An Overview of Game Theoretic Approach to Intrusion Detection System in MANETs

Bobby Sharma

School of Technology, Dept. of CSE & IT, Assam Don Bosco University
Email: Bobby.sharma@dbuniversity.ac.in

Abstract-Mobile ad hoc networks (MANETs) are a collection of mobile nodes that communicates over wireless media. Performance of MANET depends on the cooperative participation of nodes in packet forwarding. During packet forwarding from source to destination, it takes help of middle hop depending on the distance. Middle hops play different role in different times. Nodes in MANETs suffer from limited resources specially battery power. To save its resources, middle hop acts like selfish node in which nodes are simply dropping packets instead of forwarding the same to its neighbor. Malicious nodes drop packets maliciously instead of forwarding them to destination. Performance parameters of network are effected by malicious behavior of nodes. Intrusion detection system (IDS) are designed to detect malicious nodes. Some of these IDS suffer from some arbitrariness. Game theoretic approach helps to remove these arbitrariness from the IDS and to define the equilibrium state of the network. Objective of this paper is to discuss the game theory in MANETs and also to discuss about game theoretic approach to detect malicious nodes in MANETs.

Key words-MANETs, IDS, game theory, selfish node, packet forwarding, malicious node.

I. INTRODUCTION

Game theory can be identified as mathematical model of conflict and co-operation amongst intelligent rational decision makers [14].Though game theory is basically a part of mathematics and it is used vastly in economics; still it can be used in any other field of application. It explains the study of mathematical models of conflict and co-operation between decision makers. It is an interactive decision situation which is represented by mathematical model. Game theory can be modeled to MANETs nodes which are autonomous but interdependent of rational decision makers. In order to maintain multi hop network like MANETs, nodes must forward packets to next hop [18]. Performance of MANETs depends on node cooperation. Nodes in MANETs are restricted from energy consumption. While forwarding packets, node consumes its own resource, specially the battery power. Hence to compensate the same, incentive must be provided to nodes to cooperate the process of packet forwarding. Repeated interaction amongst the nodes is necessary to provide relative incentive to get smooth service [19]. To invoke nodes for packet forwarding, reputation based system may also be called [20] [21]. In [18], author says that under specific conditions, cooperation is availed without reputation or incentive based process. Non cooperative nature of nodes may collapse the network which is similar to Prisoner's Dilemma Game (PDG) of game theory [19]. Packet forwarding dilemma of MANETs can be addressed by game theory of applied mathematics to resolve the problem of conflict and cooperation [22]. It provides a process to formulate the problem with strategic scenarios to analyze and understand.

Section II of this paper contains overview of game theory, section III contains classification of games, section IV of this paper contains MANETs and game theory, section V contains definition of utility function while section VI contains game theoretic approach and IDS. Section VII contains the conclusion.

II. GAME THEORY

Game theory which is a part of applied mathematics deals with strategic interactions among multiple decision makers. It is implemented in a situation in which decision makers are under mutual confliction to take decision. A well defined utility function plays vital role in game theory. Utility function must be proposed based on which decision makers promote their choices.

III. CLASSIFICATION OF GAMES

Game theory in MANETs is specially modeled to remove arbitrariness from different problem solver [24]. Based on participation of players in the game, it is either 2-player game or n-player game, with n>2. Depending on cooperation of nodes, payoffs and strategies of players, game can be classified as follows:

In non cooperative game, players take the decision independently. Each player follows their strategy to achieve goal individually. Players try to increase their own individual payoffs in the game. It is a competitive game that played amongst different players for their individual benefits [25].

In cooperative game, multi-players cooperate with each other to achieve highest benefit. Set of strategies are available for the players and there must be some payoffs for each possible strategies. Players form coalition amongst them, individual player contributes to the coalition to increase the overall utility of coalition.

The coalitional game theory tries to find the player's optimum strategies with an objective to fulfill common goal. Outcomes of a coalition are the set of all feasible payoffs for the coalition members. Total outcome is distributed amongst the players in case of transferable payoff game. But in case of non transferable game, usually nodes think of their individual benefit with common objective.

In sequential and simultaneous move games, players take their decision sequentially. Players are aware about the strategies of other players and their moves are observable. Each player has the knowledge about the decision of a player who moves ahead of it. Such games require strategic interaction in terms of player's current move.

In Zero-Sum game, the total payoffs of all the players are equal to zero at the end of the game. Such games are competitive as decision is taken in such a way that total win-total loss of the players is deduced.

IV. MODELING MANETS AS GAME

Game theory has been implemented in MANETs and cellular network to solve several problems [9].

Models of cooperation in MANETs can be classified as credit based model and trust model. Credit based model is based on economic incentive while trust based model is based on reputation [26]. To encourage the nodes for cooperation in packet forwarding, two basic mechanisms are followed. One is reputation based mechanism and other is price-based mechanism. In reputation based mechanism, any node keeps a record of its neighbor's reputation. The more cooperative a node is the better reputation it gains. In price-based mechanisms, the loss that a cooperative node makes is compensated by some kind of virtual money. The price of relaying a packet may be different. Therefore, an effective price-based mechanism should be supplemented by a technique which determines the price accurately.

Non cooperative game theory can be applied to MANETs for forwarding packets; Nodes are also involved in cooperation aware routing protocol [27][4]. A non cooperative game may contain the elements such as number of players, objective function of each player for which it tries to optimize utilities, preference, utility, actions, strategies etc [138].

Normally a game may contain the following Components:

- players
- actions
- strategies
- information
- outcomes
- payoffs
- Equilibrium concept

Goals of players are articulated by utility functions and utility is defined over outcomes. Actions and strategies can be defined as follows:

- Any plan or steps for performing some actions are known as strategy.
- In some cases, actions and strategies are taken as equivalent.

But in some cases both actions and strategies are granted differently. In such cases strategies are recognized as primary choice of actions.

- The payoff for each player depends on the combined actions of all players.

Strategic game consists of three main basic components,

- A set players (N = {1,2,….n}) where N>=2
- A set of actions for each player
- Utility function for each player

MANETs components can be set as equivalent game components as follows:

Player Set: Basically player sets in MANETs implies different nodes that participated in communication in the network including packet forwarder, attacker and some other categories of nodes.

Action set: Nodes may act as,

a. Source i.e. sender

b. Destination i.e. receiver

c. Forwarder

d. Attacker

e. Attack detector etc.

f. Game strategies

In game theory, there may be infinite numbers of strategies [11]. Nodes in MANETs may follow any of the strategies. Accordingly plan should be generated. Some examples are given below:

a. Always defects (AIID) : Nodes with this strategy are assumed that these are always defective

b. Always cooperate (AIIC): Nodes with this strategy always start with cooperation

c. Tit-for-Tat (TFT): Nodes with this strategy are very unreliable as they start with cooperation but gradually they mimic the behavior of their opponent.

d. Suspicious Tit-for-tat (S-TFT): In this strategy, behavior of nodes is suspicious. It needs strong monitoring system to understand the behavior of the nodes.

e. Anti Tit-for-Tat (Anti-TFT): Here, behavior of the nodes is exactly opposite to the behavior of its opponents.

V. UTILITY FUNCTION

Utility function plays prime role in game theoretic approach. Each player in the game tries to increase their utility. Based on the value of utility function, overall utility of the network can be determined. A game with complete information implies that each player knows the facts about the game such as set of players, strategies and utility functions. Of course, set of complete information always doesn't mean that these are complete information.

In both cooperative and coalition game, it considers the cooperative actions of number of players and then analyze the results accordingly. It is also a kind of strategic game, as all the players have the idea about their strategies; they make the outcome of the game based on their decision. Solution of a strategic game is either Nash equilibrium or stability. It is the point from which no other players want to deviate unilaterally.

Nash equilibrium:

Most of the game cannot be solved by iterated dominance technique [7]. In Nash Equilibrium, an action vector reaches an equilibrium point in such a way that no player can be benefited by deviating unilaterally. It occurs when each player is pursuing their best possible strategy in the full knowledge of the other players' strategies. In Nash equilibrium, both the players maximize their payoffs [1]. As a result none of the player changes its strategy to increase its payoff. Hence it is a strategy profile with best responses of the players [7][8]. The game achieves at least a Nash equilibrium that leads to a defense strategy for the defender [10]

VI. GAME THEORETIC APPROACH AND IDS

Notion of game theory can be utilized in the current scenarios for intrusion detection system in MANETs. It also assists in defining and reconfiguring security policies [23].

In [10], author proposed a realistic model with the help of Bayesian game to model the interaction between IDS (Intrusion detection system) and attacker(malicious nodes). Author also solved the game by Bayesian Nash equilibrium and by that they have shown that proposed IDS work intermittently without compromising its effectiveness. It is modeled in such a way that the interaction between IDS and attacker is one stage game and it has two Bayesian Nash equilibrium. It is also modeled as multi staged game. In this scenario, author said that IDS doesn't have any fixed prior probabilities about its opponent and can update its assumption or belief after each stage of the game and also showed that this game has a mixed strategy with perfect Bayesian equilibrium. There is no cooperation between the two players namely intruder and detector. Author also considers that an IDS needs not be running all the time during which the wireless ad hoc network is up. Proposed game theoretic approach is a kind of multi-stage game, where IDS does not have fixed prior probabilities about the type of its opponent and can update its belief at the end of each stage of the game.

In [11], Though in most cases, it is found that to have cooperation of nodes in MANETs, nodes must be benefitted either by incentive or by gaining payoffs. But in this paper, author addresses a system in which cooperation is expected without incentives. Based on game theory and graph theory, a model is proposed to investigate packet forwarding equilibrium conditions. Equilibrium conditions are proved in this paper for both cooperative and non cooperative strategies. The condition for cooperation is derived from the topology as well as from the existing routes. Author considers the static network only. From this paper, author generated one conclusion i.e. as cooperation solely based on self-interest of nodes can in theory only. However, it is concluded that there may be some nodes that have AIID(Always Defect) as their best strategies and these nodes always expect incentives to cooperate. Of course such kind of properties effects only a small part of the network.

In [13], author provides a novel game theoretic incentive mechanism for network congestion control in context of selfish user. Scenario had been articulated as M/M/I queuing game with each user. Optimization had been used to find throughput and delay. An incentivizing packet dropping scheme had been proposed to improve the outcome efficiency with throughput-delay tradeoffs. The utility function had been defined in terms of throughput and delay and it is defined as power which is widely used in gateway congestion control context.

$$\text{Power}=(\text{Throughput})^{\alpha i} / \text{Delay} \text{------}(1)$$

where αi is a parameter chosen based on the relative emphasis placed on throughput versus delay. $\alpha i > 1$ when throughput is more important, while $0 < \alpha i < 1$ when it wants to emphasis delay more, and $\alpha i = 1$ when the throughput and delay are emphasized equally.

In [22], author mentioned that though IDS has been utilized in detection and response strategies, still finding an effective policy and to find the right balance between them is also an issue. IDS sensitivity and false alarm rate are also equally important. The system may wish to have a response strategy even after getting a satisfactory solution. Traditional intrusion detection systems are not enough to have complex detection and response system. There must be a logically formalized system which will be able to detect and response in a better way.

In [8], author mentioned that existence of selfish nodes, threat the applicability of MANETs. So, to mobilize the flow of data, author proposes a novel price based method for stimulating the cooperation of nodes as nodes cooperation is must for MANETs to get better communication. It utilizes a game theoretic approach to distribute the earnings of a cooperation coalition among the nodes.

VII. CONCLUSION

Performance of MANETs depends on cooperation of nodes. Cooperation depends on self interest of nodes. Malicious nodes try to decrease the network performance. Though several IDS had been proposed to detect malicious node, but to have an effective policy to eliminate malicious nodes and to increase network performance, game theoretic approach is essential. Nodes try to increase their payoff or they need incentives to cooperate. Objective of this paper is to show MANETs as game space in which malicious nodes are in one side of the game. Malicious nodes always try to decrease the network utility. Any other nodes other than malicious nodes try to increase the network performance. Utility function plays major role in the game theory. At Nash equilibrium, an action vector reaches an equilibrium point in such a way that no player can be benefited by deviating unilaterally. At this point, both the player maximizes their payoffs.

REFERENCE

[1] Emmanouil A. PANAOUSIS and Christos POLITIS, "Non-Cooperative Games Between Legitimate Nodes and Malicious Coalitions in MANETs," Future Network and MobileSummit 2011 Conference ProceedingsbPaul Cunningham and Miriam Cunningham (Eds)bIIMC International Information Management Corporation, 2011 ISBN: 978-1-905824-23-6

[2] Marcela Mejiaa,_, N´estor Pe˜naa, Jose L. Mu˜nozb, Oscar Esparzab, Marco A. Alzatec, "A Game Theoretic Trust Model for On-Line Distributed Evolution of Cooperation in MANETs," Preprint submitted to Journal of Network and Computer Applications (JNCA)

[3] Chiranjeeb Buragohain, "Game Theory in Ad Hoc Networks"

[4] Luiz A. DaSilva and Allen B. MacKenzie, "Cooperation in Ad Hoc Networks: A Game-theoretic Approach," WICAT Workshop on Cooperative Communications New York, NY – 21 October 2005

[5] Tamer Ba_sar, "Lecture Notes on Non-Cooperative Game Theory", July 26, 2010

[6] Diman Zad Tootaghaj, Farshid Farhat, Mohammad-Reza Pakravan, Mohammad-Reza Aref, "Game-Theoretic Approach to Mitigate Packet Dropping in Wireless Ad-hoc Networks,"

[7] Mark Felegyhazi, Jean-Pierre Hubaux, "Game Theory in Wireless Networks: A Tutorial,"

[8] Azadeh Omrani and Mehran S. Fallah, "A Game-theoretic Cooperation Stimulus Routing Protocol in MANETs," IAENG International Journal of Computer Science, 35:1, IJCS_35_1_23

[9] Dr B. Paramasivan and K. Mohaideen Pitchai, "Comprehensive Survey on Game Theory based Intrusion Detection System for Mobile Adhoc Networks," IJCA Special Issue on "Network Security and Cryptography" NSC, 2011

[10] Hua Wei, Hao Sun, "Using Bayesian Game Model for Intrusion Detection in Wireless Ad Hoc Networks," Int. J. Communications, Network and System Sciences, 2010, 3, 602-607 doi:10.4236/ijcns.2010.37080 Published Online July 2010 (http://www.SciRP.org/journal/ijcns/).

[11] Mark Felegyh´azi, Jean-Pierre Hubaux and Levente Buttyan, "Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks," IEEE transactions on mobile computing

[12] Qishi Wu, Sajjan Shiva, Sankardas Roy, Charles Ellis, Vivek Datla, "On Modeling and Simulation of Game Theory-based Defense Mechanisms against DoS and DDoS Attacks"

[13] Yi Gai, Hua Liu, and Bhaskar Krishnamachari, "A Packet Dropping-Based Incentive Mechanism for M/M/1 Queues with Selfish Users," This research was sponsored in part by the U.S. Army Research Laboratory under the Network Science Collaborative Technology Alliance, Agreement Number W911NF-09-2-0053, and by the U.S. National Science Foundation under CNS-0831545.

[14] Luiz A. DaSilva and Allen B. MacKenzie, "Game Theory and MANETs: A Brief Tutorial"

[15] Yongkang Xiao, Xiuming Shan And Yong Ren, "Game Theory Models for IEEE 802.11 DCF in Wireless Ad Hoc Networks," IEEE Radio Communications • March 2005, 0163-6804/05/$20.00 © 2005 IEEE

[16] Y. Liu, C. Comaniciu, H. Man, "Modeling Misbehavior in AdHoc Networks: A Game Theoretic Approach for Intrusion Detection," Copyright °c 200x Inderscience Enterprises Ltd

[17] Dr B. Paramasivan and K. Mohaideen Pitchai "Comprehensive Survey on Game Theory based Intrusion Detection System for Mobile Adhoc Networks," IJCA Special Issue on "Network Security and Cryptography" NSC, 2011

[18] M´ark F´elegyh´azi, Jean-Pierre Hubaux and Levente Butty, "Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc

Networks," IEEE TRANS-ACTIONS ON MOBILE COMPUTING

[19] Charles A. Kamhoua, Niki Pissinou, Alan Busovaca And Kia Makki, "Belief-Free Equilibrium Of Packet Forwarding Game In Ad Hoc Networks Under Imperfect Monitoring," IEEE, 2010

[20] L. Butty´an and J.-P. Hubaux, .Stimulating Cooperation in Self Organizing Mobile Ad Hoc Networks,. in ACM/Kluwer Mobile Networks and Applications (MONET) Special Issue on Mobile Ad Hoc Networks, Vol. 8 No. 5, October 2003.

[21] P. Michiardi and R. Molva, .Core: A COllaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks,. Communication and Multimedia Security 2002, Portoroz, Slovenia, September 26-27, 2002.

[22] Anis Alazzawe, Asad Nawaz and Murad Mehmet Bayraktar, "Game Theory and Intrusion Detection Systems," ISA 767 Secure E-Commerce, Spring 2006

[23] Vesal Hakami and Mehdi Dehghan "Cognitive Forwarding Control in Wireless Ad-Hoc Networks with Slow Fading Channels,"

[24] Javidi M.M. and Aliahmadipour L., "Game theory approaches for improving intrusion detection in MANETs," Scientific Research and Essays, Vol. 6(31), pp. 6535-6539, 16 December, 2011

[25] I. A. Shah, S. Jan, I. Khan and S. Qamar, "An Overview of Game Theory and its Applications in Communication Networks," International Journal of Multidisciplinary Sciences And Engineering, VOL. 3, NO. 4, APRIL 2012, [ISSN: 2045-7057]

[26] Ricardo Puttini, Ludovic Mé, Jean-Marc Percher and Rafael de Sousa, "A Fully Distributed IDS for MANET," Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on 2004, Vol. 1, Page(s):331-338, Print ISBN:0-7803-8623-X, INSPEC Accession Number:8230035

[27] Marcela Mejiaa, Nestor Penaa, Jose L. Munozb, Oscar Esparzab and Marco A. Alzatec, "A Game Theoretic Trust Model for On-Line Distributed Evolution of Cooperation in MANETs," Preprint submitted to Journal of Network and Computer Applications (JNCA)