ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Game Theoretic Study on Channel-Based Authentication in MIMO Systems

Prof. Jyoti Raghatwan, Alka Taur,

RMD Sinhgad School of Engineering, Pune, India

Student, RMD Sinhgad School of Engineering, Pune, India

ABSTRACT: Multiple-input multiple-output (MIMO) techniques can improve the capacity and reliability of wireless communication systems, and increase secrecy capacities against eavesdropping. While it involves multiple technologies, MIMO can essentially be boiled down to this single principle: a wireless network that allows the transmitting and receiving of more than one data signal simultaneously over the same radio channel. Standard MIMO networks tend to use two or four antennas. Massive MIMO, on the other hand, is a MIMO system with an especially high number of antennas.There’s no set figure for what constitutes a Massive MIMO set-up, but the description tends to be applied to systems with tens or even hundreds of antennas. For example, Huawei, ZTE, and Facebook have demonstrated Massive MIMO systems with as many as 96 to 128 antennas.Because MIMO systems need to physically pack more antennas into a small area, they require the use of higher frequencies (and hence shorter wavelengths) than current mobile network standards.

KEYWORDS: MIMO, Channel Based, Game Theory.

I. INTRODUCTION

1.1 MIMO

Multiple-input multiple-output (MIMO) techniques can improve the capacity and reliability of wireless communication systems, and increase secrecy capacities against eavesdropping. While it involves multiple technologies, MIMO can essentially be boiled down to this single principle: a wireless network that allows the transmitting and receiving of more than one data signal simultaneously over the same radio channel. Standard MIMO networks tend to use two or four antennas. Massive MIMO, on the other hand, is a MIMO system with an especially high number of antennas.

There’s no set figure for what constitutes a Massive MIMO set-up, but the description tends to be applied to systems with tens or even hundreds of antennas. For example, Huawei, ZTE, and Facebook have demonstrated Massive MIMO systems with as many as 96 to 128 antennas.

Because MIMO systems need to physically pack more antennas into a small area, they require the use of higher frequencies (and hence shorter wavelengths) than current mobile network standards.

Advantages of MIMO:-

The advantage of a MIMO network over a regular one is that it can multiply the capacity of a wireless connection without requiring more spectrums. Early reports point to considerable capacity improvements, and could potentially yield as much as a 50-fold increase in future.

The more antennas the transmitter/receiver is equipped with, the more the possible signal paths and the better the performance in terms of data rate and link reliability.

A Massive MIMO network will also be more responsive to devices transmitting in higher frequency bands, which will improve coverage. In particular, this will have considerable benefits for obtaining a strong signal indoors.

The greater number of antennas in a Massive MIMO network will also make it far more resistant to interference and intentional jamming than current systems that only utilise a handful of antennas.

DOI: 10.15680/IJIRCCE.2018.0605007

1.2Game theory

Game theory is a powerful mathematical tool to analyse the interactions among autonomous players that have the same or different goals.

Game theory creates a language and formal structure of analysis for making logical decisions in competitive environments. The term “game” can be misleading. Even though game theory applies to recreational games, the concept of “game” simply means any interactive situation in which independent actors share more-or-less formal rules and consequences.

The formal application of game theory requires knowledge of the following details: the identity of independent actors, their preferences, what they know, which strategic acts they are allowed to make, and how each decision influences the outcome of the game. Depending on the model, various other requirements or assumptions may be necessary. Finally, each independent actor is assumed to be rational.

Game theory has a wide range of applications, including psychology, evolutionary biology, war, politics, economics and business. Despite its many advances, game theory is still a young and developing science.

Game theory is "the study of mathematical models of conflict and cooperation between intelligent rational decision-makers". Game theory is mainly used in economics, political science, and psychology, as well as in logic and computer science. Originally, it addressed zero-sum games, in which one person's gains result in losses for the other participants. Today, game theory applies to a wide range of behavioral relations, and is now an umbrella term for the science of logical decision making in humans, animals, and computers.

1.3 Game types

1) Cooperative / Non-cooperative

A game is *cooperative* if the players are able to form binding commitments externally enforced (e.g. through contract law). A game is *non-cooperative* if players cannot form alliances or if all agreements need to be self-enforcing (e.g. through credible threats).

2) Symmetric / Asymmetric

A symmetric game is a game where the payoffs for playing a particular strategy depend only on the other strategies employed, not on who is playing them. If the identities of the players can be changed without changing the payoff to the strategies, then a game is symmetric. Many of the commonly studied 2×2 games are symmetric. Most commonly studied asymmetric games are games where there are not identical strategy sets for both players. For instance, the ultimatum game and similarly the dictator game have different strategies for each player. It is possible, however, for a game to have identical strategies for both players, yet be asymmetric. For example, the game pictured as follows is asymmetric despite having identical strategy sets for both players.

	E	F
E	1, 2	0, 0
F	0, 0	1, 2

Fig. 1.2.1An asymmetric game

3) Zero-sum / Non-zero-sum

Zero-sum games are a special case of constant-sum games, in which choices by players can neither increase nor decrease the available resources. In zero-sum games the total benefit to all players in the game, for every combination of strategies, always adds to zero (more informally, a player benefits only at the equal expense of others). Poker exemplifies a zero-sum game (ignoring the possibility of the house's cut), because one wins exactly the amount one's opponents lose. Other zero-sum games include matching pennies and most classical board games including Go and chess.

Many games studied by game theorists (including the famed prisoner's dilemma) are non-zero-sum games, because the outcome has net results greater or less than zero. Informally, in non-zero-sum games, a gain by one player does not necessarily correspond with a loss by another.

Constant-sum games correspond to activities like theft and gambling, but not to the fundamental economic situation in which there are potential gains from trade. It is possible to transform any game into a (possibly asymmetric) zero-sum game by adding a dummy player (often called "the board") whose losses compensate the players' net winnings.

	A	B
A	–1, 1	3, –3
B	0, 0	–2, 2

Fig. 1.2.2 A zero-sum game

4) Simultaneous / Sequential

Simultaneous games are games where both players move simultaneously, or if they do not move simultaneously, the later players are unaware of the earlier players' actions (making them *effectively* simultaneous). Sequential games (or dynamic games) are games where later players have some knowledge about earlier actions. This need not be perfect information about every action of earlier players; it might be very little knowledge. For instance, a player may know that an earlier player did not perform one particular action, while he does not know which of the other available actions the first player actually performed.

5) Perfect information and imperfect information

An important subset of sequential games consists of games of perfect information. A game is one of perfect information if all players know the moves previously made by all other players. Most games studied in game theory are imperfect-information games. Examples of perfect-information games include tic-tac-toe, checkers, infinite chess, and Go.

Many card games are games of imperfect information, such as poker and bridge. Perfect information is often confused with complete information, which is a similar concept. Complete information requires that every player know the strategies and payoffs available to the other players but not necessarily the actions taken. Games of incomplete information can be reduced, however, to games of imperfect information by introducing "moves by nature".

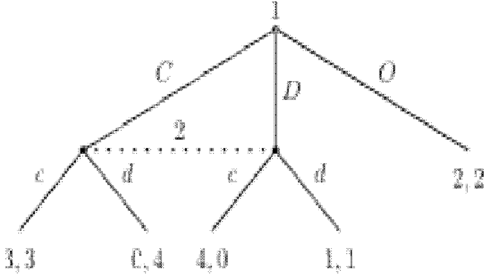

Fig. 1.2.3 A game of imperfect information (the dotted line represents ignorance on the part of player 2, formally called information set)

6) Combinatorial games

Games in which the difficulty of finding an optimal strategy stems from the multiplicity of possible moves are called combinatorial games. Examples include chess and go. Games that involve imperfect information may also have a strong combinatorial character, for instance backgammon. There is no unified theory addressing combinatorial elements in games. There are, however, mathematical tools that can solve particular problems and answer general questions.

7) Infinitely long games

Games, as studied by economists and real-world game players, are generally finished in finitely many moves. Pure mathematicians are not so constrained, and in particular study games that last for infinitely many moves, with the winner (or other payoff) not known until *after* all those moves are completed.

8) Discrete and continuous games

Much of game theory is concerned with finite, discrete games, that have a finite number of players, moves, events, outcomes, etc. Many concepts can be extended, however. Continuous games allow players to choose a strategy from a continuous strategy set. For instance, Cournot competition is typically modeled with players' strategies being any non-negative quantities, including fractional quantities.

9) Differential games

Differential games such as the continuous pursuit and evasion game are continuous games where the evolution of the players' state variables is governed by differential equations. The problem of finding an optimal strategy in a differential game is closely related to the optimal control theory. In particular, there are two types of strategies: the open-loop strategies are found using the Pontryagin maximum principle while the closed-loop strategies are found using Bellman's Dynamic Programming method.

10) Many-player and population games

Games with an arbitrary, but finite, number of players are often called n-person games. Evolutionary game theory considers games involving a population of decision makers, where the frequency with which a particular decision is made can change over time in response to the decisions made by all individuals in the population. In biology, this is intended to model (biological) evolution, where genetically programmed organisms pass along some of their strategy programming to their offspring. In economics, the same theory is intended to capture population changes because people play the game many times within their lifetime, and consciously (and perhaps rationally) switch strategies.

11) Stochastic outcomes (and relation to other fields)

Individual decision problems with stochastic outcomes are sometimes considered "one-player games". These situations are not considered game theoretical by some authors. They may be modeled using similar tools within the related disciplines of decision theory, operations research, and areas of artificial intelligence, particularly AI planning (with uncertainty) and multi-agent system. Although these fields may have different motivators, the mathematics involved are substantially the same, e.g. using Markov decision processes (MDP).

Stochastic outcomes can also be modeled in terms of game theory by adding a randomly acting player who makes "chance moves" ("moves by nature").This player is not typically considered a third player in what is otherwise a two-player game, but merely serves to provide a roll of the dice where required by the game.

12) Metagames

These are games the play of which is the development of the rules for another game, the target or subject game. Metagames seek to maximize the utility value of the rule set developed. The theory of metagames is related to mechanism design theory.

The term metagame analysis is also used to refer to a practical approach developed by Nigel Howard. Whereby a situation is framed as a strategic game in which stakeholders try to realise their objectives by means of the options available to them. Subsequent developments have led to the formulation of confrontation analysis.

13) Pooling games

These are games prevailing over all forms of society. Pooling games are repeated plays with changing payoff table in general over an experienced path and their equilibrium strategies usually take a form of evolutionary social convention and economic convention. Pooling game theory emerges to formally recognize the interaction between optimal choice in one play and the emergence of forthcoming payoff table update path, identify the invariance existence and robustness, and predict variance over time. The theory is based upon topological transformation classification of payoff table update over time to predict variance and invariance, and is also within the jurisdiction of the computational law of reachable optimality for ordered system.

II. LITERATURE SURVEY

2.1 Introduction

K. Zeng, K. Govindan, and P. Mohapatra[1]Lower/physical layer characteristics have been considered as potential alternatives/complements to provide security services in wireless networks. This article provides an overview about various non-cryptographic mechanisms for user authentication and device identification in wireless networks using lower/physical layer properties or information.We discuss merits and demerits of these authentication/identification schemes and the practical implementation issues. Future research on crosslayer security design concludes this paper.

J. Yang, Y. Chen, W. Trappe, and J. Cheng[2]Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. In this paper, author propose to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for (1) detecting spoofing attacks; (2) determining the number of attackers when multiple adversaries masquerading as a same node identity; and (3) localizing multiple adversaries. Author evaluated our techniques through two test beds using both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network in two real office buildings.

Fiona Jiazi Liu, Xianbin Wang, and Serguei L. Primak[3] the reliability of CIR-based authentication is substantially reduced at low signal to- noise ratio (SNR) conditions due to the presence of communications noise, channel estimation error and mobility induced channel variation. To this end, we integrate additional multipath delay characteristics into the CIR-based physical layer authentication and propose a two dimensional quantization scheme to tolerate these random errors of CIRs for reduced false alarm rate and more reliable spoofing detection. Instead of directly comparing the estimated CIRs from different transmitters for authentication purpose, we first quantize the CIR estimates in two dimensions and then differentiate transmitters based on the quantizer outputs with a binary hypothesis testing.

J. Chen, Q. Yu, P. Cheng, Y. Sun, Y. Fan, and X. Shen[4]In this paper, multi-channel allocation in wireless sensor and actuator networks is formulated as an optimization problem which is NP-hard. In order to efficiently solve this problem, a distributed game based channel allocation (GBCA) Algorithm is proposed by taking into account both network topology and routing information. For both tree/forest routing and non-tree/forest routing scenarios, it is proved that there exists at least one Nash Equilibrium for the problem. Furthermore, the sub optimality of Nash Equilibrium and the convergence of the Best Response dynamics are also analyzed. Simulation results demonstrate that GBCA significantly reduces the interference and dramatically improves the network performance in terms of delivery ratio, throughput, channel access delay, and energy consumption

L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang[5] In this paper, author investigate the PHY-layer authentication that exploits radio channel information to detect spoofing attacks in wireless networks. The interactions between a legitimate receiver and spoofers are formulated as a zero-sum authentication game. The receiver chooses the test threshold in the hypothesis test to maximize its utility based on the Bayesian risk in the spoofing detection. The Nash equilibrium of the static authentication game is derived and its uniqueness is discussed.

C. J. Watkins and P. Dayan [6] Q-learning (Watkins, 1989) is a simple way for agents to learn how to act optimally in controlled Markovian domains. It amounts to an incremental method for dynamic programming which imposes limited computational demands. It works by successively improving its evaluations of the quality of particular actions at particular states. This paper presents and proves in detail a convergence theorem for Q,-learning based on that outlined in Watkins (1989). We show that Q-learning converges to the optimum action-values with probability 1 so long as all actions are repeatedly sampled in all states and the action-values are represented discretely. We also sketch extensions to the cases of non-discounted, but absorbing, Markov environments, and where many Q values can be changed each iteration, rather than just one.

R. S. Sutton and A. G. Barto [7] Reinforcement learning has always been important in the understanding of the driving forces behind biological systems, but in the past two decades it has become increasingly important, owing to the development of mathematical algorithms. Barto and Sutton were the prime movers in leading the development of these algorithms.

A. W. Moore and C. G. Atkeson [8]This paper present a new algorithm, prioritized sweeping, for efficient prediction and control of stochastic Markov systems. Incremental learning methods such as temporal differencing and Q-learning have real-time performance. Classical methods are slower, but more accurate, because they make full use of the observations. Prioritized sweeping aims for the best of both worlds. It uses all previous experiences both to prioritize important dynamic programming sweeps and to guide the exploration of state-space. We compare prioritized sweeping with other reinforcement learning schemes for a number of different stochastic optimal control problems. It successfully solves large state-space real-time problems with which other methods have difficulty.

L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe [9] Multiple-input multiple-output (MIMO) techniques allow for multiplexing and diversity gain, and will be widely deployed in future wireless systems. In this paper, authorpropose a MIMO-assisted channel-based authentication scheme, exploiting current channel estimation mechanisms in MIMO systems to detect spoofing attacks with very low overhead. In this scheme, the use of multiple antennas provides extra dimensions of channel estimation data, and thus leads to a “security gain” over single input single-output (SISO) systems. We investigate the security gain of MIMO systems in several system configurations via simulations for a specific real indoor environment using ray tracing software.

H. Wen, S. Li, X. Zhu, and L. Zhou [10] In this article author focus on the security in cognitive radio, which is one of the needs for new technologies requiring spectrum bands. The PHY-layer in CR is more complex than a conventional wireless communication system because of spectrum sensing and the dynamic spectrum access mechanism. Therefore, it becomes vulnerable to be invaded. We present the PHY-layer approaches to defense against security threats in CR networks.

P. Baracca, N. Laurenti, and S. Tomasin [11] In a wide band and multipath rich environment, precise channel estimation allows authenticating the source and protecting the integrity of a message at the physical layer without the need of a pre-shared secret key. This allows also a reduction of the burden on the authentication protocols at higher layers. In this paper we develop an authentication scheme in the framework of hypothesis testing that suits a multiple wiretap channels environment with correlated fading, as is the case of multiple input multiple output (MIMO) systems and/or orthogonal frequency division multiplexing (OFDM) modulation.

C. Chen, M. Song, C. S. Xin, and J. Backens [12] Cognitive radio networks are a promising solution to the spectrum scarcity issue. However, cognitive radio networks are vulnerable to various kinds of security attacks, among which the jamming attack has attracted great attention as it can significantly degrade spectrum utilization. In this article we model the jamming and anti-jamming process as a Markov decision process. With this approach, secondary users are able to avoid the jamming attack launched by external attackers and therefore maximize the payoff function. We first use a policy iteration method to solve the problem. However, this approach is computationally intensive. To decrease the computation complexity, Q-function is used as an alternate method. Furthermore, we propose an algorithm to solve the Q-function. The simulation results indicate that our approach can achieve better performance than existing approaches to defend against the jamming attack.

Y. E. Sagduyu and A. Ephremides [13] in this paper author consider a random access system of non-cooperative selfish transmitters with the individual objectives of jointly optimizing throughput rewards, energy and delay costs. The goal is to evaluate the effects of malicious nodes that have the dual objectives of blocking the packet transmissions of the other selfish nodes as well as optimizing their individual performance measures. We formulate a non-cooperative random access game of selecting individual probabilities of transmitting packets to a common receiver and derive the transmission strategies in non-cooperative Nash equilibrium depending on the throughput rewards, energy and delay costs.

A. Mukherjee and A. L. Swindlehurst [14]this paper author investigates transmission strategies in a MIMO wiretap channel with a transmitter, receiver and wiretapper, each equipped with multiple antennas. In a departure from existing work, the wiretapper is able to act either as a passive eavesdropper or as an active jammer per channel use, under a half-duplex constraint. The transmitter therefore faces a choice between dynamically allocating all of its power for data; or broadcasting artificial noise along with the information signal in order to selectively degrade the eavesdropper's channel. We model the network as a zero-sum game in strategic form with the MIMO secrecy rate as the payoff function.

B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy [15] in this paper, author investigate the security mechanism when secondary users are facing the jamming attack, and propose a stochastic game framework for anti-jamming defense. At each stage of the game, secondary users observe the spectrum availability, the channel quality, and the attackers' strategy from the status of jammed channels. According to this observation, they will decide how many channels they should reserve for transmitting control and data messages and how to switch between the different channels. Using the minimax-Q learning, secondary users can gradually learn the optimal policy, which maximizes the expected sum of discounted payoffs defined as the spectrum-efficient throughput.

B. F. Lo and I. F. Akyildiz [16]in this paper, author introduce a jamming resilient control channel (JRCC) game to model the interactions among cognitive radio users and the attacker under the impact of primary user activity. Author propose the JRCC algorithm that enables user cooperation to facilitate control channel allocations and adapts to primary user activity with variable learning rates using the Win-or-Learn-Fast principle for jamming-resilience in hostile environments. It is shown that the optimal strategies converge to Nash equilibrium or the expected rewards of the strategies converge to that of Nash equilibrium. The results also show that the JRCC algorithm effectively combats jamming under the impact of primary user activity and sensing errors. Moreover, the control channel allocation policy can be improved by enhancing transmission and sensing capabilities.

R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen [17] in this paper, authors propose a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data. Based on the random graph characteristics of sensor node deployment and the cooperative bit-compressed authentication technique, the proposed BECAN scheme can save energy by early detecting and filtering the majority of injected false data with minor extra overheads at the en-route nodes.

D. He, C. Chen, S. Chan, and J. Bu [18] in this paper author shows that prior handover authentication schemes incur high communication and computation costs, and are subject to a few security attacks. Further, a novel handover authentication protocol named Pair-Hand is proposed. PairHand uses pairing-based cryptography to secure handover process and to achieve high efficiency. Also, an efficient batch signature verification scheme is incorporated into PairHand. Experiments using our implementation on laptop PCs show that PairHand is feasible in real applications.

2.2 Existing system

Advances in communication and networking technologies are rapidly making ubiquitous network connectivity a reality. Wireless networks are indispensable for supporting such access anywhere and anytime. Due to its "open air" nature, the wireless environment imposes greater challenges on ensuring network security than in wired networks. Because of the broadcast nature of the wireless medium, the communication can be easily eavesdropped or intercepted. The wireless devices can be compromised and modified to behave maliciously or selfishly. These vulnerabilities in wireless networks would undermine the authenticity, confidentiality, integrity, and availability if they are not carefully addressed. On the flip side, the inherent and unique characteristics of the wireless medium or devices can be exploited to enhance the network security.

Among the various types of attacks in wireless networks, identity-based attacks (i.e., MAC address spoofing) are easy to launch and can significantly degrade the network performance. Identity-based attacks are considered as the first step in an intruder’s attempt to launch a variety of attacks, including denial of service (DoS), session hijacking, man-in-the-middle, data modification, and sniffing. Although traditional cryptographic techniques can potentially prevent identity-based attacks in wireless networks, they are either inefficient or fall short in certain existing scenarios. A few shortcomings can be identified as follows. First, although existing 802.11 security techniques provide authentication for data frames, management and control frames are usually not protected. Second, most of the cryptographic techniques are ill suited for a less equipped distributed wireless network due to high complexity and computational requirements. In addition, the conventional cryptographic security mechanisms need key management to distribute, refresh, and revoke the keys. However, key management is difficult in ad hoc networks where nodes join and leave the network frequently. Third, even when the traditional cryptographic means are feasible, wireless devices are subject to physical compromises in an adversarial environment. Any unprotected keying materials used for authentication stored on the device may be compromised through physical attacks, which will diminish the strength of the security mechanisms.

III. PROBLEM STATEMENT AND OBJECTIVE

a. Problem Statement

The decoding of massive MIMO systems forms a complex computational problem.Given these distributions, we now precisely define MIMO decoding for the eavesdropper in the MIMO wiretap channel, which we denote as the MIMO-Search problem. The search problem asks us to recover the transmitted vector x without error. We loosely use the term “MIMO decoding problem” to refer to the search problem. we discuss how to use the hardness of the problem to construct cryptographically secure systems, and provide a comparison between cryptographer’s notions of security with ones used by information theorists.

b. Objective

The main objective of this is for the authentication based on radio channel information in multiple-input multiple output (MIMO) systems, and formulate the interactions between a receiver with multiple antennas and a spoofing node as a zero-sum physical (PHY)-layer authentication game. In this game, the receiver chooses the test threshold of the hypothesis test to maximize its Bayesian risk based utility in the spoofing detection, while the adversary chooses its attack rate.

We used the Nash equilibrium (NE) of the static PHY-layer authentication game and present the condition that the NE exists, showing that both the spoofing detection error rates and the spoofing rate decrease with the number of transmit and receive antennas. Dyna architecture and prioritized sweeping (Dyna-PS) used to improve the spoofing detection in time-variant radio environments. Dyna-PS based spoofing detection algorithm reduces the spoofing detection error rates and increases the utility of the receiver.

We used a PHY layer spoofing detection algorithm for MIMO systems based on Q-learning, in which the receiver applies the reinforcement learning technique to achieve the optimal test threshold via trials in a dynamic game without knowing the system parameters, such as the channel time variation and spoofing cost.

IV. METHODOLOGY

Channel-based authentication methods exploit the spatial decorrelation property of radio propagation to detect spoofing attacks in wireless systems. For instance, received signal strength measured at the mobile node is compared with the channel record of the claimed transmitter to detect the spoofing attacks in wireless networks. The spoofing detection algorithm developed uses the generalized likelihood ratio test to discriminate radio nodes according to their channel frequency responses in MIMO systems. The PHY-layer authentication system proposed evaluates the estimated channel responses to detect both primary user emulation attacks and Sybil attacks in cognitive radio networks. The spoofing strategies against MIMO systems as evaluated can be detected by the PHY-layer authentication even in the presence of the optimal spoofing strategy, if the channel estimation is precise. The channel impulse response based PHY-layer authentication introduces a two dimensional quantization scheme to tolerate the random errors and reduce the spoofing error rates. Game theory has been used to study wireless security. For instance, a zero-sum jamming game provides the optimal anti-jamming communication strategy for cognitive radio nodes with perfect channel information. A non-cooperative random access game addresses jamming attacks in a wireless network with unknown jamming models. The MIMO transmission against a dual-threat attacker that performs both eavesdropping and jamming is formulated as a zero-sum game. The interaction between a secondary user and a jammer as a stochastic game with minimax-Q learning.The transmission over the control channel with reinforcement learning to achieve the optimal channel allocation in ad hoc networks against jamming.The interactions between a legitimate receiver and a spoofing node as a zero-sum channel-based authentication game. We have extended the work to formulate a MIMO spoofing detection game, and found that the detection accuracy increases with the number of transmit antennas. we investigate in this paper the NE of the static spoofing detection game in a generic case, and propose a Dyna-PS based detection scheme to improve the detection accuracy of MIMO systems compared with the Q-learning based scheme in dynamic radio environments.

b. PHY-Layer Authentication Game in MIMO Systems

In this section, we apply game theory to investigate the authentication based on the spatial decorrelation of channel frequency responses. At time slot *k*, either Alice or Eve sends signals to Bob claiming to be Alice. The channel based spoofing detection establishes a hypothesis test to decide whether or not the signal that Bob receives at time slot *k* is sent by Alice. The null hypothesis ΄H_0 indicates that the signal is indeed sent by Alice (i.e., the channel gain is $H^k{}_A$). In the alternative hypothesis ΄H_1, the claimant node is Eve. Thus the hypothesis test in the spoofing detection is given by
΄H_0 :$H^k{}_t$= $H^k{}_A$ (1)
΄H_1 :$H^k{}_t$≠ $H^k{}_A$ (2)

Bob compares the new channel vector ˜$H^k{}_t$with the channelrecord of Alice $\hat{H}_A$. If the channel gain ˜$H^k{}_t$ is significantlydifferent from the channel record of Alice, Bob chooses thealternative hypothesis and sends a spoofing alarm; otherwise,there is every reason to believe that the signal is sent by Alice.The test statistic, denoted by *L*, is chosen as the normalizedEuclidean distance between the channel estimate ˜$H^k{}_t$ andthe channel record of Alice, and is compared with the testthreshold X^kat time slot *k*. As the test statistic *L* is positive,we have X^k> 0. If the test statistic *L* is less than X^k , Bobaccepts the null hypothesis ΄H0; otherwise, Bob accepts ΄H_1. Thus the PHY-layer authentication is given by

$$L\left(\tilde{\mathbf{H}}_t^k, \hat{\mathbf{H}}_A\right) = \frac{\left\|\tilde{\mathbf{H}}_t^k - \hat{\mathbf{H}}_A\right\|^2}{\left\|\hat{\mathbf{H}}_A\right\|^2} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} x^k \qquad (3)$$

where‖ · ‖ is the Frobenius norm. The detection accuracy of the PHY-layer authentication
depends on the test threshold X^k. For instance, the successful detection rate decreases with X^k. The false alarm rate of the spoofing detection, denoted by p_f, is defined as the probability
that Bob discards Alice's signal by mistake, i.e.,

$$p_f(x) = \Pr\left(\mathcal{H}_1|\mathcal{H}_0\right) = \Pr\left(L\left(\tilde{\mathbf{H}}_A^k, \hat{\mathbf{H}}_A\right) > x\right) \qquad (4)$$

where$P_r(\cdot|\cdot)$ is the conditional probability. The miss detection rate, denoted by P_m, is defined as the probability that a spoofing signal passes the PHY-layer detection and given by

$$p_m(x) = \Pr\left(\mathcal{H}_0|\mathcal{H}_1\right) = \Pr\left(L\left(\tilde{\mathbf{H}}_E^k, \hat{\mathbf{H}}_A\right) \leq x\right). \qquad (5)$$

Based on the detection accuracy and security cost, the utility of each player in the static game can be defined according to the Bayesian risk of the detection as

$$\begin{aligned} u_B(x,y) = -u_E(x,y) = &\left(G_1\left(1-p_f(x)\right) - C_1 p_f(x)\right)(1-y) \\ &+ \left(G_0\left(1-p_m(x)\right) - C_0 p_m(x) + C_s\right)y. \qquad (6) \end{aligned}$$

4.2 NE of the PHY-Layer Authentication Game

We consider the Nash equilibrium of the static PHY-layer authentication game, denoted by (x∗, y∗), in which neither Bob nor Eve can increase his or her utility by unilaterally choosing another strategy, i.e.,

$$x^* = \arg\max_{x\geq 0} \ u_B(x, y^*) \qquad (7)$$

$$y^* = \arg\min_{0\leq y\leq 1} u_B(x^*, y) . \qquad (8)$$

If the channel responses at M frequencies from each of the Nt×Nr antenna pairs are independent and identically distributed, we have

$$L'\left(\tilde{\mathbf{H}}_t^k, \hat{\mathbf{H}}_A\right) = \left\|\tilde{\mathbf{H}}_t^k - \hat{\mathbf{H}}_A\right\|^2 \sim \chi^2(2N_tN_rM) \qquad (9)$$

The detection accuracy of the spoofing detection depends on the test threshold x, the average power gain along the path σ^2, the average SNR of the signal received by Bob ρ, the channel time variation α, and the average ratio of the SNR between Eve’s and Alice’s signals β. we have

$$p_f(x) = 1 - F_{\chi^2}\left(\frac{2x\rho}{\sigma^2(2+\alpha\rho)}, 2N_tN_rM\right) \qquad (10)$$

$$p_m(x) = F_{\chi^2}\left(\frac{2x\rho}{\sigma^2(2+\rho+\beta\rho)}, 2N_tN_rM\right) \qquad (11)$$

4.3 PHY-layer spoofing detection with Q-learning

We formulate the repeated interactions between Bob and Eve in a dynamic radio environment as a dynamic PHY-layer authentication game, in which Bob builds the hypothesis test as shown in (3) to detect spoofing attacks in each time slot. For simplicity, we assume that either Alice or Eve sends *T* signals in a time slot. The expected sum utility of Bob is denoted by $U^k$and defined as

$$U^k = \sum_{n=(k-1)T+1}^{kT} u_B^n(x^k, y^k)$$

4.4 PHY-Layer spoofing detection with DYNA-PS

To improve the performance of the Q-learning based spoofing detection in time-variant radio environments, we apply the Dyna architecture that formulates a learned world model from real experience, and use prioritized sweeping that prioritizes the backup state-action pairs according to their urgencies. More specifically, the Dyna-PS based spoofing detection prioritizes the state-action pairs, and remembers the predecessors of each state, i.e., the states that have a non-zero transition probability to a given state. The spoofing detection maintains a queue for each state-action pair, and prioritizes the state-action pairs according to the change of their values. The scheme first applies Q-learning to obtain real experiences, and then establishes the Dyna architecture for the hypothetical experience corresponding to the change of the Q-function of the state-action pairs in the state updates. More specifically, at time slot k, Bob evaluates the error rates of the spoofing detection at the last time slot to form the state $S^k = [P^{k-1}_f , P^{k-1}_m] \in S$, where S is the feasible state set, and chooses the test threshold X^k according to the ε-greedy policy. Then, the hypothesis test is performed according to determine whether or not the transmitter that sent the T signals at time slot k is Alice. The security performance is then evaluated to obtain both the immediate utility and the sum utility U^k. Bob then updates his Q-function and value function.

V. ALGORITHMS

5.1 Algorithm 1 MIMO spoofing detection with Q-learning.

```
1: Initialize $\varepsilon, \mu, \delta, Q(s, x) = 0$, and $V(s) = 0, \forall x \in \{l/K\}0 \le l \le K$
2: for $k = 1, 2, 3, \ldots$ do
3:     Choose $X^k$
4:     for $n = 1$ to $T$ do
5:         Receive signal n at time slot k
6:         Channel estimation to obtain $\tilde{H}^n_t$
7:         Calculate L via (9)
8:         if $L \le X^k$ then
9:             Perform the higher-layer authentication
10:            if signal n is accepted then
11:                $\hat{H}A \leftarrow \tilde{H}^n_t$
12:            else
13:                Send spoofing alarm for signal n
14:            end if
15:        end if
16:    end for
17:    Observe $P^k_f$ and $P^k_m$ to form $S^{k+1} = [P^k_f, P^k_m]$
18:    Update $Q(S^k, X^k)$
19:    Update $V(S^k)$
20: end for
```

5.2 Algorithm 2 MIMO spoofing detection with Dyna-PS.

```
1: Initialize: $\varepsilon, \mu, \delta, \theta, J, Q = 0, V = 0, \Delta = 0, \Phi = 0, \Phi' = 0, \Psi = 0, R' = 0, R = 0$, and $\Pi = 0$
2: for $k = 1, 2, 3, \ldots$ do
3:     Authenticate the received T signals and update $Q(S^k, X^k)$ and $V(S^k)$ by Step 3-19 in Algorithm 1
4:     Obtain the real experience$(S^k, X^k, S^{k+1}, U^k)$
5:     Calculate $\Delta(S^k, X^k)$
6:     Insert$(S^k, X^k)$ into $\Psi$ with priority $\Delta(S^k, X^k)$
7:     Update $\Phi' (S^k, X^k, S^{k+1})$
8:     Update $\Phi(S^k, X^k,)$
9:     Update $R' (S^k, X^k, \Phi(S^k, X^k))$
10:    Update $R(S^k, X^k)$
$^{11}$:    Update $\Pi(S^k, X^k, S^{k+1})$
12:    Set $j = 0$
13:    while $j < J$ do
14:        Select the state-action pair $(S^j, X^j)$ with the highest priority in $\Psi$
15:        if $\Delta(S^j, X^j) > \theta$ then
16:            Set $\Delta(S^j, X^j) = 0$
17:            Obtain the reward $U^j = R(S^j, X^j)$
18:            Update $Q(S^j, X^j)$
19:            Update $V(S^j)$
20:            for all the predecessors $(\bar{S}, \bar{X})$ of state $S^j$ do
21:                Calculate $\Delta (\bar{S}, \bar{X})$
```

```
Insert $(\bar{S}, \bar{X})$ into $\Psi$ with priority $\Delta(\bar{S}, \bar{X})$
end for
j++
else
break
end if
end while
end for
```

VI. CONCLUSION

While doing survey of this seminar topic we have study the PHY-layer authentication in MIMO systems and presented the NEs of the static authentication game, showing that the receiver chooses its test threshold and adversary decides its attack probability based on the SNR, attack costs, channel conditions, and channel gain time variation. We have also learnt about the Q-learning and Dyna-PS based spoofing detections, in which the test threshold in the spoofing detection is chosen via the reinforcement learning techniques. For example, in the MIMO system with 5 transmit antennas and 20 MHz bandwidth, the miss detection rate of the Q-learning based detection decreases by 42.9% to 1.9%, and the false alarm rate decreases by 55.6% to 0.1%, if the number of receive antennas changes from 2 to 4. The Dyna-PS based spoofing detection further reduces the miss detection rate to 1.3% in the 5 × 4 MIMO system. The utility of the receiver with the Q-learning based authentication is 2.6% higher than the benchmark scheme, which is further improved by 3.1% with Dyna-PS.

We study the interactions between a receiver performing the channel-based spoofing detection and a spoofing node in MIMO systems as a zero-sum PHY-layer authentication game. We learn about the NE of the static PHY-layer authentication game and provide the conditions that the game has no NE. We study the dynamic PHY-layer authentication game and propose a channel-based spoofing detection algorithm based on Q-learning for MIMO systems in a dynamic radio environment. We further learn its performance with Dyna architecture and prioritized sweeping. We study the Q-learning based spoofing detection algorithm for MIMO systems and the Dyna-PS based spoofing.

REFERENCES

[1] K. Zeng, K. Govindan, and P. Mohapatra, “Non-cryptographic authentication and identification in wireless networks,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.

[2] J. Yang, Y. Chen, W. Trappe, and J. Cheng, “Detection and localization of multiple spoofing attackers in wireless networks,” *IEEE Trans.Parallel and Distributed Systems*, vol. 24, no. 1, pp. 44–58, Jan. 2013.

[3] F. J. Liu, X. Wang, and S. L. Primak, “A two dimensional quantization algorithm for CIR-based physical layer authentication,” in *Proc. IEEEInt’l Conf. Commun. (ICC)*, pp. 4724–4728, Budapest, Jun. 2013.

[4] J. Chen, Q. Yu, P. Cheng, Y. Sun, Y. Fan, and X. Shen, “Game theoretical approach for channel allocation in wireless sensor and actuator networks,” *IEEE Trans. Automatic Control*, vol. 56, no. 10, pp. 2332– 2344, Aug. 2011.

[5] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, “PHY-layer spoofing detection with reinforcement learning in wireless networks,” *IEEE Trans.Vehicular Technology*, vol. 65, no. 12, pp. 10037–10047, Feb. 2016.

[6] C. J. Watkins and P. Dayan, “Q-learning,” *Machine learning*, vol. 8, no. 3, pp. 279–292, May 1992.

[7] R. S. Sutton and A. G. Barto, *Reinforcement learning: An introduction*. MIT press, Sep. 1998.

[8] A. W. Moore and C. G. Atkeson, “Prioritized sweeping: Reinforcement learning with less data and less time,” *Machine Learning*, vol. 13, no. 1, pp. 103–130, Oct. 1993.

[9] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “MIMO-assisted channel-based authentication in wireless networks,” in *Proc. IEEEInformation Sciences and Systems (CISS)*, pp. 642–646, Princeton, Mar. 2008.

[10] H. Wen, S. Li, X. Zhu, and L. Zhou, “A framework of the PHY-layer approach to defense against security threats in cognitive radio networks,” *IEEE Network*, vol. 27, no. 3, pp. 34–39, May 2013.

[11] P. Baracca, N. Laurenti, and S. Tomasin, “Physical layer authentication over MIMO fading wiretap channels,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, Jul. 2012.

[12] C. Chen, M. Song, C. S. Xin, and J. Backens, “A game-theoretical anti-jamming scheme for cognitive radio networks,” *IEEE Netw.*, vol. 27, no. 3, pp. 22–27, May 2013.

[13] Y. E. Sagduyu and A. Ephremides, “A game-theoretic analysis of denial of service attacks in wireless random access,” *Wireless Netw.*, vol. 15, no. 5, pp. 651–666, Apr. 2009.

[14] A. Mukherjee and A. L. Swindlehurst, "Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in MIMO channels," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, pp. 1695– 1700, San Jose, Oct. 2010.

[15] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas inCommun.*, vol. 29, no. 4, pp. 877–889, Apr. 2011.

[16] B. F. Lo and I. F. Akyildiz, "Multiagent jamming-resilient control channel game for cognitive radio ad hoc networks," in *Proc. IEE Int'lConf. Commun. (ICC)*, pp. 1821–1826, Ottawa, Jun. 2012.

[17] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, "BECAN: A bandwidthefficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," *IEEE Trans. Parallel and DistributedSystems*, vol. 23, no. 1, pp. 32–43, Jan. 2012.

[18] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Trans. WirelessCommunications*, vol. 11, no. 1, pp. 48–53, Jan. 2012.