the threshold is not reached.

- Bayesian Signaling game: A dynamic signaling game has two players in general they are the sender and the receiver. The senders' type is his private information. Depending on the knowledge of his own type, the sender picks a message from a pool of possible messages to deliver. The receiver observes only the message but not about the senders' type. Then the receiver chooses an action from a set of feasible actions available. The two players' utility depends on the senders' type, the message chosen by the sender and the possible action chosen by the receiver. A strategic game is designed where the receiver gives the sender proposals based on its type and do not choose an action based on the signal. Here we can play the game by evaluating the upcoming scenario based on the previous information gathered i.e., designing strategies with unclear information.

The optimal decision rules for both malicious and regular can be best described by the Bayesian approach. The connection between the best strategy profile and the cost and gain of individual strategies is revealed using this approach. The PBE strategies of both regular as well as malicious nodes are summarized apart from that an enhanced approach is designed to address multi attacker collusion.

The complete strategy profiles of regular and malicious nodes are considered in general to initialize the moves of the player strategy. We consider the above parameters and update their values as the game progresses. At the beginning of the game all parameters are set to their initial values. With every detected cooperation and decline, α and β values are updated respectively. All the basic parameters used were taken from the single attacker model of the Bayesian approach in [10]. The neighbor evaluation parameters like uncertainty, belief and disbelief are changed as the game progresses to the other stages. Apart from that the probability of detected attack and regular node cooperation are updated.

- Path security: The malicious behavior can be addressed to a maximum extent by verifying the authenticated user before a message transfer. At first for a message transfer between source to destination a route request is generated and by one hop method the route is detected and during the process each node adds its signature to the message passed from its

predecessor to the successor and the route is traced back and in this process if any node drops a packet then the signature is not available and it can be detected as a malicious event. The duplicate message transfer problem is also addressed in order to save network resources. The message id is stored in a table along with the node data and a message with same id is not transferred to the node again.

Algorithm:
/* Route establishment from source to destination*/
Begin
Step 1: Initialize the process at src_node
Step 2: Repeat
Add the signature of the present node and send it to the next hop address along with route _request
Update the routing table
Until(pre_node!=des_node)
Step 3: Now initialize the process at des_node and generate route _reply
Step 4: Repeat
Add the signature of the present node and send it to the previous address along with route _reply
Verify the previous signature with present one
If any node drops the message in between then goto step 6
Update the routing table
Until(pre_node!=src_node)
Step 5: The signature is verified and the route_reply reached the src_node and a secured path is established.
Increment α (Detected cooperation)
Calculate U and report node i as regular node. Goto End.
Step 6: The signature is not verified and the route reply doesn't reach the source node.
Increment β (Detected decline or attack)
Calculate U and report node i as malicious node.
End

IV. Simulation and Result Analysis

We simulate the entire scenario to evaluate the regular and malicious nodes' single and multi attacker game strategy and the above scenario is designed as a multi stage game.

- Simulation Setup: The proposed strategies have been implemented and compared on a custom discrete event simulator. Randomly generated MANETs are used to conduct all simulations. The regular node can track its neighbor's outgoing packets by neighbor monitoring. One hundred nodes are placed in random manner over a 900 m ×900 m region which is evenly divided into nine clusters. The range of transmission is 250 m.

Any two nodes within the same cluster are considered neighbors. Nodes follow the cluster based mobility model is considered for nodes. Any node can move from cluster Cx to Cy with probability Pxy.

- Comparison with previous schemes: We compare the performance of the proposed scheme with that of the previous schemes. The comparisons are made with single attacker vs. multi attacker and found the results were much better with multiple attackers than single attacker as shown in the table 1.2 the proposed approach of multiple attackers is compared with previous Bayesian approach for single attacker scenario.

The utility of the node during various levels of belief and disbelief conditions are considered. These parameters are considered for both single and multi attacker collusion approaches. Furthermore the path security and node level security implementation shows its impact on the result as we can see both single and multi attacker situations show much similar results. The introduction of the security at the node level helps us to transfer the data to the destined user without any malicious intervention in an easy manner.

The complexity depends upon the key value used. And the digital signature implementation enables us to find a secure path between source and destination, any obstacle results in the termination of data transfer. This ensures that the multi collusion attack can be encountered successfully when compared to the Bayesian approach. The path security method is also used to enhance cooperation among the players.

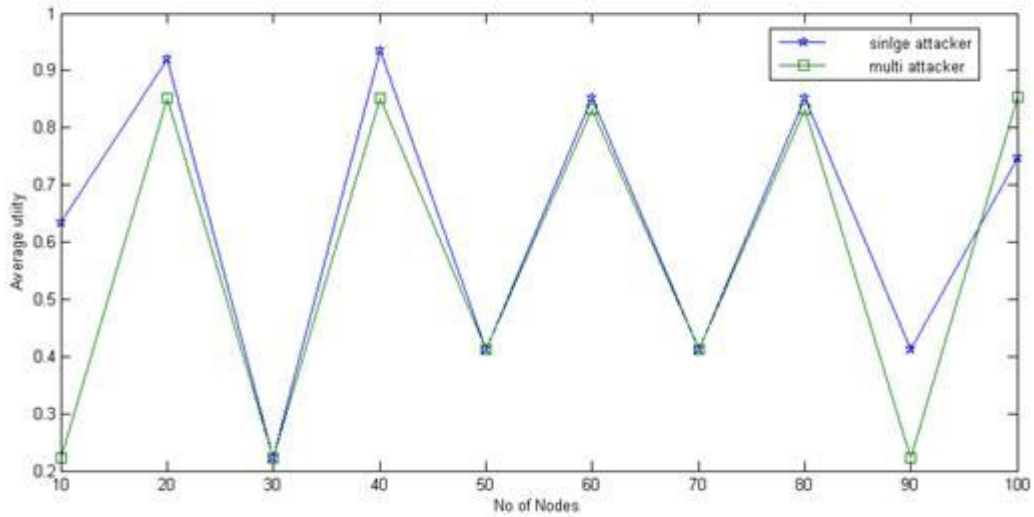

Fig 1.1 shows the comparison between the belief of single attacker and multi attacker.

Table 1.1 shows belief values of single and multi attacker scenario

No of nodes	Belief values of multi attacker	Belief values of single attacker
10	0.222	0.634
20	0.852	0.919
30	0.222	0.222
40	0.852	0.936
50	0.412	0.412
60	0.833	0.852
70	0.412	0.412
80	0.833	0.852
90	0.222	0.412
100	0.833	0.747

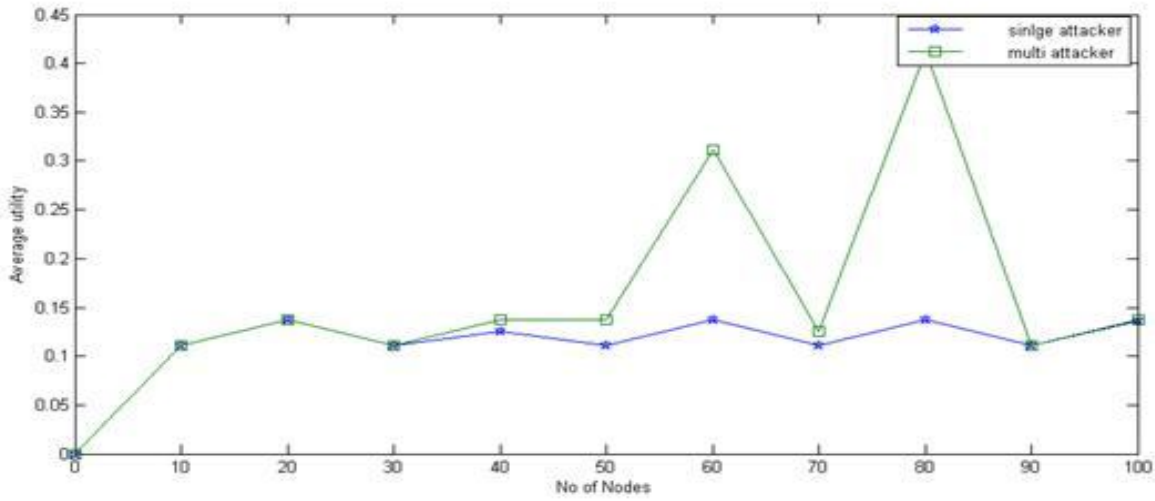

Fig 1.2 shows the comparison between the disbelief of single attacker and multi attacker.

Fig 1.2 shows the comparisons of disbelief of single attacker with respect multi attacker. From the graph we can analyze that the average utility of the node is more when applied path security method with multi attacker mode compared to the single attacker Bayesian scenario. This analysis tells us that the proposed method is much more sophisticated and efficient when compared to the traditional one.

Table 1.2 shows disbelief values of single and multi attacker scenario.

No of nodes	Disbelief values with multi attacker	Disbelief values with single attacker
10	0.111	0.111
20	0.137	0.137
30	0.111	0.111
40	0.137	0.126
50	0.137	0.111
60	0.312	0.137
70	0.126	0.111
80	0.412	0.137
90	0.111	0.111
100	0.137	0.137

V. Conclusion

The stingy behaviors of the players degrade the performance of the overall network. They tend to attack other nodes and disturb normal functionality of the network. Our analysis on the multi attacker collusion shows that the path security method yields better results when compared to the Bayesian strategy. One can further enhance by introducing much sophisticated approaches in key selection and the accuracy can be increased by introducing probability like decision tree classification of data mining to predict behavior of the players.

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] 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.

[3] 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.

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

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

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

[7] 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.
[8] S. Sarkar, E. Altman, R. El-Azouzi, and Y. Hayel, “Information concealing games, ” in Proc. IEEE INFOCOM, 2008, pp. 2119–2127.
[9] F. Li and J. Wu, “Hit and run: A Bayesian game between malicious and regular nodes in mobile networks, ” in Proc. IEEE SECON, 2008, pp. 432–440.
[10] Feng Li, Member, IEEE, Yinying Yang, Student Member, IEEE, and Jie Wu, Fellow, IEEE "Attack and Flee: Game-Theory-Based Analysis on Interactions Among Nodes in MANETs", in Proc. IEEE Cybernetics, 2010, pp. 612-622.