Computer Networks 71 (2014) 63–83

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A game theoretic approach to detect and co-exist with malicious nodes in wireless networks ☆

Wenjing Wang [a], Mainak Chatterjee [b,*], Kevin Kwiat [c], Qing Li [a]

[a] Blue Coat Systems, Inc., Sunnyvale, CA, United States
[b] EECS, University of Central Florida, Orlando, FL, United States
[c] Air Force Research Laboratory, Rome, NY, United States

ARTICLE INFO

Article history:
Received 12 February 2013
Received in revised form 19 May 2014
Accepted 14 June 2014
Available online 26 June 2014

Keywords:
Malicious node
Game theory
Coexistence
Bayesian games
Markov Bayes–Nash Equilibrium

ABSTRACT

Identification and isolation of malicious nodes in a distributed system is a challenging problem. This problem is further aggravated in a wireless network because the unreliable channel hides the actions of each node from one another. Therefore, a regular node can only construct a belief about a malicious node through monitoring and observation. In this paper, we use game theory to study the interactions between regular and malicious nodes in a wireless network. We model the malicious node detection process as a Bayesian game with imperfect information and show that a mixed strategy perfect Bayesian Nash Equilibrium (also a sequential equilibrium) is attainable. While the equilibrium in the detection game ensures the identification of the malicious nodes, we argue that it might not be profitable to isolate the malicious nodes upon detection. As a matter of fact, malicious nodes can co-exist with regular nodes as long as the destruction they bring is less than the contribution they make. To show how we can utilize the malicious nodes, a post-detection game between the malicious and regular nodes is formalized. Solution to this game shows the existence of a subgame perfect Nash Equilibrium and reveals the conditions that are necessary to achieve the equilibrium. Further, we show how a malicious node can construct a belief about the belief held by a regular node. By employing the belief about the belief system, a Markov Perfect Bayes–Nash Equilibrium is reached and the equilibrium postpones the detection of the malicious node. Simulation results and their discussions are provided to illustrate the properties of the derived equilibria. The integration of the detection game and the post-detection is also studied and it is shown that the former one can transit into the latter one when the malicious node actively adjusts its strategies.

1. Introduction

In a distributed wireless system where multiple nodes work towards individual or common goals, cooperative behavior among the nodes (such as controlling the transmit power level, reducing interference for each other, revealing private information, adhering to network policies) is highly desired for increasing system capacity. Though this desirable property makes it easy to analyze a system due to state space reduction; in reality, this assumption might be too strong. For example, there might be entities in the network (also called nodes) which might act in a selfish manner. These selfish nodes, governed by their utility function, care about their own payoffs and

☆ Approved for Public Release; Distribution Unlimited: 88ABW-2014-2735 dated 05 June 2014.

* Corresponding author. Tel.: +1 4078235793.
E-mail addresses: wenjing.wang@bluecoat.com (W. Wang), mainak@eecs.ucf.edu (M. Chatterjee), kevin.kwiat@rl.af.mil (K. Kwiat), qing.li@bluecoat.com (Q. Li).

http://dx.doi.org/10.1016/j.comnet.2014.06.008
1389-1286/

choose corresponding strategies to maximize them. Usually, the payoffs are the benefits a node can derive from other nodes or the network. However, it is possible that there are some nodes whose objective is to cause harm and bring disorder to the network. These nodes, referred as *malicious* nodes, do not reveal their identities while disrupting network services. The objective of such malicious nodes is to maximize the damage before they are detected and isolated. They are also rational, and their payoff is determined by the amount of damage they cause to the network.

In order to minimize the impact of the malicious nodes, detection mechanisms need to be in place. Thus, a regular node should monitor its surroundings and distinguish a malicious node from a regular one. However, the detection process has challenges. First, active monitoring can be costly. To identify malicious behaviors, a regular node has to listen to the channel and/or process the information sent by the nodes being monitored. These monitoring activities consume resources and hence, an "always on" monitoring scheme is not efficient even if plausible. Second, the malicious node can disguise itself. To reduce the probability of being detected, a malicious can behave like a regular node and choose longer intervals between attacks. Third, the randomness and unreliability of the wireless channel bring more uncertainty to the monitoring and detection process.

In spite of the above challenges, mechanisms to detect malicious nodes can always be designed. However, the important question is 'what should the regular node do upon detecting a malicious node?' Though the reasonable response would be to immediately isolate the malicious node, there might be situations where malicious nodes can be kept and made use of. The most straightforward reason for the coexistence is that a malicious node has no idea whether it has been identified or not, and it will continue to operate like a regular node to avoid detection. During this time, i.e., when the malicious node cooperates in disguise, it can be exploited for normal network operations. This "involuntary" help from the malicious node may be valuable, especially when the network resource is limited. As a matter of fact, from the perspective of the malicious nodes, coexistence gives them a longer lifetime in the network and the opportunity to launch future attacks. As far as the regular nodes are concerned, they have a criteria to evaluate the benefit from the malicious nodes. The criteria also determine when to terminate the coexistence and isolate the malicious nodes.

To make the process of detection even more difficult, the malicious nodes do not act passively and wait to be detected. Instead, they also study the interaction they have with the rest of the network and adjust their subsequent actions accordingly. It is also possible that a malicious node is wise enough to learn and predict the actions of the regular nodes to assist itself in making its own decisions on how to behave. The options available to the malicious nodes complicate the solution space and most traditional control theoretic approaches fail to find the equilibrium strategies for both the regular and malicious nodes. In particular, these problems fall more appropriately in the domain of static and dynamic distributed games and thus the application of game theory is an elegant way to tackle such problems. It is important that solution concepts from game theory are used to guide the protocol design process such that nodes working in a distributed manner can co-exist, even with different intents.

Game theory [7,24] has been successfully applied to solve various problems in wireless networks including cooperation enforcement [5,6,11,21,26], routing protocols [10,22,30,34] and other system design issues [2,13,17,20,25,32,33]. Recently, much work has been done that investigates the interactions between the regular and malicious nodes using game theory. Kodialam et al. formally propose a game theoretic framework to model how a service provider detects an intruder [14]. However, their assumptions of zero-sum game and complete, perfect knowledge have limitations. Agah et al. study the non-zero-sum intrusion detection game in [1]; their results infer the optimal strategies in one-stage static game with complete information. In [19], Liu et al. propose a Bayesian hybrid detection approach to detect intrusion in wireless ad hoc networks. They design an energy efficient detection procedure while improving the overall detection power. The intrusion detection game with networked devices are investigated in [35], where Zhu et al. introduce an N-person non-cooperative game to study incentive compatibility of the collaborative detection. [18] models the intention and strategies of a malicious attacker through an incentive-based approach. The importance of the topology on the payoffs of the malicious nodes is investigated in [28]. An interesting flee option for the malicious node is proposed in [16]. In that analysis, a malicious node decides to flee when it believes it is too risky to stay in the network. While the approach focuses on how the flee action affects the result of the game, it does not consider the noises in observation.

There have been some recent researches that focus on the effects of imperfect and/or incomplete information in networking and communications security. In [23], the attacker defender game is modeled as a fictitious play (FP) game, and the authors study the effect of observation errors on the convergence of Nash Equilibrium when the error probability in the channel is unknown. They showed that in a stochastic FP game, the attacker can conceal its true strategy by including an entropy term in the payoff functions. The authors in [8] propose an interesting application of physical layer security game, where the source node pays the surrounding friendly jammer nodes to interfere the eavesdropper, so that the eavesdropper can be masked. The focus is on how to apply game theory to set the price charged by the friendly jammers. The research in [3] deals with malicious jammers when the user does not know how the jamming efforts are distributed among sub-carriers or the fading gains with certainty. The equilibrium strategies in closed form are derived and the range of sub-carriers where the transmitter can expect the jamming attack is specified. The jamming game in multi-band covert timing networks is considered in [25], where the camouflaging resources in the covert time network introduce uncertainty. In their modeling, a sensing game is played so that covert timing network can