Game Theoretic Inventive Mechanism for Shielding Collaborative Wireless Network

Seema U. Purohit, Venkatesh Mahadevan, Shruti D. Mantri, and Devank. U. Purohit

***Abstract*—In this paper, the researchers have presented a Game Theoretic model for identifying bad or malicious users in a collaborative wireless network. Objective of the malicious users is to damage the collaborative wireless network. To bind the damage caused Game theory provides an inventive mechanism. The proposed approach helps in obtaining optimal wireless network. The model is based on graphical representation and repeated graphical games with incomplete information. The framework is applicable to any general network topology.**

***Index Terms*—Collaborative networks, incomplete information, repeated game.**

I. Introduction

A. Collaborative Wireless Network

A wireless network is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. Basic components of a Wireless network are access points (APs), nodes, base stations, Network Interface Cards (NICs), client adapters and server. As wireless network evolve they move towards decentralization in which each node plays multiple roles at different situations without relying on a best station or access points to make decision. It is characterized by distributed, dynamic, self organizing architecture. These characteristics lead to the need of distributed decision that takes into account the network and channel conditions. An individual node may need to have access to control information regarding other nodes actions, network congestion etc. Each node in the network is capable of adopting its actions / operations based on the current environment independently, providing a distributed and dynamic environment for wireless networks.

In the absence of centralized control each node is free to choose its actions in a legitimate or selfish or malicious way. For the successful working of network the perfect understanding and collaboration among the users is needed.

The term "Collaboration" if defined in terms of following certain protocols and sharing of resources and expenditure incurred on these resources in an environment, the phrase "Collaborative Networks" refers to addressing the issues in such environment.

Manuscript received May 21, 2012; revised June 26, 2012.

S. U. Purohit is with Department of Mathematics, Kirti College and Department of Technology and Mgmt, NMITD, Mumbai, India (e – mail: supurohit@gmail.com)

V. Mahadevan is with Information Systems & eBusiness, Swinburne University of Technology, Melbourne, Australia. (e–mail: vmahadevan@swin.edu.au)

S. D. Mantri is with Department of CS & IT, Kirti M. Doongursee College, Mumbai, India .(e - mail: shrutimantri@gmail.com)

D. U. Purohit is with Dept. of Applied Mathematics, DIAT (DU), Girinagar, Pune, India (e - mail:devank.purohit@gmail.com)

B. Need of Secure Collaborative Wireless Network

In dynamic environment users communicate and collaborate with one another with a greater extent. As per the course of action chosen the main three types of network users are: legitimate users, selfish users, malicious or bad users; who work in this collaborative environment. Among them malicious users are motivated and more knowledgeable than the average legitimate users and are always ready to take the advantage of the collaborative environment in which legitimate users work. Any strategy, best practice, or protection mechanism used by the legitimate user is compromised by the malicious ones, and exploited within no time. Hence we need a secure wireless network when it comes to working in collaboration.

C. Importance of Game Theory for Wireless Network

An ad hoc wireless network is a self-configuring, multihop network in which there is no central authority. Thus, every aspect of the configuration and operation of an ad hoc network is completely distributed. As mentioned before furthermore, nodes are often severely energy and power constrained. In emerging wireless networks, such as sensor networks, mesh networks, and pervasive computing systems, many of these same features - decentralized operation, self configuration, and power/energy awareness - are often desirable.

The requirement of dynamic distributed environment of collaborative wireless network is provided by Game theory, which is a study of the interaction of autonomous agents. In a modern wireless network, each node running a distributed protocol must make its own decisions (possibly relying on information from other nodes). These decisions may be constrained by the rules or algorithms of a protocol, but ultimately each node will have some flexibility in setting parameters or changing the mode of operation. These nodes, then work as autonomous agents, making decisions about transmit power, packet forwarding, back off time, and so on. In making these decisions, the node may seek to optimize the following: (a) The "greater good" of the network as a whole (b) Behave selfishly, looking out for only their own user's interests (c) Behave maliciously, seeking to ruin network performance for other users. In the second and third cases, the application of game theory may be straightforward, as game theory traditionally analyzes situations in which players objectives are in conflict. In the first case, node objectives may be aligned (as all players seek the "greater

good" of the network), but game theory may still offer useful insights. Even when nodes have shared objectives, they will each have a unique perspective on the current network state, leading to possible conflicts regarding the best course of action. Thus, the promise of game theory as a tool to analyze wireless networks is clear: By modeling interdependent decision makers, game theory allows us to model scenarios in which there is no centralized control with a full picture of network conditions.

D. Review of Related Literature

Over the years researchers have tried their level best to devise the strategy or game plan to handle the attacks on collaborative networks. The use of game theory in modeling dynamic situations for ad hoc networks where nodes have incomplete information has led to the application of largely unexplored games such as games of imperfect monitoring.

The existing model use tree games with incomplete information, i.e., the graph of the game is a tree structure and the players have private information, but there is no history (the game is not repeated). They provide algorithms for finding approximate Bayesian-Nash equilibrium. In the literature for inducing cooperation among network users, the stress is mostly given on selfish users, where incentives are provided for users to cooperate [1], [2]. However, they are presenting/modeling malicious users as "Never Cooperative" users. For example, in [3],[4] the authors assume that the payoff function of a user is non-decreasing in the throughput experienced by the user. Bad malicious users do not care about their data being transmitted. In other related work; a modified version of Generous Tit for Tat technique is used (for an early famous paper in the history of Tit for Tat see [5]), but they have no concept of topology and, consequently, of neighborhoods. In their setting, each user is comparing his frequency of cooperation to the aggregate frequency of cooperation of the rest of the network. In [6], a scheme is proposed for punishing users whose frequency of cooperation is below the one dictated by certain Nash equilibrium. Researchers have aimed particularly against free-riding in wireless networks in [7],[8]. Though malicious users are modeled in [9] in a different way; game theoretic modeling of malicious users is still an open problem. They have considered a virus inoculation game, in which selfish users decide whether to pay the cost for installing anti-virus software (inoculation), or not pay and risk getting infected. The malicious users declare that they have been inoculated, when in fact they have not, so as to mislead the selfish ones. After the selfish users have made their decisions, the attacker chooses an uninoculated user, uniformly at random, and infects him The infection propagates to all unprotected users that can be reached from the initially infected users on paths consisting of unprotected users (the malicious ones are equivalent to unprotected). One major difference is that in this model the selfish users are supposed to know the topology of the network (a grid, in particular), whereas in the proposed adoption of game theoretic model they only know their local neighborhood topology. The proposed model is inspired by the pioneering work done in [10].

II. Problem Definition

The mathematical formulation of the proposed model is given as follows: The network is considered as an undirected graph $G = (V, E)$ where each node in V corresponds to one user. Denote the legitimate users as "good users" and malicious users as "bad users". An edge connecting two nodes indicates a communication link between two users. Let V_b and V_g denote a set of bad users and good users respectively.

$$\Rightarrow V_b \cap V_g = \varnothing,\ V_b \cup V_g = V$$

Type $t_i \varepsilon\{G, B\}$ denotes whether a user is good or bad. The users have 2 choices: C (for cooperate) and D (for defect/ non - cooperate). Each user receives a payoff that depends upon his own action and neighbor's action. Payoff of a user i is denoted by when i's action is and i's type is. When j is neighbor of i, payoff of i is denoted by $R_i(a_i\ a_j \mid t_i\ t_j)$. So, the decomposition of i's payoff along each adjacent link can be written as

$$R_i(a_i \mid t_i) = \sum_{j \in N_i} R_i(a_i a_j \mid t_i\ t_j) \quad (1)$$

Or

$$R_i(a_i \mid t_i) = \sum_{j \in N_i} R_i(a_i a_j \mid t_i) \quad (2)$$

when i's payoff does not depend on the types of his neighbours. With the assumption that there are no links between two bad users the objective is to develop a mathematical frame work which will depict the interaction between the good and bad users in collaborative networks by considering a general case of star topology, where

1. The central good user will have more than one bad user neighbours, but will not know the exact number.
2. Good user will have different number of good and bad user neighbours.

Eventually, with this frame work good user will be able to detect all bad user neighbors and upon discovering a bad user, good user will be able to break the link that joins them, thus altering the game graph.

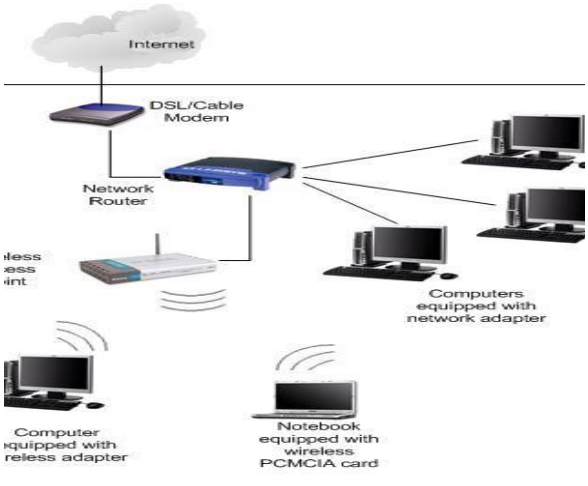

Fig. 1. Wireless network made up of

III. Methodology Adapted

A. Construction of Undirected Graph

An undirected graph $G = (V, E)$ is created representing a star topology with the nodes in a wireless network. An edge connecting two nodes indicates a communication link between two users.

B. Integrated Framework

The strategy used for developing the model uses four major steps:

1) *Identifying the set of Bad users and Good users:* We first identify a set $V_b = \{v_{b1},\ldots,v_{bn}\}$ of Bad users and a set $V_g = \{v_{g1},\ldots,v_{gn}\}$ of Good users from the set of all users $V = \{v_1,\ldots,v_n\}$. Type *1)* $t_i \in$ denotes whether a user is Good or Bad.

2) *Selection of Choice:* Users have a choice between two actions: C (for Cooperate), and D (for Defect). A C means that a user makes himself available for communication that is, forwarding traffic of other. A link becomes active (i.e., data is exchanged over it) only when the users on both endpoints of the link cooperate, that is, play C. when both players on a link play C, the Good player (or both players, if they are both Good) receives N (for Network) minus E (for Energy) for a total of $N - E$. On the other hand, when a Good player plays C and the other player D, then the Good player only wastes his energy since the other endpoint is not receiving or forwarding any data. The payoff is then only $-E$. When all users choose their actions, each user receives a payoff that depends on his own and his neighbors' actions, and his own and his neighbors' types.

3) Detection of bad users: We need to identify bad users, as good users want to cooperate with other good users, but

4) not with bad users. bad users, on the other hand, want to cooperate with good users. We consider a star topology network where central node is a Good user and his neighbors are "N" good users and one bad users. Assume that the central Good user i has memory of the past history (own and neighbor moves, as well as received payoffs). Let CN^t_i be the subset of i's neighbors that play C at round t. We assume that i plays C at round t, so i's payoff at round t is $|CN^t_i|$ if the Bad user played D, or $|CN^t_i| - 2$ if the bad user played C (Remember that a C from a good user gives +1, whereas from a bad user it gives −1.). So, just by looking at his payoff, the central good user i can deduce whether the bad user played C or D at round t. The bad user is then known to be either in the set $CN^t{}_i$ or in $DN^t i$ Without loss of generality, let's assume that the Bad user played C. In the next round (t + 1), if the Bad user plays C again, Then i can deduce that he is in the intersection $CN^t{}_i \cap CN^{t+1}{}_i$. If he plays D, then he is in $CN^t i \cap DN^{t+1}{}_i$.

5) Calculation of payoff: The payoff is decomposed as a sum of payoffs, one term for each adjacent link. Each term of the sum depends on the user's own action and type, and the action of his neighbor along that link. User i's payoff along each adjacent link is calculated as explained in (1) After the Bad user has been detected, the link to him is severed and the Good nodes are free to play C forever.

IV. Findings

A. Game Theory Model

In a star topology, the central good user has more than one bad neighbor. . At each observation, the central good user will know how many bad neighbors played C at that round. As a heuristic, the good users can play C in the first round, which would disclose immediately how many bad neighbors each good user has. Later, by suitable randomization, the bad users will definitely be detected: At the very least, in some round the central good user will play C and all other good users will play D so the bad users who play D at that round will be detected. Also, in a general topology each good user will have a different number of good and bad neighbors, so the optimal cooperation probabilities will be different for each good user. Even then, however, we claim that, as long as there is randomization in the actions of the good users, they will eventually be able to detect all the bad ones.

B. Technology

For this research a wireless network made up of access points and base station in a star topology is considered. Base station is considered as the central good user surrounded by good users and Bad users.

C. Software Customization

The model is customized to make it user friendly, interactive using MATLAB. User friendly graphics and symbols have been used where ever necessary. The project windows contain interface and command buttons. New node can be added as well as the existing node can be removed. The methodology has been customized in above mentioned solution for user friendly interface and easy implementation.

V. Conclusion

This paper tackles identification of Bad users in a wireless network. Taking a general case of star topology by making suitable randomization and different combinations of choices C and D, the model ultimately becomes capable of detecting the bad users. A future objective is to develop a general network topology game theory model that identifies and quantifies the tradeoff between malicious users' knowledge and their equilibrium payoffs.

References

[1] A. Blanc, Y. K. Liu, and A. Vahdat, "Designing incentives for peer-to-peer routing," Presented at Proceedings IEEE Infocom 2005, Miami, FL, March 2005.

[2] L. Buttyán and J. P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," *ACM/Kluwer Mobile Networks and Applications*, vol. 8, no. 5, 2003.

[3] M. Félegyházi, J. P. Hubaux, and L. Buttyán, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 5, pp. 463–476, May 2006.

[4] A. Urpi, M. Bonuccelli, and S. Giordano, "modelling cooperation in mobile ad hoc networks: a formal description of selfishness," in *Proceedings WiOpt 2003: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, INRIA Sophia-Antipolis, France, March 2003.

[5] R. Axelrod, and W. D. Hamilton, "The evolution of cooperation," *Science*, vol. 211, no. 4489, pp. 1390–1396, March 2002.

[6] E. Altman, A. Kherani, P. Michiardi, and R. Molva, "Non-cooperative Forwarding in Ad Hoc Networks," INRIA, Tech. Rep. RR-5116, 2004.

[7] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Sustaining cooperation in multi-hop wireless networks," in *Proceedings 2nd Networked Systems Design and Implementation (NSDI)*, Boston, MA, May 2005.
[8] M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica, "Free-riding and whitewashing in peer-to-peer systems," in *Proceedings 3rd Annual Workshop on Economics and Information Security (WEIS04)*, May 2004.
[9] T. Moscibroda, S. Schmid, and R. Wattenhofer, "When Selfish Meets Evil: Byzantine Players in a Virus Inoculation Game," in *Proceedings 25th Annual Symposium on Principles of Distributed Computing (PODC)*, Denver, Colorado, USA, July 2006.
[10] G. Theodorakopoulos and J. S. Baras, "Game Theoretic Modeling of Malicious Users in Collaborative Networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 7, pp. 1317-1327, September 2008.

Dr. S. Purohit, born in Ahmadabad, India on 8th August 1962. She has received M.Sc. degree in Applied Mathematics and Ph. D. in Computational Mathematics in 1990 from University of Mumbai and working as a Professor in Kirti M. Doongursee College and Director, NMITD, Mumbai. Her specializations include Research methodology and research based teaching and learning techniques. Currently she is working on problems in Artificial Intelligence, Optimization, Simulation and Mathematical Modeling and published and presented her work in International Conferences and referred Journals including IEEE explorer. She is a Research Guide for doctoral students in the subject of Computer Science, Information Technology and Management. She is an educational consultant and is an active member contributing to curriculum designs. Dr. Purohit is a Senior Member of IACSIT, Singapore, MIR LABS, USA, IEEE, WIE, and CSI, India.

Dr V. Mahadevan has received a B.E. in Electrical and Electronics Engineering in 1989 form Institution of Engineers, India , M.E. in Computer Systems Engineering in 1997 form University of Auckland, New Zealand Ph. D. in E – business Technology in 2007 form University of Sydney, Australia and has an extensive research experience
in the different phases of the usability design lifecycle, from user research, requirement specifications and conceptual design through to usability attributes testing of a Tele-collaboration (TC) business system. He has joined the Faculty of Higher Education, Lily-dale as Lecturer in Information Systems (IS) and e-Business. He has presented his research findings at several national and international conferences and workshops. He is Founder Chair of Forum for Telecommunications Networking Simulations (using OPNET, OMNeT++ etc) at UTS. Cross-institutional Coordinator for Telecommunications Networking Simulations for the Technical University of Budapest (Hungary) at UTS . He worked as a Director and senior member of IACSIT Sydney Chapter and Chennai (India) Chapter. He is an Editorial Board Member, Australian Journal of Information Systems (JIS) and ICTACT Journal of Communication Technology (ICTACTJCT). Dr. Mahadevan is a Member of IEEE (SIG - Society on Social Implications of Technology) , Association of Information Systems (SIG - E-Business) , International Association for Development of Information Society (IADIS), International Consortium for Electronic Business (ICEB) , Human Capital Institute (HCI) , Sydney Networks Interested Research Forum (Sydney), Institution of Engineers (India) .

S. D. Mantri born in Mumbai, India on 25th July 1978. She has done her M.Sc. in Physics with specialization in Electronics and Telecommunication from University of Mumbai, India in the year 2001. The author has then acquired her Master of Philosophy in Information Technology from Yeshwantrao Chavan Open University, India in the year 2009. The author is currently pursuing Ph. D. in Computer Science from University of Mumbai, India. She has worked as a summer trainee with Indian Register of shipping and then as a software programmer with the Datamatics Technologies. She then worked as a Lecturer with Department of Computer Science, K.C. College, Mumbai, India. She is currently working as an Asst. Professor, Department of Computer Science and Information Technology, Kirti M. Doongursee College, Mumbai, India. Ms. Mantri is a member of IACSIT and MIR LABS, USA.

D. U. Purohit born in Mumbai, India on 17th September 1987. He has received Bachelor of Engineering (B. E.) degree in Electronics and Telecommunication from K. J. Somaiya College of Engineering affiliated to the University of Mumbai, Mumbai, in 2009. He is currently pursuing Master of Technology (M. Tech.) in Modeling and Simulation at Defence Institute of Advanced Technology (Deemed University), Pune, an autonomous organization fully funded by Department of Defence Research and Development, Ministry of Defence, Government of India. He is currently working on game theoretic approach to dynamic spectrum allocations in cognitive radio networks, as a final year M. Tech. dissertation. His research interests include application of game theory to wireless communication networks, digital signal processing, cognitive radio networks, discrete event simulation, statistical modeling. Mr. Purohit is an IEEE member.