Multi Attacker Collision Analysis in MANETs using Conditional likilihood

Nitta Rajkiran

Received: 14 December 2012 Accepted: 31 December 2012 Published: 15 January 2013

Abstract

Mobile ad hoc networks will aim to provide services to the wireless network without depending on any fixed infrastructure There are basically two approaches to motivate players: 1) by denying service to misbehaving players by means of a reputation mechanism or 2) by remunerating honest players, using for example a micropayment scheme. In these works, malicious players are modelled as never cooperative, without any further sophistication, since their main focus was discouraging selfish players. There is no degree of selfishness that can approximate the behaviour of malicious players. This work will focus on multi-attacker collusion in the regular/malicious player game. The Proposed System also model the regular/malicious player game as a multistage dynamic Bayesian signalling game to find the optimal strategy of regular and malicious players. Apart from that utility function, degree of selfishness of a player and degree of uncertainty are also considered.

Index terms— bayesian signaling game, game theory, mobile ad hoc networks (MOBILE AD HOC NETWORKS), mobility, reputation systems, sequential rationality, uncertain

1 Introduction

anets is the self organizing nature without relaying on any fixed infrastructure. The beautiful nature of the mantes is their topology is dynamic. They do not fallow any fixed topology in nature. As we know that in the network their two kinds of nodes. Malicious nodes other are regular. The malicious nodes always tend to attack other nodes and alter the data or waste the resources. We can consider this as a wrestling scenario between the two. There are so many approaches to find the malicious nodes. But we have taken the game theory to find the malicious nodes because game theory is the study of wrestling between the nodes. In the game theory everything is probality based. We shall be considering the scenario between the two players as a game. At the time of playing the game we usually intend to know 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, that concept is called as baysion signalling game. At the time of playing we keep mentoring other players, that concept is know is neighbouring monitoring. As we malicious nodes always tend to attack and keep fleeing to avoid punishment. So what it does is it goes to the other network and attack or Author : Computer Science/M.Tech Bangalore, 560097, India. E-mail : rajkiran8630@rediffmail.com cooperate with the other nodes at some point i.e. is the threshold point the malicious nodes get caught. Normal players will aim to focus with their resources on cooperating with regular nodes and do not accept the requests of from suspicious neighbouring and keep reporting when the neighbouring is considered to be malicious. Both regular and malicious nodes' best responses are guided by threats about certain reactions from other players. [1] Such threats are dependent on their current beliefs. [1] The regular node sets a reputation threshold and judges other nodes' types based on the evaluated belief and this threshold. [1] The malicious node continuously evaluates the risk, which is decided by the possibility that a regular node would choose to report under current conditions. [1] On the basis of the risk and expected fleeing cost, the malicious node makes a decision on fleeing. [1] The contributions of this paper are as follows: 1) We had theorized a Bayesian game framework to understand and study the strategy of regular and malicious nodes in MANETs; 2) we will be simulating it for multiple and single attacker for regular nodes to report and malicious nodes to flee [1].

2 II.

3 Related Work

In the existing work most of the game theory is based on single attacker and multiple individual attacker. So in general those attackers will not cooperate with each other so the strategy of every attacker is independent of other. In the existing work most of the game theory is based on single attacker and multiple attacker. So in general those attackers will not cooperate with each other so the strategy of every attacker is independent of other. The payoff for players to cooperate are analyzed and presented in [1]- [3]. Well, in this works, malicious players are structured as never cooperative, since there main motive is to discouraging players which are stingy. As we know that the good players' behaviour in [5] is simple, and it fails to consider the possibility that an attacker can choose different attack frequencies toward different opponents depending upon the requirement [26]. There can be no degree of stingy that can approximate the attitude of malicious players. In this, we have modelled 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. In recent works we studied the payoff for malicious players and simulated their behaviour more rationally. In [4], Liu et al. present a general incentivebased method to model the attackers' intents, objectives, and strategies. In [5], Theodorakopoulos and Baras further study the payoff of the malicious players and identify the influence of 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 modelling interactions among self-interested players and predicting their choice of strategies [7]- [10]. Therefore, wireless ad hoc networks [11]- [13] are more often studied using game theory [26]. The equilibrium of the contention window game is studied in [13] [26]. In the previous work they have simulated for single attacker using the PBE strategy with other strategy and found that PBE works much better compared to other. But in the current work we have taken same PBE strategy for multiple attackers and found that belief, disbelief and uncertainty is much efficient to find the malicious nodes by comparing with single attacker [26].

4 III.

5 Proposed Model

Some how this type of attacker model may not create to serious theats in the data transmission so this will give flexi able sometimes equal probality to attack or flee. Because of probality it is not possible to predict the strategy of the attacker. If the attacker drops problity is equal to overcome these limitations there is a need to introduce cryptographic technique as well as considerations of multiple collisions attackers model.

To specify the collision attacker we need to consider conditional probity as well as lo likili hood of the player's strategy. According the the conditional probility we can verify the strategy of a player for given class where class indicates the evidence already we having so there reprentation is given by P(x|c). In the above representation x specifies strategy of current player and c represents the total strategic the game. Likili hood specifies for given behaviour to a given class. In this paper we are also applying condition probility and likilihood between players also by applying the condition probility between the two players specifies what the level of support coming from other player is. Based on this assumption we can divide the player into two groups 1) specifies high transmission error rate and other group specifies high packet delivery ratio. Based on the probility in the error transmission group we can also say that those players are playing the game with cooperation. This will be treated as collision attacker with respect to the high transmission error group. To achieve this there is need to monitor and record the activates of each players throughout the game. If the player is a new comer in the game than is a need to find the likilihood of the player. Likili hood calculate involves behaviour of the player so that there is a need to verify the behaviour against the available strategy.

Apart from the pure probility theory there is a need to provide cryptographic solution for path security. We need to incorporate digital signature for the strategy of a 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 very much useful when the attackers are try to introduce wormhole attack in the given path. a) Neighbour Observing By exploring the nature of broadcast intercommunication in wireless network, players will track the outgoing of packets from one-hop neighbours through passive observation. But, a player will able to differentiate whether a failure in communication is caused by its opposite player A or D [26]. Therefore, an detail observation will be classified as either a detected C or a detected A/D. The correspond discrete variable namely ? for detected C and ? for detected A/D, will be incremented as shown in Fig. **??**(b). This mechanism is called neighbour monitoring [24] [26]. In practical MOBILE AD HOC NETWORKs, the detection process has challenges. First, the malicious player can disguise itself. Second, the unreliability and the wireless channelizes bring more uncertain to the observing to the process [26]. The schemes which ignore 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. Else it would be impossible to distinguish a malicious player by Neighbour observing.

6 b) Decision Reckon

We analyze the MOBILE AD HOC NETWORK to find the best decision rules and action by using the dynamic Bayesian game framework Fig. ??(b) shows the process of regular and malicious players to take decision. The regular player obtains feedback from its neighbor observing and calculates the belief and sufficiency of evidence toward the opposite player based on the ? and ? values. It follow 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 [26]. The malicious player calculates the risk of being caught. It follows rule to decide whether to flee or not depending on the threshold. If else, the malicious player chooses A with a probability ?.

7 c) Bayesian Signalling Game

A signaling game is a dynamic, Bayesian game with two players, the sender (S) and the receiver (R). The sender has a certain type, t, which is given by nature. [1] (The sender observes his own type while the receiver does not know the type of the sender. [1] Based on his knowledge of his own type, the sender chooses to send a message from a set of possible messages M = {m 1 ,

8 Global Journal of Computer Science and Technology

Volume XIII Issue III Version I The equilibrium concept that is relevant for signaling games is Perfect Bayesian equilibrium. Perfect Bayesian equilibrium is a refinement of Bayesian Nash equilibrium, which is an extension of Nash equilibrium to games of incomplete information. Perfect Bayesian equilibrium is the equilibrium concept relevant for dynamic games of incomplete information) ??1] [26].

9 Figure 1(b)

By seeing the above block diagram we can find the flow of the game. In the above diagram first the regular node decides to cooperate or not if it fails to do so Beta value will be incremented else alpha value will be incremented if it alpha it will calculate the trust if the threshold is reached it will be reporting else the process keeps continuing else if it is a malicious nodes it will tracks the regular node trust and evaluate the risk of being caught and it estimates the risk i.e. if the risk is greater than flee cost than it will flee else it will attack. at last end of the game.

The PBE of this game describes the optimal decision rules for both regular and malicious players and reveals the connection between the best strategy profile and the cost and gain of individual strategies [26]. From the discussion, we can summarize player j's PBE strategy ?*j as strategy profile 1. The regular type player i has the same PBE strategy profile as j, and the PBE strategy ?*i of malicious-type player i is listed as strategy profile [26].

V.

10 Experimental Results and Analysis

All proposed have been implemented and compared on a discrete event simulator. All simulations are conducted in randomly generated MOBILE AD HOC NETWORKs. The regular player can track its neighbor's outgoing packets by neighbour monitoring. We have taken 10 players to 50 players and made 10 iterations for each player are randomly placed in a 900 m ×900 m region which is evenly divided into clusters. The transmission range is 50 m. Any two players within the same cluster are considered as neighbours. Players follow the cluster based mobility model [25]. It shows this mobility model for players in Fig. ?? m 2 , m 3 ,..., m j } [1]. The receiver observes the message but not the type of the sender. Then the receiver chooses an action from a set of feasible actions A = {a 1 , a 2 , a 3 ,...., a k }. The two players receive payoffs dependent on the sender's type, the message chosen by the sender and the action chosen by the receiver. A related game is a screening game where rather than choosing an action based on a signal, the receiver gives the sender proposals based on the type of the sender, which the sender has some control over ??1] [26].

11 VI. Comparison with Previous Schemes

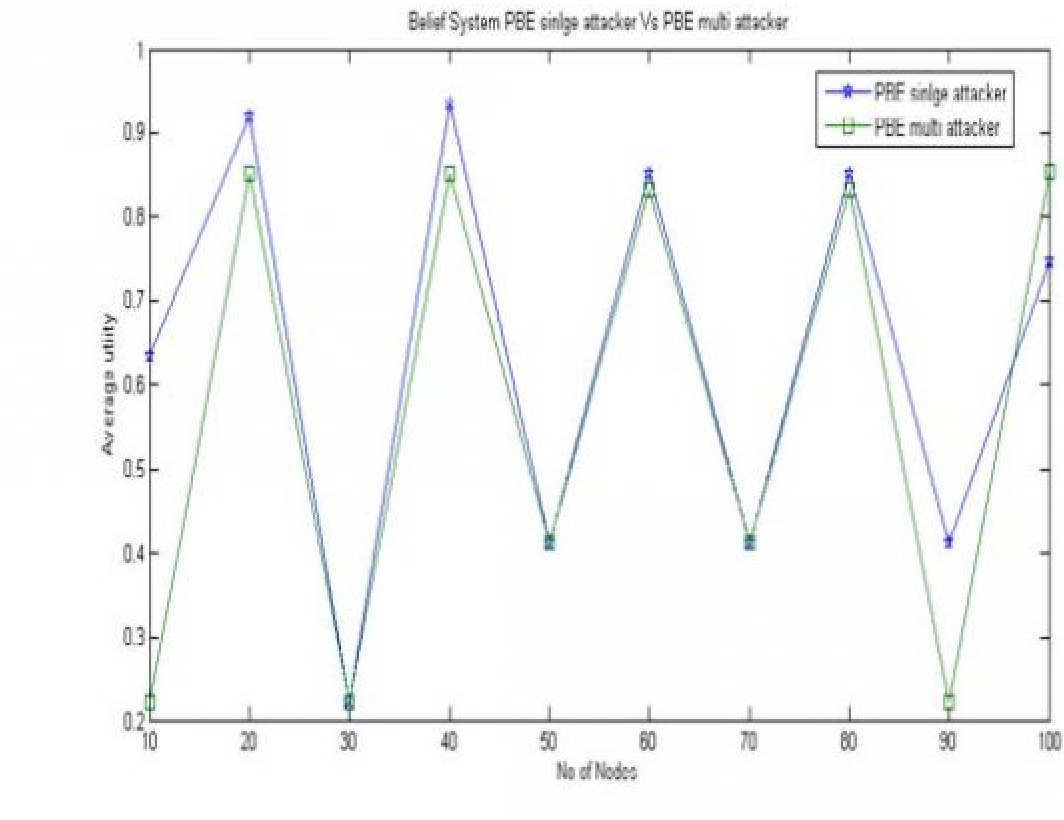
In this section, we compare the performance of the proposed scheme with those for the previous schemes, namely Yinying Yang [25], Jie Wu [25]. The comprations are made with single attacker vs multiple attackers and found the results were much better with multiple attackers than single attacker as shown in the table 2 the proposed approach of multiple attackers is compared with previous approaches. Table ?? Figure 2 : Shows the comparations with single attacker with multi-attacker The values in the above table taken by considering the belief system of multi attacker and single attacker and found that graph 3 for belief system for multi attacker increases but the graph for the single attacker slowly decreasing with respect of nodes and the graph is plotted which is show in the fig 2.

Table 2

[1]

2

Figure 1: 2 E



3

Figure 2: Figure 3 :

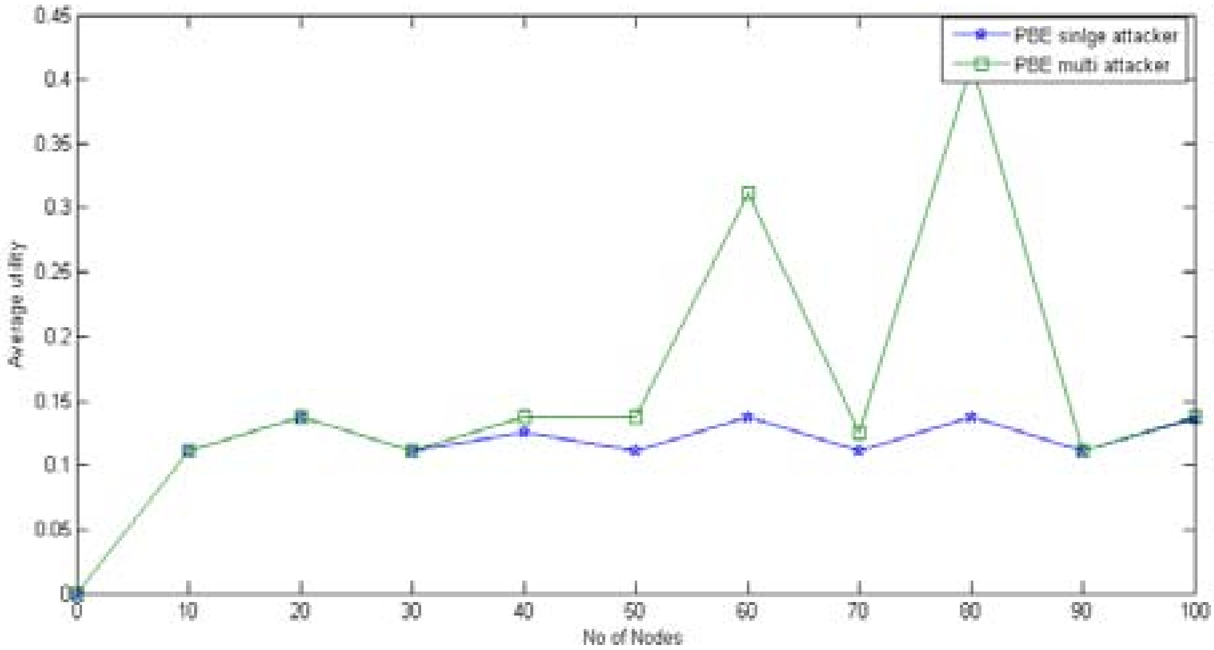


Figure 3:

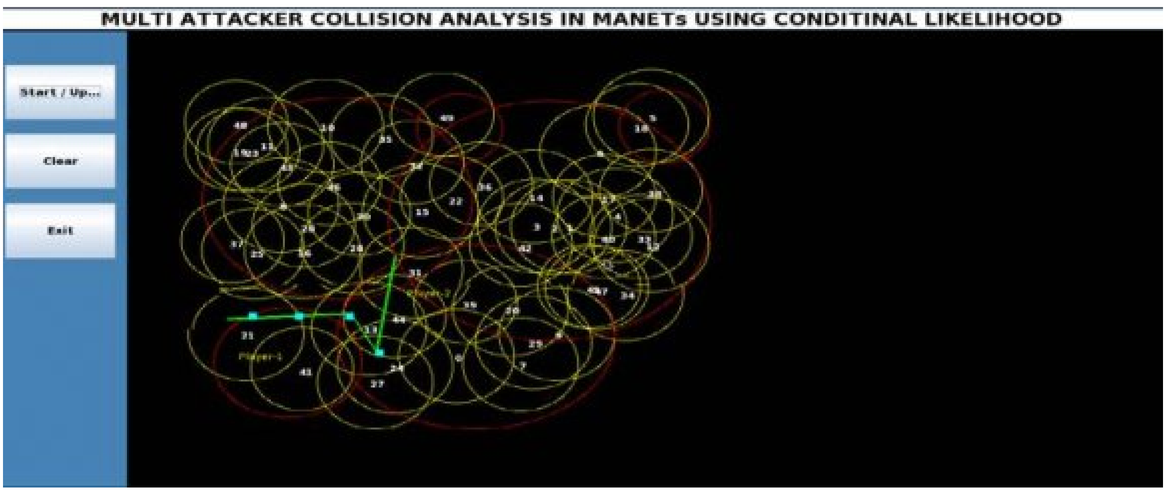


Figure 4:

.1 Screen Shots

The above pic its shows the screen shots for 100 nodes simulated on the JNS In the above screen shots it shows the values taken at the time of iteration

.2 VII. onclusion

The proposed system is simulated in java network animator and found that the results were good and efficient compared to the previous approach. In this paper, there is need to enhance the by introducing probality decision tree classification of data mining to predict behaviour of the players to increase the accuracy.

.3 Global Journals Inc. (US) Guidelines Handbook

www.GlobalJournals.org

[Fudenberg et al. ()] , D Fudenberg , J Tirole , Game Theory . 1991. Cambridge, MA: MIT Press.

[Decis. Support Syst (2007)] , *Decis. Support Syst* Mar. 2007. 43 (2) p. .

[Liu et al.] 'A Bayesian game approach for intrusion detection in wireless ad hoc networks'. Y Liu , C Comaniciu , H Man . *Proc. ACM Game Nets*, (ACM Game Nets) p. 4.

[Nuggehalli et al.] *A game-theoretic analysis of QoS in wireless MAC*, P Nuggehalli , M Sarkar , K Kulkarni , R Rao .

[Buchegger and Boudec ()] 'A robust reputation system for P2P and mobile ad-hoc networks'. S Buchegger , J Boudec . *Proc. 2nd Workshop Econ. Peer-to-Peer Syst*, (2nd Workshop Econ. Peer-to-Peer Syst) 2004. p. .

[Josang et al.] *A survey of trust and reputation systems for online service provision*, R Josang , C Ismail , Boyd .

[Li et al.] 'Attack and Flee: Game-Theory-Based Analysis on Interactions among Nodes in MANETs'. Feng Li , Yinying Yang , Jie Wu . *Proc. IEEE*, (IEEE)

[Srinivasan et al. ()] 'Cooperation in wireless ad hoc networks'. V Srinivasan , P Nuggehalli , C Chiasserini , R Rao . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) 2003. p. .

[Michiardi and Molva ()] 'CORE: A collaborative reputation mechanism to enforce player cooperation in mobile ad hoc networks'. P Michiardi , R Molva . *Proc. Commun. Multimedia Secur*, (Commun. Multimedia Secur) 2002. p. .

[Blanc et al. ()] 'Designing incentives for peer-to-peer routing'. Y Blanc , A Liu , Vahdat . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) 2005. p. .

[Ng and Seah ()] 'Game-theoretic model for collaborative protocols in selfish, tariff-free, multihop wireless networks'. S Ng , W Seah . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) 2008. p. .

[Li and Wu ()] 'Hit and run: A Bayesian game between malicious and regular players in mobile networks'. F Li , J Wu . *Proc. IEEE SECON*, (IEEE SECON) 2008. p. .

[Liu et al. (2005)] 'Incentive-based modeling and inference of attacker intent, objectives and strategies'. P Liu , W Zang , M Yu . *ACM Trans. Inf. Syst. Secur* Feb. 2005. 8 (1) p. .

[Sarkar et al. ()] 'Information concealing games'. S Sarkar , E Altman , R El-Azouzi , Y Hayel . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) 2008. p. .

[Theodorakopoulos and Baras ()] 'Malicious users in unstructured networks'. G Theodorakopoulos , J Baras . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) 2007. p. .

[Marti et al. ()] 'Mitigating routing misbehaviour in mobile ad hoc networks'. S Marti , T J Giuli , K Lai , M Baker . *Proc. ACM MobiCom*, (ACM MobiCom) 2000. p. .

[Li and Wu ()] 'Mobility reduces uncertainty in MOBILE AD HOC NETWORKs'. F Li , J Wu . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) 2007. p. .

[Hsu et al. ()] 'Modeling timevariant user mobility in wireless mobile networks'. W Hsu , T Spyropoulos , K Psounis , A Helmy . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) 2007. p. .

[Felegyhazi et al. (2006)] 'Nash equilibria of packet forwarding strategies in wireless ad hoc networks'. M Felegyhazi , J Hubaux , L Buttyan . *IEEE Trans. Mobile Comput* May 2006. 5 (5) p. .

[Altman et al. ()] 'Non-cooperative forwarding in ad hoc networks'. E Altman , A Kherani , P Michiardi , R Molva . RR- 5116. *INRIA* 2004. (Tech. Rep.)

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

[Buchegger and Boudec ()] 'Performance analysis of the confidant protocol'. S Buchegger , J Boudec . *Proc. ACM MobiHoc*, (ACM MobiHoc) 2002. p. .

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

[Liu et al. ()] 'SPREAD: Foiling smart jammers using multi-layer agility'. X Liu , G Noubir , R Sundaram , S Tan . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) 2007. p. .

[Buttyan and Hubaux (2003)] 'Stimulating cooperation in self-organizing mobile ad hoc networks'. L Buttyan , J Hubaux . *ACM Mobile Netw. Appl* Oct. 2003. 8 (5) p. .

[Axelrod and Hamilton (1981)] 'The evolution of cooperation'. R Axelrod , W Hamilton . *Science* Mar. 1981. 211 (4489) p. .

[Li et al. ()] 'Uncertainty mitigation for utility-oriented routing in MOBILE AD HOC NETWORKs'. F Li , A Srinivasan , M Lu , J Wu . *Proc. IEEE GLOBECOM*, (IEEE GLOBECOM) 2007. p. .