Game Theory for Network Security

Xiannuan Liang and Yang Xiao, *Senior Member, IEEE*

***Abstract*—As networks become ubiquitous in people's lives, users depend on networks a lot for sufficient communication and convenient information access. However, networks suffer from security issues. Network security becomes a challenging topic since numerous new network attacks have appeared increasingly sophisticated and caused vast loss to network resources. Game theoretic approaches have been introduced as a useful tool to handle those tricky network attacks. In this paper, we review the existing game-theory based solutions for network security problems, classifying their application scenarios under two categories, attack-defense analysis and security measurement. Moreover, we present a brief view of the game models in those solutions and summarize them into two categories, cooperative game models and non-cooperative game models with the latter category consisting of subcategories. In addition to the introduction to the state of the art, we discuss the limitations of those game theoretic approaches and propose future research directions.**

***Index Terms*—Network security, Game theory, Attack-defense, Security assessment.**

I. Introduction

PEOPLE benefit greatly from the applications of network technologies, but they also encounter challenges of network security. Networks provide users with a convenient way to access information and a sufficient communication channel to communicate. Unfortunately, networks have many security issues including: Internet attacks, cyber crimes, flooding Denial of Service (DoS) attacks, illegal data access, data stealth, etc. Network attacks can cause public institutions or private entities to lose money, important data, or their reputations. Reports of new hackers, cyber crimes, and cyberspace incidents [1], [2], [3] indicate that network security is a challenging topic.

The traditional solutions to network security have shortcomings. These solutions are implemented either by employing a preventive device, such as a firewall, or a reactive device, such as an anti-virus program, or by using them together; however, these types of solutions are no longer sufficient. Intrusion Detection Systems (IDSs), which are reactive devices, have become a necessary addition to every organization's security due to increasingly severe types of attacks in recent years [4]. An IDS is a software or hardware system that is used to monitor events occurring in a network or computer system [68]-[78]; an IDS is also used to analyze these events in order to determine whether an attack has occurred using such methods as attack signature identification, pattern detection, and statistical analysis [5]. Once an attack is detected, a report is sent to the network administrator and he/she will act to stop or mitigate the attack. Some types of IDSs are capable of reacting to a detected attack without notifying the administrator [6], and such reacting IDS are called Intrusion Prevention Systems (IPSs). Two weaknesses of IDSs are that they are not very sophisticated and that they rely on ad hoc schemes and experimental work [7]. Due to these, IDSs need design tools to handle sophisticated, organized attackers.

Game theoretic approaches have been proposed by many researchers to improve network security. On the one hand, the weakness of traditional solutions to network security is their lack of a quantitative decision framework [8]. Game theory addresses problems in which multiple players with contradictory incentives or goals compete with each other; it can provide a mathematical frame for analyzing and modeling security problems regarding networks. Furthermore, game theory is capable of analyzing many possible scenarios (up to hundreds of thousands) before determining the appropriate course of actions [9]. This can greatly sophisticate the administrator's decision making.

On the other hand, security measurement [10] is an important aspect of network security; it is an evaluation of confidentiality, integrity, availability, vulnerability, and security risks. Network security measurement is a large category that includes the measurement of every aspect of network security. Risk assessment [11] is one of these measures. Network security measurements involve the interactions of attackers and defenders, and the result of a measurement can be affected by their interactions. For example, one of the metrics in risk assessment for a network system is the probability of it being attacked. There is a need to predict the actions of both the defenders and the attackers. Since the interaction process between attackers and defenders is a game process, game theory can be applied in every possible scenario to predict the actions of the attackers and then to determine the decisions of the defenders. Therefore, game theory-based solutions have been proposed for network security problems.

This paper presents a survey of game theoretic solutions that have been applied to improve network security. Classification of these solutions is provided in terms of the application scenarios and modeling methods of games. The purposes of this paper are to compare different game theory solutions, to discuss their limitations, and to propose new directions for research on network security problems.

The organization of the rest of the paper is as follows: Section II gives definition and classification of game theory; Section III provides a classification of the applications of game theory in network security; Section IV classifies the modeling of game theoretic approaches to network security and discusses the limitations of existing game theoretic approaches:

Manuscript received 9 April 2011; revised 17 October 2011 and 11 February 2012.

X. Liang and Y. Xiao are with Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487-0290 USA (e-mail: yangxiao@ieee.org).

Digital Object Identifier 10.1109/SURV.2012.062612.00056

Section V proposes new directions for research; and finally, Section VI concludes the paper.

II. Definition and Classification of Game Theory

Definitions of some basic game theory terms which refer to [12], [13], [14] are presented in order to help readers better understand game theory. More detailed and formal explanations of these concepts can be found in [12], [13], [14], [79], [80]. Other related papers include [51]-[67].

A. Definition

Game theory is a mathematical tool used to describe and solve games. Game theory describes a game by specifying the entities (players) involved in the game, the order in which the entities take actions (an entity's "taking action" means a move), the possible actions of the entities, each player's knowledge of the previous actions taken by another player before he/she takes action in his/her move, and each player's knowledge about the payoff function of all players. Note that game theory assumes each player is rational; this means that, when he/she responds to other players' actions, each player aims to choose the response that brings him/her the greatest benefit.

A ***Game*** includes the interactions between entities in any situation. Note that in a game, there are at least two entities. A game is non-cooperative if entities interact competitively. A game is cooperative if entities interact cooperatively.

In game theory, the following four terms are basic elements for describing a game:

- **Players**: The entities involved in a game. These entities can be people, institutions, animals, or any other things that can interact with each other.
- **Actions**: In each move of a player, he/she takes an action. Game theory assumes that each player knows the possible actions of every other player.
- **Payoff**: After all of the players have taken actions in the game, each of them will get either a negative or a positive return. The return of each player is his/her payoff.
- **Strategies**: A player's strategy is his/her plan of action that specifies which action to take based on his/her knowledge of the action history. Strategies can be pure or mixed.

Based on the assumption that the players are rational in game theory, the players will choose strategies to maximize their playoff when responding to other players' strategies. This will lead to the concept of Equilibrium in a game, which can be treated as the solution of a game.

An ***Equilibrium*** in a game is a combination of the players' strategies so that each player's strategy is the best response to the strategies of the other players. "Best" means that the strategy leads to a maximum payoff given other players' strategies. A ***Nash Equilibrium*** [13] is one kind of equilibrium that can be applied to solve the solution of a game.

B. Classification

In terms of different aspects, games can be classified in different ways. The following are three different ways of classification.

1) Based on the number of stages

The first way of classification is based on whether the game has one stage or multiple stages.

Static/Strategic Game is a one-shot game in which players take actions at the same time. A static game can be viewed as a game of imperfect information since, at each time, only one player takes his/her move [13].

Dynamic/Extensive Game is a game consisting of multiple stages or moves. The number of stages can be finite or infinite [13].

Stochastic Game is a type of dynamic game in which there is a start state and states can transit from one to another according to a transition probability; at the start state, players take actions and receive payoffs with the current state transiting to another state; this requires a certain probability based on the current state and the actions taken.

2) Based on perfect information or not

The second way of classification is based on whether the game has perfect information.

In a ***Game of Perfect Information***, each player knows all of the previous actions of players when he/she takes his/her move. An example of this kind of game is a chess game.

In a ***Game of Imperfect Information***, at least one player does not know all of the previous actions when he/she takes his/her move.

3) Based on complete information or not

The third way of classification is based on whether the game has complete information.

In a ***Game of Complete Information***, every player in the game knows all players' payoff functions. The well-known "prisoners' dilemma" is an example of this kind of game.

In a ***Game of Incomplete Information***, at least one of the players does not know all players' payoff functions.

In [13], the author identifies ***Bayesian Games*** as games of incomplete information. In Bayesian games, the term "type" is used to capture the incomplete information. The number of possible types of a player could be one or multiple. The payoff structure of each player of any type is known to all players. However, the incomplete information of the game is that at least one player does not know all of the exact types of other players with multiple possible types. Bayesian analysis is applied to predict the players' strategies. An example of Bayesian games is the auction game in [13].

III. Definition and Classification of Game Theory Applications in Network Security

In this section, a classification of applications of game theory in network security is presented. Subsection III-A gives an explanation of the terms related to the surveyed network security applications. In the subsection III-B, applications of game theory are classified into two categories; a classification for each category is presented along with a discussion of each category.

A. Definition

When defense-attack interactions in networks are discussed, they are abstracted into the following scenario: attackers launch attacks on network or computer systems, and defenders respond to these attacks. The following descriptions of terms are provided to explain this abstraction.

- **System**: In networks, a system can be a node, a device, a host, a software entity, a process, or a collection of two or more of these items.
- **Attacker**: Any person or thing that launches an attack on a system on his/her/its behalf for the purpose of damaging the system or carrying losses for the owner of the system.
- **Attack target**: The system being attacked or at risk of being attacked.
- **IDS**: A software or hardware system used to monitor the events occurring in a network or computer system and then used to analyze these events in order to determine whether an attack is occurring or has occurred [4]. In the application scenarios below, IDSs are always assumed to be error-free; in other words, the IDS will set off an alarm if there is an attack, but it will not if there is no attack. However, in most realistic scenarios, an IDS is not error-free; it usually makes two kinds of possible mistakes: false alarms (setting off an alarm when there is no attack) and missing-attacks (not setting off an alarm when there is an attack).
- **Virtual sensor**: A software agent used to monitor the system and collect data for detection purposes [15]. Virtual sensors can be regarded as a part of the IDS.
- **Defender**: An entity capable of monitoring the events occurring in the attack target, analyzing these events, determining that an attack has occurred, and responding to attacks. An IDS capable of responding to attacks on behalf of the network administrator is regarded as a defender. As introduced before, such an IDS is also called IPS. The whole composition of an IDS and the network administrator is regarded as a defender if the response to the attack is conducted by the network administrator.

B. Classification

In terms of application purpose, the applications of game theory in network security can be classified into two categories. Fig. 1 shows the relationships between these two categories.

- **Applications for analysis of network attack-defense (quantitative decision making)**: modeling the interaction between attackers and defenders as games, predicting the actions of the attackers, and determining the responding defense strategy.
- **Applications for network security and dependability** [3] **measurement**: predicting the strategies of attackers and defenders and evaluating the security of the system based on this prediction.

1) Applications for analysis of network attack-defense

As stated in the introduction, traditional network security solutions show weaknesses when they face sophisticated or well-organized attackers. These security solutions need a quantitative decision framework. Game theory can be applied to develop such a quantitative framework, which can be called an analysis of network attack-defense. It includes modeling the interactions between attackers and defenders as games, predicting the actions of the attackers, and determining the responding defense strategy. The applications for analysis of network attack-defense consist of two sub-classes: a) those for general analysis of attack-defense, and b) those for specialized analysis of attack-defense, explained in the following subsections.

a) Those for general analysis of attack-defense

This kind of application first emerges among the two kinds of analyses of attack-defense. In the problem scenario of this application, the networks are often not specific but abstract; the scenario is one attacker versus one defender, and the actions of the attacker are to attack and to do nothing. The actions of the defender are to defend and to do nothing. Furthermore, some other applications [16] present a scenario in which the defender has no perfect information as to whether one node in the network is an attacker or a normal user; it can only make inference based on its belief.

In [16], an intrusion detection method in mobile ad hoc networks is considered. Within this scenario, the defending node is not sure whether its neighbor is an attacker or a regular user and thus must infer based on its belief. The defending node can choose to defend, to take no action, or randomly to choose one of the two actions. A basic signal game [16] model is used to model the interaction between each pair of nodes consisting of a defending node and one of its neighbors; it is then used to determine the best defense strategy.

In [17], the authors analyze four competition scenarios between attackers and defenders in information warfare. Each scenario is modeled as a two-player static game. The authors illustrate how the attacker and the defender in an information warfare context may play with effective strategies.

b) Those for specialized analysis of attack-defense

Most applications fall into this sub-class. Problem scenarios of this kind of applications have at least one of the following elements: a specialized network where attack events happen (like a wireless sensor network [7] or wireless ad hoc network [18]), more complex attack or defense actions [19] (like multiple kinds of attack methods on multiple attack targets and multiple kinds of countermeasures for defending each attack targets), or a consideration of multiple stages of interaction between defenders and attackers [20]. The following examples are typical applications of this subclass.

In [43], the authors present a modeling approach for security risk management. In their approach, they consider a security organization as a combination of different divisions. As an example that they gave, a company which offers video services consists of five divisions: core networks, mobile TV infrastructure, last mile equipment, IT administrators and support, and video on-demand service. They consider the security resources, such as the budget and the investment in each division, to have a linear dependency between them, and so they consider the vulnerabilities in each division. Based on those linear dependencies, they develop two generic math

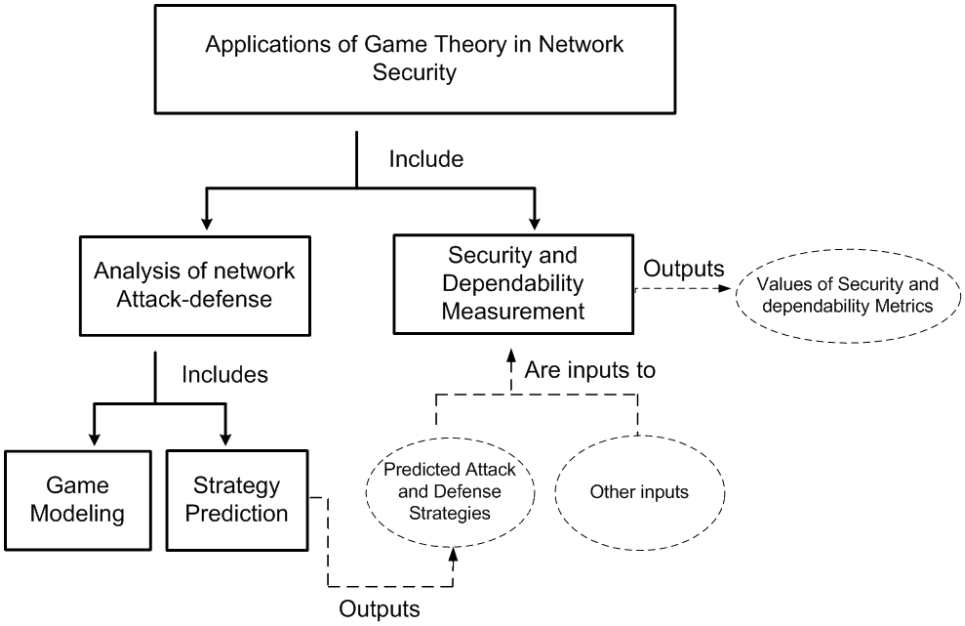

Fig. 1. Relationship among game theory applications in network security

models, with one dealing with the multiple-player (with two or more players) non-operative game between the divisions and the other addressing the operative game between them.

In [44], the authors propose a game-theory based framework for the administrator of an organization with multiple nodes or assets to choose optimal actions to diffuse the risks among the assets. Their framework includes a risk framework which captures the amounts of risks among the assets and the propagation of the risks between the assets, a discrete-time Markov stochastic model which divides the continuous space of risks in the assets into several regions and construct a concept of the transition probability matrix between different states, a game-theoretic game model which takes the current states, the further state and the strategies of the administrator and the attacker to be the factors determining the transition matrix and a saddle point method which determines the "optimal" strategy for the administer, and a Q-learning method which is employed to determine converging optimal strategies for the attacker and the administrator in the case that the transition matrix is not known. In [45], [46], with multiple users in a certain network having a pair of mainly conflicting goals, to improve the private security of themselves and to improve the public security of the whole internet, the authors propose a model to address the problem for the network users to allocate their investments in network security, i.e., how much internet users should invest to improve their private security and the public security, respectively. Their approach models this multiple-user scenario as a multiple-user non-cooperative game and defines multiple sets of pretty abstract utility functions for the users based on multiple diverse definitions of the security level. For each of the definitions of the security level, i.e., total effort, weakest-link, best shot, and weakest-target, and the security game based on that definition of the security level, the authors give a Nash Equilibrium analysis of the strategies of the users in terms of the existence and the expression of the Equilibriums.

In [48], the authors deal with jamming games in the medium access control (MAC) level of the wireless network in which each of the nodes in that network only knows its type which can be a selfish user type or a malicious user type that tries to jam the communication channel but not other nodes' type. The authors model the jamming game as a multi-stage two-player Bayesian game. The set of the transmission probabilities in random access among which a node can choose is considered the action set of the node. The utility function of a selfish user is the difference of its reward function which is an increasing function of the SINR (signal-to-inference-plus-noise rate) and the energy cost function which is an increasing function of the node's own power. The utility function of a malicious node is the difference of its reward function and its energy cost function where its reward function is the opposite of the function of the other user if the other user is a selfish user and zero if the other user is a malicious node. The authors also consider the Bayesian Nash Equilibriums in their model to be the expected strategies of the nodes.

In [42], a Fictitious Play (FP) approach is presented to model the uncertainty in multi-stage attacks. In the application scenario, the administrator of a network keeps track of the attacker's actions and targets attacked, and updates his /her defense strategy against the attack when the administrator updates his/her knowledge about the attacker's actions and targets.

In [18], the authors propose a Bayesian game approach for intrusion detection in wireless ad hoc networks. For intrusion detection in these networks, most of the existing solutions require implementing IDSs in every defending node because ad hoc networks feature decentralized management. This means that the IDS in every defending node must always be active, but always-on is insufficient since nodes in wireless networks are resource-constrained. The authors propose two methods to reduce the resource consumption of each defending node: 1) adapting a probability of defending

when there is a sign of attack and 2) alternatively using two different monitors: a) when an attack is probable, a lightweight monitor that consumes fewer resources, and b) a heavyweight one that consumes more resources but is more effective in attack detection and is assumed to be error-free. In the first method, a static Bayesian game between a defending node and its neighbor is modeled, and the probability of defending is obtained by solving the game. This method is better than always-on because there is the probability that the monitor does not defend when there is a sign of an attack. In the second method, two scenarios are considered: 1) one where a defending node within a wireless ad hoc network is monitoring all of its neighbors and 2) another where one node is defending against one of its neighbors. Each of the scenarios is modeled as a dynamic Bayesian game between the defending node and the neighbor(s) that it is defending. In the game, from the defender's perspective, each of its neighbors can be an attacker or a regular user, but the defender is unable to determine. Instead, the defender must consider all possible types for each of its neighbors, while all of the defender's neighbors know its type.

The dynamic Bayesian game in [18] includes multiple stages, and each of the stages is a static game. At the end of each stage, the inference made by the defending node concerning its neighbor(s) type(s) is updated using the historical profile; this profile contains the defender's observations of the actions of its neighbor(s) from the first stage up to the current stage. In each stage, the inference of the neighbor's type obtained at the end of the last stage is not used to determine the probability of monitoring but rather to determine the use of either the lightweight monitor or the heavyweight monitor. The updated inference of the type of the neighbor(s) is supposed to reflect the likeliness of an attack; if the likeliness is high, then the heavyweight monitor is used. If not, the lightweight one is used. This is better than the always-on method since, when it is used, a lightweight monitor consumes fewer resources.

The paper [6] handles the problem of how an IDS in an enterprise network should allocate defending resources when it responds to network attacks on the subsystems in the network. In this problem scenario, an erroneous IDS is deployed in a distributed way so that virtual network sensors are distributed to the subsystems of the network for the purpose of monitoring the subsystems; the subsystems can be network devices, computer programs, or processes over multiple hosts. Game theory is used to model ways to defend resources allocated to the subsystems as strategies for the IDS, and it is also used to determine which strategy is the best.

In [5], game theory is use to analyze intrusion detection in access control systems. As in [6], access control systems are deployed in enterprise networks to help protect stored information from illegal access. An IDS is integrated into the access control system, and it should respond to different attacks, like illegal accesses, against important stored information in the study. Virtual sensors are also distributed among the information storing entities in order to provide attack information to the IDS. Game theory is used to model the interaction between the attacker and the access control system and to determine which access control strategy is the best for the access control system.

In [21], the authors model the interactions between an attacker and the administrator of a local network as a two-player stochastic game. Three attack scenarios, "defacing web site," "a Dos attack," and "stealing confidential data," are addressed in the form of case studies. In each scenario, network states are introduced to reflect different levels of goal (system) vulnerability to the goal (system) of the attacker as well as multiple degrees of functional damages to the system which are caused by attacks. The optimal strategies of the attacker and of the administrator in a given system state are determined by analyzing a multi-stage game with a discount factor.

The paper [20] studies the problem of defending against denial-of-service attacks within networks. The author proposes a puzzle-based defense solution that can be distributed or non-distributed in order to cope with this kind of attack. A puzzle-based defense can be described as follows: first, a client requests a service from the service provider; the latter will then send one puzzle within the puzzle pool to the former for an answer. Finally, the service provider will assign the resource to the client if the returned answer is right. The author models the non-distributed DoS attack and the puzzle-based defense as a two-player stochastic game, and the author provides a way to gain the optimal defense strategy for the service provider; the defense strategy is in the form determined by the difficulty level of the puzzle that is sent, and this is done by selecting one puzzle from the puzzles of that difficulty level and then by sending it to the client. A distributed DoS attack on a system is considered to be a two-player stochastic game. In the game, the distributed attackers are considered to be a whole that aims to maximize its global return. The solution for the distributed DoS attack is based on the solution for non-distributed DoS attack games.

In [19], the authors address the intrusion detection problem in heterogeneous networks where IDSs are deployed to monitor the network nodes targeted by the attackers. The cases of one defender (IDS) defending an attack target against one attacker as well as multiple defenders (IDSs) defending multiple attack targets against multiple attackers are addressed. Multiple attackers and multiple defenders are viewed to attack/defend as a whole in a cooperative way in order to maximize their global payoff. Game theory is used to model this game as a static game. The best defense strategies are provided for the case where one IDS monitors each attack target and for the case where multiple IDSs can monitor each attack target; the strategy of the defender(s) is determined by the amount of defense resources that the IDSs allocate to each of the attack targets. The authors also extend the static model to a model of a Stackelberg game [14] (i.e., a two-player two-stage game of perfect and complete information).

In [7], the authors address the optimal strategy for a jamming-attack attacker and the resulting problems for wireless sensor network defense. In this network, both the attackers and the defenders are nodes that cannot transmit and receive packets simultaneously. In addition to a fraction of unsuccessfully transmitted packets resulting from the access control issue of the formal communication between the nodes, the attacker tries to send jamming packets during each transmission time slot in order to make the performance of the network as

poor as possible by adapting its medium access probability; this is the probability that the attacker sends packets during every transmission time slot while the defending node(s) tries to mitigate the jamming effects by adapting its (their) medium access probability. The best attack/defense strategies-medium access probabilities-are considered in two cases: one attacker versus one defender and one attacker versus multiple defenders. Game theory models the problem as a static game between the attacker and defender(s) in order to obtain optimal strategies for them. It is remarkable that the static game captures the power constraint of the nodes.

In [22], the author proposes a method where the defender can determine the optimal strategy to minimize the risk of this system. In the problem scenario, the attacker assails the vulnerability of the system in order to raise the system risk, and the defender attempts to repair the vulnerability in order to mitigate the system risk. A zero-sum stochastic game is used to model the interaction between the attacker and the defender.

In [23], the author proposes a fictitious play (FP) method that the defense system may use to determine defense strategies against the attacker in the case where both the attacker and the defender know their payoff functions but not their opponent's. In the fictitious play method, the defender observes the history of the attacker's actions, computes the frequency of each action, and determines the best strategy to be used in response to the attacker's strategy; from the defender's perspective, this may be a combination of the frequencies of the attacker's actions. The defenders update the frequency after observing new actions by the attacker, and they then update the best defense strategy.

There are other applications that fall into this subclass, such as in [24], [25], [26].

c) Discussions on advantages and drawbacks on the applications for attack-defense analysis

The advantages of the applications of game theory for general analysis of attack-defense interaction are its simplicity and its easiness. Since the scenario is simple, the attack-defense interaction can be modeled as a simple game, such as a two-player static game or a Bayesian game. Since game theory provides solutions for this kind of well studied game, the solution of the game is relatively easy to obtain. However, the disadvantage is its ineffectiveness in more complex problem scenarios. The advantages of the specialized analysis of attack-defense interaction are that it considers more complex or realistic scenarios and that it better captures the dynamic of the interaction. Its disadvantages are its complexity and possible lack of robustness. The game models used for this kind of analysis are more complex than those used for general analysis. The solution of the game is not easy to obtain and may require a great deal of computation, and the obtained solution may deviate from the theoretical solution; this may make the prediction of the attackers' strategies ineffective and may lead to a poor defense decision.

2) Applications for network security assessment

Security is a concept concerned with confidentiality, integrity, reliability, and availability [27].

Security measurement evaluates security level. Dependability [27] is intertwined with security, and it overlaps security in the attributes of availability and integrity. There are multiple metrics for security and dependability measurement, such as mean time to failure (MTTF), mean time to first failure (MTFF) [28], mean time between failures (MTBF) [29], mean time to next failure, and risk [11]. Also, the Price of Anarchy [50] (POA) has been proposed to be a metric to evaluate the effectiveness of the systems in terms of security. To better evaluate network security and dependability, a prediction of the actions of the attacker and defenders is needed. Network security measurements involve the interactions of attackers and defenders, and this may affect the result of a measurement. Since the interaction process between attackers and defenders is a game process, game theory can be applied to predict the actions of the attackers and to determine the decisions of the defenders. In fact, the prediction of the strategies in many approaches to security and dependability measurement is used as input for a measurement module [11], [29], [30], [31] in order to compute the metrics of security and dependability. The following are the applications of game theory for security and dependability measurement.

In [47], the authors investigate how the selfish investments of the users in networks affect the network security. The authors consider the Price of Anarchy (POA) as the metric of the effectiveness of the network system which is the ratio of the maximum sum of the social costs (utilities) of the users in a Nash Equilibrium and the sum of the social costs of the users in a Social Optimum. The authors propose a generic strategy game model and a repeated game model based on that strategy game model to capture the interdependency between the investments of the users, the heterogeneities of the user preferences in security investment and of the unit cost of investment, and the logical dependency (e.g., the imbalance of the network traffic due to a coordinator node) among the users. For two particular cases of the generic strategy game model, the Effective-Investment model (EI) and the Bad-Traffic model (BT), the authors in [47] show that the POA tends to increase with the increase of the dependency, the network size, and the imbalance of network traffic. Also, they show that the POA is bounded in the EI model. The repeated game models based on the EI and BT strategy models are studies as well. However, they adopt the ratio between the sum of the users' social costs in the "Socially Best Subgame Perfect Equilibrium" and the sum of the users' social costs in the social optimum. The authors show that in the repeated game models, better performance can be achieved than in the strategy game models in spite of the requirement of more coordination on and more information exchange between users. Moreover, the authors in [47] show that even if the security technology is improved, the effectiveness of the system will not be improved because of the users' lack of incentive of security investments. Finally, the authors in [47] consider the correlated equilibrium (CE) to capture the implicit coordination between users in the repeated EI and BT game. They show that the bounds of the POA in a discrete CE in the repeated EI and BT models are the same as those in the strategy CE and BT models, respectively.

In [29], the metrics for security and dependable measurement, the MTTF and MTFF, are studied for a defended system

(attack target) in a network; this provides an example of measuring the DNS server for a case study. Game theory is used to model the attack-defense game and to predict the strategies of both the attackers and the defenders. Based on the predicted strategies, the transition rate matrix of the continuous Markov process is obtained and then forwarded to the measurement module for input.

In [30], the following three concepts are introduced: a real time method to measure the security metrics, the mean time to next failure (MTNF), and the probability that the time until the next failure is greater than a given time for an attacker target. The interaction between the attacker and defender is modeled as a stochastic game [29] to predict the attack/defense strategy and to determine the transition matrix. A monitor consisting of distributed network sensors is used to observe the states and to use them in order to estimate the probability of current states in addition to the predicted defense/attack strategy. The estimated probability of the current state and the transition matrix are used as inputs for the security measurement module.

In [11], the authors propose a method for assessing network security risks. In this method, an attacker and a defender are modeled as two players in a static game who have action sets, {to attack, not to attack} and {to defend, not to defend}, respectively. This simple game ensures that both their strategies and the probabilities to attack and to defend are far easier to predict than in the aforementioned stochastic game model. The risk metric in the paper is a function of the probabilities of attacking and of defending.

In [31], the problem of quantifying the network situational awareness (NSA), a security metric, is addressed using game theory to predict the strategies of the attacker and the defender. The model method of the attack-defense play is the same as that in [29]. The NSA of the network-a function of the strategies of the attacker and the defender-is interpreted as the number of requests per unit of time from users, where there are service providers in the network such as http servers, ftp servers, and NFS servers.

IV. Classification of Game Modeling

All game theoretic approaches applied in network security require attack-defense; the interactions between attackers and defenders may be modeled as games which may then be described and solved using game theory. The previous sections have shown this fact. As follows, the classification of the game models for modeling attack-defense interactions is presented. These models may be placed into two classes, cooperative game models and non-cooperative game models, with non-cooperative game models including two subclasses, static games and dynamic games. Moreover, within static game subclass and dynamic game subclass, game model can be further grouped in terms of whether they are of complete information and whether they are of perfect information. The approaches also require the solutions of the game for predicting the actions of attackers and for determining defense strategies. The methods of obtaining the solutions to these games are also presented. In [32], a classification of the games in network security is presented as a conference paper; the classification in our paper differs from theirs in [32] in that 1) we added new game models which have not been surveyed before such as cooperative game models [43], multiple(more than two)-player security game models [43], [45], [46], [47], security investment game models [45], [46], [47] and newly proposed security game models such as those in [44], [29], [19]; 2) we classify stochastic games into the subclass of dynamic games of imperfect rather than perfect information; 3) our paper provides a much comprehensive survey as a journal paper other than a conference paper as [32]. We feel that it is a better choice for classification to have an emphasis on game models rather than on the problem scenarios. We notice that when solving the stochastic models surveyed, each game element-a game element is associated with a state-of each game model is treated as if it were a static game of imperfect information; 4) The final difference is that discussion of the models is presented. Table I shows a way of classifying the games in network security. In subsections IV-A and IV-B, we also provide a classification of the security games according to the way of classifying games provided in [13].

A. Cooperative game models

The authors of [43] publish their work on security risk management in 2010, proposing a cooperative game model along with a non-cooperative model between multiple divisions of a security organization. One assumption on which both models base is that there are linear dependencies between the security resources in the divisions and between the vulnerabilities in those divisions. In the cooperative model, one positive influence matrix and a negative influence one are introduced based on the positive influence matrix and the negative influence matrix given in the non-operative model, representing the dependencies between the security resources and between the vulnerabilities in the divisions, respectively. To capture the positive effect of forming a coalition, any two divisions in the same coalition will have increased positive effect and reduced negative effect between them than they do without coalitions. Also to capture the cost of the coordination within a coalition, a cost function is introduced which takes a friction graph and that coalition as arguments, where the friction graph captures the degree of friction between each pair of divisions. One of the interesting conclusions is that, in the cooperative game, for two coalitions each consisting of more than one division, if and only if the price of forming a coalition per unit friction is below a threshold, they will form a new coalition.

B. Non-Cooperative game models

1) Static game models

All static games are one-shot games of imperfect information; therefore, static game models only have two subclasses — static games of complete information and static games of incomplete information. In network security context, researchers use static game models of complete information to analyze the scenario in which only the interactions between attackers and defenders are considered; however, when defenders could not always distinguish attackers from regular users, not only the interactions between attackers and defenders but

TABLE I
CLASSIFICATION OF MODELS

Cooperative games	• Coalition formation game between multiple divisions in a security organization [43] • The number of divisions can be more than two • Different coaltions can merge into one if the mergence can improve the overall unitlity. • Assume that any pair of divisions in a coalition have more positive effect and less negative effect between them than they have when they are not in the same coaliton.			
Non-cooperative games	• Complete information	• Perfect inforamtion	• Static game	• The kind of game does not exist since all static games are of imperfect information
			• Dynamic game	• Strackelberg network intrusion detection game [14]: • Two-player general-sum • One leader who moves first and one follower
		• Imperfect information	• Static game	• About how selfish investments affects network security between network users, two or more players [47] • The information security game between multiple network users about how to allocate their investments to pulic protection and their self-insurances [46] • About how users in a network should choose the public protection investment level and the self insurance investment level with those two levels conflicting to each other in terms of the investment incentive of the users, two or more players [46] • Risk assement of a network, two-player, zero-sum [11] • In heterogenous networks, two-player [19] • Information warfare, two-player, general sum [17]
			• Dynamic game	• Stochastic games [8], [20], [21], [22], [26], [29], [30], [31], [36], [37], [44] • Problem : • to determine the best strategies for the administrator to diffuse the risks among the asserts in a network against the attacker [44] • to obtain best optimal defense strategy [8], [20], [21], [36] • to evalute secutiy and dependability level [22], [26], [29], [30], [31], [37] • The state transition of a system is a Markov process [21], [29], [44] • Use Q-learning to obtain the converging optimal strategies when the transition matrix is not known [44] • Use Shapley's method [35] to calculate the Nash Equilibrium of the game [29] • Use a method called NPL_1 in [34] to obtain the Nash Equilibrium of the game [21] • Repeated security investment game between network users, two or more players [47]
	• Incomplete information	• Perfect information	• Static game	• The kind of game does not exist since all static games are of imperfect information
			• Dynamic game	• Intrusion detection in Ad hoc wireless network, two player basic signaling game [16]. • Players have little information about the payoff function of each other [39], [42] • Two-player fictitious play (FP) • Each player keeps updating the frequecy of its oppenents • Two-player Multi-stage Bayesin game in MAC level wireless jamming attack scneario with each player updating its strategy following the dynamic fictitious play [49] scheme or the dynamic gradient play scheme [49] at the end of each stage [48]
		• Imperfect inforrmation	• Static game	• The information security game between a rational expert and several naive short-sighted agents with all the users having limited informaiton about others' risk factors, more than two players [45] • Two-player Bayesian game [33] • Two-player general-sum Bayesian game [18]
			• Dynamic game	• Two-player Multi-stage Bayesin game, each player keeps updating its inference about the type of its oppenent; the solution of the game is a series of optimal one-stage strategies based on the updated inference [18] • Suggest about how to model the this kind of game and about how to solve the game [40]

also those between regular nodes and defenders should be considered, and thus the games are modeled as static game models of incomplete information in which defenders only keeps an inference of the type (malicious or regular) of another node as its opponent. The solution to a static game of complete information is the Nash equilibrium [13], and the solution to a static game of incomplete information is the Bayesian Nash equilibrium [13].

TABLE II
PAYOFF MATRICES FOR THE DEFENDER AND ITS OPPONENT WHEN THE OPPONENT NODE IS A MALICIOUS NODE [18]

	Monitor	Not monitor
Attack	$(1-2\alpha)w - c_a, (2\alpha-1)w - c_m$	$w - c_a, -w$
Not attack	$0, -\beta w - c_m$	$0, 0$

TABLE III
PAYOFF MATRICES FOR THE DEFENDER AND ITS OPPONENT WHEN THE OPPONENT NODE IS A REGULAR NODE [18]

	Monitor	Not monitor
Not attack	$0, -\beta w - c_m$	$0, 0$

a) Static game of complete information

The multiple-player non-operative model proposed in [43] dealing with the risk management for the multiple divisions in a security organization falls in this category. The model is based on the assumption of the linear dependencies between the security resources in the divisions and between the vulnerabilities in the divisions, with the dependencies represented by two matrices, the positive influence matrix and the negative influence matrix. The utility of each division is the difference between its benefit and its threat (by the attackers) cost where its benefit and threat cost are functions taking arguments as the positive influence matrix and the security resources in the divisions, and the negative influence matrix and the vulnerability in the divisions, respectively.

In [46], the authors introduce a multiple-player game model for network users to optimally allocate their investments for the public protection and their self-insurances. The utility functions of the users are abstract and general enough to capture the interaction between the multiple (could be more than two) users and the attackers. The Nash Equilibriums are considered by them to be the optimal strategies for the network users.

In [47], a multiple-player game model is proposed to analyze how the investment strategies of selfish users affect the security effectiveness in a network. Different from [46], the authors only consider the amounts of the investments without discriminating the public protection investments and the self-insurance investment. The worst-case Nash Equilibrium and the Social Optimum are obtained for the computation of the Price of Anarchy.

In [11], the authors model the attack-defense interaction for the risk assessment of a network as a general-sum, two-player static game in which the action sets of the players are simply {attack, not attack} and {defend, not defend}. The payoff functions for the players capture the damage to the system and the costs to attack and to defend. The mixed strategy Nash equilibrium is obtained as the solution of game in the form of a combination consisting of the attacking probability and the defending probability.

In [19], the authors model the attack-defense game in a heterogeneous network as a two-player static game. In the game, the false alarm rate and the detection rate of the defender's IDS is considered. The actions of the attacker are interpreted as the probabilities of attacking each of the attack targets, and the actions of the defender are interpreted as the probabilities of defending against attacks for each of the attack targets.

In [17], the authors propose a general-sum, two-player model for information warfare between attackers and defenders. The authors analyze the solution of the model in cases where there is a bold player (a player that insists on its strategy despite the strategy of the other) and in cases where the players can choose mixed strategies.

The game models in [6], [7], [25] also fall in this subclass.

b) Static game of incomplete information

The game model proposed in [47] is a multiple-player game model based on the model proposed in [46] yet with the consideration of incomplete information. The model captures the interactions of a network expert and several naive short-sighted users with the network expert having limited information about the utility functions of other users.

The authors in [33] propose a two-player Bayesian game model for the network attack-defense problem in the case that the defender does not have enough information to verify a potential attacker. This model specifies the types of the potential attacker as {good, bad} and the utility functions of the defender and attacker, if their actions and the type of the potential attacker are provided. The author points out that their Nash equilibrium is the expected-utility maximizer.

In [18], a two-player general-sum Bayesian game model is proposed for a defender which is a regular user or node in a network to update its inference in the case that it is not able to verify whether its opponent, a node interacting with it, is an attacker or a regular user. Despite the fact that the authors model a multi-stage Bayesian Game, each stage of the game is a static Bayesian game. In fact, the authors first propose a static Bayesian game model before addressing the multi-stage Bayesian model. The action set of the defender consists of "monitor" and "not monitor." If its opponent is an attacker, then the opponent's action set consists of "attack" and "not attack"; however, if its opponent is a regular user, then the opponent's action set is composed of only "not attack." When the opponent node is malicious, the payoff matrices of the defender node and the opponent are presented in Table II [18]. When the opponent is a regular node, the payoff matrices of the defender and the opponent are given by Table III [18].

In tables II and III, w is the security value of the defender which for example, can be the value of network or computer resources, the confidentiality value of secret files, or the value of the service provided by the resources defended that is defended by the defender and will be lost in a successful attack. From the definition of w, the attacker (if the opponent is a malicious node) will gain a reward w at the end of a successful attack while the defender will gain a reward $-w$ (i.e. the defender loses the security value). What is interesting is that when a false alarm happens, the as the authors define, defender will lose the security value but the opponent will gain no reward; this setting makes senses, especially in the cases that when the kind of security value is the service value provided by the defended resources and the service will be terminated or deteriorated by the false alarm. c_a and c_m denote the cost to the attacker of making an attack, and the cost to the defender of keeping the monitoring system activated, both

of which should be less than w. Note that not attacking or not monitoring takes no cost. As stated in Subsection III-A, monitor devices can be subject to two errors: missing-attacks and false alarm. The authors in [18] consider those monitoring errors; $1-\alpha$ denotes the false negative rate or missing-attacks rate which is the probability that the monitoring system indicates no attack when there is actually an attack (from statistical perspective, the null hypothesis is that there is no attack), and β represents the false alarm rate. In the above tables, the row variable represents the action of the opponent node, and the column variable represents the action of the defender. In each cell of the table, there are two values; the second value and the first represent the payoff of the defender and the one of its opponent, respectively. As shown in the tables, given each possible pair of strategies of the two nodes, the payoff of each of the nodes is an average value in terms of the probabilities of the errors in the monitoring system. For example, in the case that the opponent is a malicious node(table II), when the defender chooses strategy "monitor" and the opponent chooses "attack", with a probability $1-\alpha$ that the monitoring system will miss the attack and another probability α that the monitoring system will catch the attack, the opponent will 1) successfully attack the defended resources and thus get w as its reward leaving the defender getting $-w$ as its reward, and 2) fail to attack the resources and thus get a reward $-w$ which is opposite to the defender's reward w, respectively; Therefore, given that the pair of strategies in the example above and that the opponent is a malicious node, the payoffs of the opponent and the defender are their average rewards minus their costs of implementing their strategies, respectively, and thus are $(1-2\alpha)w-c_a$ and $(2\alpha-1)w-c_m$, respectively. The payoffs of the nodes over other pairs of strategies are defined in a similar way. Let μ_0 denote the probability according to the belief of the defender that its opponent is a malicious node. Given μ_0, the strategies of the opponent and the defender can be represented by a tuple (p,q) where p represents the probability that the opponent plays attack and q represents the probability that the defender plays monitoring. Note that based on the assumptions in the problem setting that the defender only keeps its inference (i. e. the defender's belief of the probability that the opponent is a malicious node) and that the opponent knows the defender's inference, the defender needs to consider both the cases of whether the opponent is malicious and thus will choose a strategy optimal q_E to maximize its expected payoff over the inferred probability μ_0 in response to the opponent strategy p_E which is chosen by the opponent to maximize the opponent's expected payoff. (p_E, q_E) is the Bayesian Equilibrium of this game given the defender's inference μ_0 and can be obtained by solving the following expressions:

$$p_E = \begin{cases} p_{E1} = \underset{0\le p\le 1}{argmax} \left\{ \begin{array}{l} p\cdot \left[\begin{array}{l} q_E((1-2\alpha)w-c_a) \\ +(1-q_E)(w-c_a) \end{array} \right] \\ +(1-p)[q_E\cdot 0+(1-q_E)\cdot 0] \end{array} \right\} \\ \text{if the opponent is malicious;} \\ P_{E2}=0 \\ \text{if the opponent is regular.} \end{cases}$$

$$q_E = \underset{0\le q\le 1}{argmax} \left\{ \begin{array}{l} \mu_0 \left[\begin{array}{l} q\left[\begin{array}{l} p_{E1}((2\alpha-1)w-c_m) \\ +(1-p_{E1})(-\beta w-c_m) \end{array} \right] \\ +(1-q)\left[\begin{array}{l} p_{E1}(-w) \\ +(1-p_{E1})\cdot 0 \end{array} \right] \end{array} \right] \\ +(1-\mu_0)\left[\begin{array}{l} q[(1-p_{E2})(-\beta w-c_m)] \\ +(1-q)[(1-p_{E2})\cdot 0] \end{array} \right] \end{array} \right\}$$

By getting one solution from the expressions above (note that there may be multiple solutions for the expressions and thus there may be multiple BNEs for the game), the authors present one of the BNEs (p_E, q_E) over μ_0 as follows,

$$(p_E, q_E) = \begin{cases} (p^*, q^*) & \text{if } \mu_0 > \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}, \\ (\overline{p}, 0) & \text{if } \mu_0 < \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}. \end{cases}$$

where $p^* = \begin{cases} \frac{\beta w+c_m}{(2\alpha+\beta)w\mu_0} & \text{if the opponent is malicious node,} \\ (0 & \text{if the opponent is a regular node.} \end{cases}$

, $q^* = \frac{w-c_a}{2\alpha w}$, and $\overline{p} = \begin{cases} 1 \text{ if the opponent is malicious,} \\ 0 \text{ if the opponent is regular.} \end{cases}$.

The above analysis about the BNE is static which is based on the latest inference μ_0 of the defender in some stage of the game. Actually, the authors later consider the game as a multiple-stage game at each stage of which, the defender updates its inference based on the history of the actions played by both the nodes so as to get its inference to better reflect the exact type of the opponent. The defender's inference updating process is as follows: with latest version of interference, the optimal strategies of the defender and its opponent are obtained; the optimal strategies and the opponent's observed actions are then utilized to compute a newer inference via a type of posterior estimation. This process can be expressed as follows [18]:

$$\mu_j(\theta_i|a_i(t_k), h_i^j(t_k)) = \frac{\mu_j(\theta_i|h_i^j(t_k))P(a_i(t_k)|\theta_i, h_i^j(t_k))}{\sum_{\overline{\theta}_i}\mu_j(\overline{\theta}_i|h_i^j(t_k))P(a_i(t_k)|\overline{\theta}_i, h_i^j(t_k))},$$

where nodes j and i denotes the defender and it opponents, repestively, $a_i(t_k)$ represents the action of player i at stage t_k, $h_i^j(t_k)$ is the history actions of node i observed by node j from stage t_0 to stage t_{k-1}, $P(a_i(t_k)|\theta_i, h_i^j(t_k))$ represents the probability that $a_i(t_k)$ is observed at stage t_k under the condition that the type of the opponent (node i) is θ_i and that the defender (node j)'s observation $h_i^j(t_k)$ on θ_i the history actions of the opponent (node i), and $\mu_j(\theta_i|a_i(t_k), h_i^j(t_k))$ represents the probability as the updated inference of node j that the type of node i is θ_i under the condition that the observed history actions of node i is $h_i^j(t_k)$ and that the action of node i at stage t_k is $a_i(t_k)$.

2) Dynamic game models

While static game models in network security only consider one-short attack-defense interactions, in dynamic game models, a network security game is considered as a multiple-stage process in each stage of which attackers and defenders play their actions in response to the history outputs of the game. Dynamic game models in network security consist of the following four subclasses: those of complete and perfect information, those of complete and imperfect information,

those of incomplete and perfect information and those of incomplete and imperfect information. In dynamic models of complete information, only the interactions between defenders and attackers are considered with an assumption that defenders are able to discriminate attackers from regular users; for network security scenarios in which the assumption above does not hold, researchers employ dynamic models of incomplete information. Dynamic games of perfect information such as the stackelberg game in [14] and the fictitious play in [39] indicates that in each stage of a game, parties (including defenders and attackers) play actions in turns and that when a party plays its action, it already knows the history actions of other parties and itself; In other dynamic games in which the parties either play actions at the same time in each stage of the game or take turns to play in each stage but have little information about the history actions in that stage when they play, researchers view the games as dynamic games of imperfect information. Existing stochastic network security game models which are dynamic games of complete and imperfect information according to our classification reflect researchers' view that the possible situations in a network security game or conditions of the defended resources in the game can be switchable between each other as a result of the actions of the parties in the game and random factors on a no-attack basis (e. g., the likelihood that the defending system is down from a normal condition even when there is no attack can be one of those factors).

a) Dynamic games of complete and perfect information

In [19], the authors propose a model of a general-sum, two-player dynamic game with complete and perfection information as an extension of their static game model; this game is called a Stackelberg network intrusion detection game. In the Stackelberg game [14] model, the authors consider both the case in which the attacker moves first in the game and the defender follows and also the case in which they exchange roles. Each action in the players' action sets is specified as either attacking or defending each of the attack targets with a certain probability. The Nash equilibriums for both cases are used to determine which role is better for each of the players. The Nash equilibrium of the Stackelberg game is also called the Stackelberg equilibrium [13].

b) Dynamic games of complete and imperfect information

The authors of [29] view the security game as a two-player zero-sum stochastic game [29] between the attacker and defender. The authors argue that, without the defense/attack interaction, the state of the targeted system is subject to change due to the normal use of the system (e.g., the administrator could carelessly refigure the system or the system could occasionally restart); therefore, the process of the state change can be modeled as a continuous-time Markov process with a transition rate matrix. Each entity in the matrix reflects the effect on the normal use of the system of the state change. The authors propose that the interaction between the attacker and the defender affects the transition rate matrix, which means that, in the case of the security game, the transition rate matrix depends on the strategies that the attackers and defenders choose and the effects of normal use. Furthermore, a Markov Decision Process (MDP) [34] (a kind of discrete-time Markov process) in which the transition probabilities depend on both the actions and the current state can be derived from the continuous time Markov process. Based on this idea, the security game is modeled as follows [29]:

1) Identify the elements of the game, which are the states that are vulnerable to attack (system failure states not included). According to one example (a DNS server) in the paper, the game elements Γ consist of three states, denoted by Γ_V, Γ_L and Γ_{IS}, respectively, which are the good state with vulnerability, the state in which it is possible to insert false entries in the server cache, and the state of false integration. In actuality, the possible states of the DNS server also include the good state with no vulnerability, the software failure state, and the hardware failure state. However, they are not included in the elements of the game because, in these states, the attacker has no way of harming the system (e.g., when the system is in the good state with no vulnerability) or no way to further damage the system (e.g. when the system fails).

2) Build action sets that capture the possible attack and defense methods in the security game for the two players; the state set of the stochastic game includes the possible states of the system. The action sets of the attacker and of the defender depend on the system state. In system state i, the action set of the attacker is denoted by $A_i = \{a_1, a_2, ..., a_{m_i}\}$, and the action set of the defender is denoted by $D_i = \{d_1, d_2, ..., d_{n_i}\}$.

3) For every pair of actions for the defender and attacker, determine the probabilities of state transition from one game element to another. These probabilities are provided by the derived MDP. Let $P_{ij}(a_k, d_l)$ denote the probability that the system state transitions to state l from state i, with the attacker and the defender taking actions a_k and d_l, respectively.

4) Determine the payoff function in each state element. In each state element and for each action pair of the player, the payoff function of the attacker is: a) an instant value in addition to the maximum expected future payoff of the next play if it successfully attacks and if the state transitions to another game element or b) an instant value if it does not. Finally, there is a payoff matrix for each game element. The payoff matrix can be denoted as follows [29]:

$$\Gamma_i = \begin{pmatrix} & d_1 & ... & d_{m_i} \\ a_1 & \gamma^i_{11} & ... & \gamma^i_{1m_i} \\ ... & ... & ... & ... \\ a_{n_i} & \gamma^i_{n_i1} & ... & \gamma^i_{n_im_i} \end{pmatrix},$$

where $\gamma^i_{kl} = \begin{cases} \gamma^i_{kl} + \sum_j p_{ij}(a_k, d_l)\Gamma_j & \text{for successful attacks,} \\ c^i_{kl} & \text{otherwise.} \end{cases}$

and γ^i_{kl} and c^i_{kl} are the instant values.

From the payoff functions, the game dynamic can be interpreted as follows: the attack-defense game can only start at the vulnerable state; if the attacker chooses not to attack or the defender responds to the attack, the game ends; if the attack is successful and the state transitions to any other than the game elements (vulnerable states), the game ends;

or if the attack is successful and the state transitions to any of the game elements, the game continues with a new play. The payoffs of the game capture both the instant effects of the player interaction on the system and any future effects on the system. Let $\pi_i = (\pi_i(a_1), ..., \pi_i(a_{m_i}))$ and $\theta_i = (\theta_i(d_1), ..., \theta_i(d_{n_i}))$ denote the strategies of the attacker and the defender in system state i. The Nash Equilibrium can be denoted as $(\pi^*, \theta^*) = ((\pi_V^*, \theta_V^*), (\pi_L^*, \theta_L^*), (\pi_{IS}^*, \theta_{IS}^*))$, where $\pi_i^* = \max_{\pi_i} \min_{\theta_i} E(\pi_i, \theta_i)$ and $\theta_i^* = \min_{\theta_i} \max_{\pi_i} E(\pi_i, \theta_i)$. Here $E(\pi_i, \theta_i) = \sum_{\forall a_k \in A_i} \sum_{\forall d_l \in D_i} \pi_i(a_k)\theta_i(d_l)\gamma_{kl}^i$. The solution to this game is a Nash Equilibrium for each game element, but it is difficult to obtain the solution because the payoff functions are not defined explicitly. The iterative method in [35] is used to solve the game, and the authors provide an iterative algorithm for the solution; details about the algorithm can be found in [29]. It is noteworthy that the iterative method is valid only when the game is a zero-sum game.

Lye et al. [21] model the network attack-defense game as a two-player general-sum discounted stochastic game [34]. The stochastic game model proposed is a Markov Decision Process in which the decisions are the action pairs of the players. The game can be viewed as plays in a sequence of time steps, where the system states in the time steps are random variables. In any time step, the players can take actions and they will gain a value for that time step based on the actions and the system state; at the next time step, the players can take actions, and so on. If, in each time step, the player holds the same strategy pair, the strategies are called stationary strategies. For a pair of players in a stage with stationary strategies, the authors define the return of each player as the expected value of the weighted sum of its gains from the current time step and the following infinite number of time steps. The weight is a discounted weight that is a positive real range between 0 and 1. The Nash Equilibrium in each state is a combination of the strategies of the players that maximize the returns. It is proved in [34] that the Nash Equilibrium for this game exists. The authors use a method of NLP-1 in [34] to obtain the Nash Equilibrium.

In [44], the authors propose a stochastic game-theory model for the administrator of an organization with multiple nodes or assets to choose optimal actions to diffuse the risks among the assets. The action sets of the administrator and of the attacker consist of the possible defending probability distributions and the attacking probability distributions among the assets, respectively. The states of the system in the stochastic game are represented by the risk levels. A saddle point method is applied to determine the "optimal" strategy for the administrator. In the case that the transition matrix is not known, the Q-learning method is employed to determine converging optimal strategies for the attacker and the administrator.

In [47], based on the strategy/static game model which is also presented in [47] and introduced above, the authors considered a multiple-player multi-stage game model with each stage has the same game structure as that static game model. In this model, the computation of Price of Anarchy requires obtaining the Socially Best Subgame Perfect Equilibrium and the Social Optimum. The game models in [8], [20], [22], [26], [30], [31], [36], [37] also fall into this subclass.

c) Dynamic games of incomplete and perfect information

The paper [16] models intrusion detection in ad hoc wireless networks as a two-player basic signaling game [38]. In the model, a defender has incomplete information for determining the type of its opponent, which can be either an attacker or a regular node. The possible actions of the defender are to defend or not to defend, while its opponent can attack actively or act passively if the latter is an attacker; in contrast, it can attack passively or act normally if the latter is a regular node. The optimal strategies of the game are interpreted as perfect Bayesian equilibrium [13] for a basic signaling game.

In [39], for the case in which the attacker and the defender have limited knowledge about their opponents' payoff functions, the authors model this attack-defense interaction as a two-player fictitious play (FP). The best strategy for the defender is determined and updated based on the computed frequencies of the actions of the attacker. The authors considered the case in which the observation of the attacker's actions is subject to error and the case in which it is error-free. In [42], the authors also propose the use of fictitious play to deal with the uncertainty in multi-stage attacks between one attacker and the attacked entity. Similar to [18], the authors in [48] propose a two-player multi-stage Bayesian game to model the MAC level jamming attack games in wireless network. The type of each of the two nodes in the network is either a jamming attacker type or a selfish user type. The action set of each node is the possible transmission probabilities of that node. However, the authors propose two schemes of "gradient play" and "fictitious play" for each node to update their actions at the end of each stage.

d) Dynamic games of incomplete and imperfect information

In [18], the authors propose a two-player multi-stage Bayesian game to model security games in which the players have incomplete information. The solution to that game model can be obtained as follows: at each stage of the game, the players' optimal strategies for that stage are obtained based on their inferences of their opponents' types; at the end of a stage, each player updates its belief about the type of its opponent based on the current optimal strategies, the current belief of the type of its opponent, and the history of observed actions of its opponent. The procedure of updating the belief of the defending node, the optimal strategies of the defending node, and the defended node based on the newest belief have been summarized in the static game model part within this section. The author proves that these beliefs and optimal strategies in every game stage compose a Perfect Bayesian Equilibrium (PBE).

The authors in [40] describe how to model the interaction between an attacker and a defender. They suggest that the attack-defense interaction with incomplete information should be modeled as a repeated game of incomplete information. They match different network security scenarios to different game models and equilibriums for the processes of attacking and defending in different scenarios to equilibriums in game theory. They also suggest a way to present the payoffs and strategies of the attacker and defender in a game theory context as well as a way to match the components of the scenario

to the components in game theory. They present a list of terms in game theory and interpret them in a network security background. They also suggest that the Mini-Max Theorem [12] and the linear program [41] be used to solve this kind of two-player zero-sum game.

C. Discussion on game modeling

These studies show that the modeling network security game is still an ad hoc scheme that depends on the problem/application scenario. For example, if the security game is played between one attacker and one defender, then it should be modeled as a two-player game. If there are multiple stages for attacking and defending between attackers and defenders, a dynamic game such as a stochastic game is used as a model. An IDS's ability to detect attacks plays an important role on the modeling of security games. If the IDS is error-free, the security game is better modeled as a game of perfect information. If it is not, the game should be modeled as a game of imperfect information.

The limitations of the existing game models are as follows.

1) Generally, they lack scalability. As we see, most of the game models for security games are two-player games; for the problem scenarios with multiple attackers versus multiple defenders, the security game is in most cases modeled as a two-player game in which the whole of the attackers is treated as one player, as is the whole of defenders [7], [19], [20];

2) The static model is not very realistic in most scenarios where the interactions between the attackers and the defenders are a series of events;

3) The stochastic models always assume that, in each state, the defender and the attacker can detect the system state with no error, but this is not true in many realistic cases where the IDSs are erroneous;

4) Stochastic models have shortcomings since they assume the states of the system are finite; however, the states of the system seem to be continuous although some models such as [44] have scheme to partition the continuous state space into finite parts;

5) Some of the stochastic game models [22], [29] are not very realistic because they assume that the game of attacking and defending is a zero-sum game. Contrastingly, a general-sum game model is more realistic.

V. Future Research Directions

We have discussed the shortcomings of the current game-theoretic approaches in network security. Possible future research directions for network security include:

1) As we review above, there are only a couple models addressing three or more players' interaction with a focus on including multiple defenders. Therefore, building game models involving three or more players for more network security application scenarios and addressing application problems in which multiple attackers can launch attacks in a non-competitive way is one of the future research directions. Consider as an example of those application scenarios the jamming attack problem in wireless networks where two or more of the neighbors of a defending node try to jam the network without cooperating.

2) Improving the existing stochastic game models by including an infinite state assumption to make the model more realistic and then solving the game. Note that the existing solutions to the stochastic game models are valid only when the state is finite.

3) Studying the construction of payoff functions on network security game models for network security and determining a guideline or set of standards for constructing payoff functions. The payoff functions in the existing security game models seem to rely on ad hoc schemes. However, predicting the strategy of the attackers and determining the best response strategy for the defenders depends on the payoff function. Improper payoff functions in a game model can reduce the effectiveness of the prediction of the attack-defense strategies.

VI. Conclusions

This paper provides a survey and classifications of existing game theoretic approaches to network security. In spite of their limitations, game theoretic approaches have shown that they are both powerful tools for solving network security problems and that new game theoretic approaches should be a pool of research directions on network security. Our terminology on the classification of existing game theoretic approach should be subject to changes due to the fact that new game theoretic approaches always become available. From this review, readers should gain better understanding on the existing game theoretic approaches, and some insights on the further research directions on network security issues.

Acknowledgment

This work is supported in part by The U.S. National Science Foundation (NSF), under grants: CNS-0716211, CCF-0829827, CNS-0737325, and CNS-1059265.

References

[1] "Security focus," security focus bugtraq vulnerability notification database, 2009. Available: http://www.securityfocus.com/archive.

[2] "US-CERT," United States Computer Emergency Readiness Team, 2009. Available: http://www.us-cert.gov.

[3] Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang, and H. Deng, "A Survey of Cyber Crimes," (Wiley Journal of) Security and Communication Networks, Vol. 5, No. 4, pp. 422-437, Apr. 2012.

[4] R. Bace and P. Mell. Intrusion detection systems. NIST Special Publication on Intrusion Detection Systems. Available:http://www.snort.org/docs/nist-ids.pdf.

[5] T. Alpcan and T. Baser, "A game theoretic analysis of intrusion detection in access control systems," *Proc. 43rd IEEE Conference on Decision and Control*, Vol. 2, pp. 1568-1573,2004.

[6] M. Bloem, T. Alpcan, and T. Basar, "Intrusion response as a resource allocation problem,". *IEEE Conference on Descision and Control*, pp. 6283-6288, 2006.

[7] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," In *Proc. IEEE International Conference on Computer Communications* (INFOCOM), pp. 1307 - 1315, 2007.

[8] T. Alpcan and T. Baser, "An intrusion detection game with limited observations," *Proc. 12th Int. Symp. on Dynamic Games and Applications*, 2006. Available: http://www.tansu.alpcan.org/papers/isdg06.pdf.

[9] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari, "The role of game theory in information warfare," *Proc. 4th information survivability workshop* (ISW-2001/2002), 2002. Available: http://www.cert.org/research/isw/isw2001/papers/index.html.

[10] *Security measurement- white paper*, http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf.

[11] W. He, C. Xia, H. Wang, C. Zheng, and Y. Ji, "A game theoretical attack-defense model oriented to network security risk assessment," *2008 International Conference on Computer Science and Software Engineering*, pp. 498 - 504, 2008.

[12] G. Owen, *Game Theory*. Academic Press, 3rd edition, 2001.

[13] R. Gibbons, *Game Theory for Applied Economists*. Princeton University Press, 1992.

[14] M. J. Obsborne and A. Rubinstein, *A course in game theory*. MIT Press, 1994.

[15] D. Zamboni, "Using internal sensors for computer intrusion detection," Ph.D. dissertation, Purdue University, August 2001.

[16] A. Patcha and J. Park, "A game theoretic approach to modeling intrusion detection in mobile ad hoc networks," *Proc. 2004 IEEE workshop on Information Assurance and Security*, pp. 280 - 284, 2004.

[17] J. Jormakka and J. V. E. Molsa, "Modelling information warfare as a game," *Journal of Information Warfare*, Vol. 4(2), pp. 12-25, 2005.

[18] Y. Liu, C. Comaniciu, and H. Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks," In *Proc. 2006 workshop on Game theory for communications and networks*, 2006.

[19] L. Chen and J. Leneutre, "A game theoreticcal framework on intrusion detection in heterogeneous networks," *IEEE Trans. Inf. Forens. Security*, Vol. 4, No. 2, pp. 165-178, June 2009.

[20] M. Fallah, "A Puzzle-based defense strategy against flooding attacks using game theory," *IEEE Transactions on Dependable and Secure Computing*, Vol. 7, No. 1, pp. 5-19, 2010.

[21] K. Lye and J. Wing, "Game strategies in network security," *International Journal of Information Security*, Vol. 4, No. 1-2, pp. 71-86, 2005.

[22] C. Xiaolin, T. Xiaobin, Z. Yong, and X. Hongsheng, "A markov game theory-based risk assessment model for network information systems," *International conference on computer science and software engineering*, Vol. 3, pp. 57-61, 2008.

[23] K. C. Nguyen, T. Alpcan, and T. Basar, "Security Games with Incomplete Information," *Proc. 2009 IEEE International Conference on Communications* (ICC 2009), Dresden, Germany, pp. 1-6, June 2009.

[24] Z. Chen, "Modeling and defending against internet worm attacks," PhD Dissertation at Georgia Institute Of Technology, 2007.

[25] L. Carin, G. Cybenko, and J. Hughes, "Cybersecurity strategies: the QuERIES methodology," *IEEE Computer*, Vol. 41, Issue 8, pp. 20-26, 2008.

[26] K. Sallhammar, B. Helvik, and S. Knapskog, "On stochastic modeling for integrated security and dependability evaluation," *Journal of Networks*, Vol. 1, No. 5, pp. 31-42, September 2006.

[27] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable Secure Computing*, Vol. 1, Issue 1, pp. 11-33, January-March 2004.

[28] John A. Buzacot,. "Markov approach to finding failure times of repairable systems" *IEEE Trans. Reliab.*, Vol. R-19, Issue 4, pp. 128-134, November 1970.

[29] K. Sallhammar, S. Knapskog, and B. Helvik, "Using stochastic game theory to compute the expected behavior of attackers," In *Proc. 2005 International Symposiu on Applications and the Internet Workshops* (Saint2005), pp. 102-105, 2005.

[30] K. Sallhammar, B. Helvik, and S. Knapskog, "Towards a stochastic model for integrated security and dependability evaluation," In *Proc. First International Conference on Availability, Reliability and Security* (AReS), 2006. Available: http://www.sis.pitt.edu/~dtipper/3957/Paper11.pdf.

[31] H. Wang, Y. Liang, and X. Liu, "Stochastic game theoretic method of quantification for network situational awareness," In *Proc. 2008 International Conference on Internet Computing in Science and Engineering*, pp. 312-316, 2008.

[32] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya and O. Wu, "A survey of game theory as applied to network security," In *Proc. 43rd Hawaii International Conference on System Science*, pp. 1-10, 2010.

[33] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies," *ACM Trans. Information and System Security* (TISSEC), Vol. 8, Issue 1, pp. 78-118, 2005.

[34] J. Filar and K. Vrieze, *Competitive Markov decision processes*. Springer, Berlin Heidelberg. New York, 1996.

[35] L. Shapley, "Stochastic games," *Proc. National Academy of Science USA*, Vol. 39, Issue 10, pp, 1095-1100.

[36] K. C. Nguyen, T. Alpcan, and T. Basar, "Stochastic games for security in networks with interdependent nodes," *Proc. Intl. Conf. on Game Theory for Networks* (GameNets), pp. 697-703, 2009.

[37] K. Sallhammar, B. Helvik, and S. Knapskog, "A framework for predicting security and dependability measure in real-time," *International Journal of Computer Science and Network Security*, Vol. 7 No. 3, pp. 169-183, March 2007.

[38] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge. MA: MIT Press, 2002.

[39] K. C. Nguyen, T. Alpcan, and T. Basar, "Security games with incomplete information," *Proc. IEEE Intl. Conf. on Communications* (ICC), pp. 1-6, 2009.

[40] X. You and Z. Shiyong, "A kind of network security behavior model based on game theory," *Proc. Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies*, pp. 950-954, 2003.

[41] H. Greenberg.,"How to analyse the results of linear program- part 3: infeasibility diagnoses," *interfaces*, Vol. 23, No. 6, pp. 120-139, 1993.

[42] Y. Luo, F. Szidarovszky, Y. Al-Nashif, and S. Hariri, "Game Theory Based Network Security," *Journal of Information Security*, Vol. 1, pp. 41-44, 2010.

[43] W. Saad, T. Alpcan, T. Basar and A. Hjørungnes, "Coalitional game theory for security risk management," In *Proc. 5th Intl. Conf. on Internet Monitoring and Protection*, pp. 35-40, 2010.

[44] P. Bommannavar, T. Alpan and N. Bambos, "Security Risk Management via Dynamic Games with Learning," *IEEE International Conference on Communications*, pp. 1-6, 2011.

[45] J. Grossklags, B. Johnson and N. Christin, "When information improves information security," In *Proc. 2010 Financial Cryptography Conference* (FC'10), 2010. Available: http://people.ischool.berkeley.edu/~johnsonb/Welcome_files/When_Information_Improves_10.pdf.

[46] J. Grossklags, N. Christin, and J. Chuang, "Secure or insure? A game-theoretic analysis of information security games," In *Proc. 2008 World Wide Web Conference* (WWW'08), pp. 209-218, 2008.

[47] L. Jiang and V. Anantharam, "How bad are selfish Investments in network security?" *IEEE/ACM Trans. Netw.*, Vol. 19, No. 2, pp. 549-560, 2011.

[48] Y. Sagduyu, R. Berry and A. Ephremides, "Jamming games in wireless networks with incomplete information," *IEEE Commun. Mag.*, Vol. 49, Issue 8, pp. 112-118, 2011.

[49] J. S. Shamma and G. Arslan, "Dynamic fictitious play, dynamic gradient play, and distributed convergence to Nash equilibria," *IEEE Trans. Autom. Control*, Vol. 50, No. 3, pp. 312-327, Mar. 2005.

[50] E. Koutsoupias and C. H. Papadimitriou, "Worst-case equilibria," *Annual Symposium on Theoretical Aspects of Computer Science*, pp. 404-413, 1999.

[51] H. Chen and B. Sun, "Editorial," *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 65-66.

[52] M. Barua, X. Liang, R. Lu, X. Shen, "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing ," *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 67-76.

[53] N. Jaggi, U. M. Reddy, and R. Bagai, "A Three Dimensional Sender Anonymity Metric," *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 77-89.

[54] M. J. Sharma and V. C. M. Leung, "Improved IP Multimedia Subsystem Authentication Mechanism for 3G-WLAN Networks," *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 90-100.

[55] N. Cheng, K. Govindan, and P. Mohapatra, "Rendezvous Based Trust Propagation to Enhance Distributed Network Security," *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 101-111.

[56] A. Fathy, T. ElBatt, and M. Youssef, "A Source Authentication Scheme Using Network Coding," *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 112-122.

[57] L. Liu, Y. Xiao, J. Zhang, A. Faulkner, and K. Weber, "Hidden Information in Microsoft Word," *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 123-135.

[58] S. S.M. Chow and S. Yiu, "Exclusion-Intersection Encryption," *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 136-146.

[59] D. Walker and S. Latifi, "Partial Iris Recognition as a Viable Biometric Scheme," *International Journal of Security and Networks*, Vol. 6 Nos. 2-3, 2011, pp. 147-152.

[60] A. Desoky, "Edustega: An Education-Centric Steganography Methodology," *International Journal of Security and Networks*, Vol. 6 Nos. 2-3, 2011, pp. 153-173.

[61] N. Ampah, C. Akujuobi, S. Alam, and M. Sadiku, "An intrusion detection technique based on continuous binary communication channels,"

International Journal of Security and Networks, Vol. 6 Nos. 2-3, 2011, pp. 174-180.

[62] T. Choi, H.B. Acharya, and M. G. Gouda, "Is that you? Authentication in a network without identities," *International Journal of Security and Networks*, Vol. 6 No. 4, 2011, pp. 181–190.

[63] Q. Chai and G. Gong, "On the (in) security of two Joint Encryption and Error Correction schemes," *International Journal of Security and Networks*, Vol. 6, No. 4, 2011, pp. 191 - 200.

[64] S. Tang and W. Li, "An epidemic model with adaptive virus spread control for Wireless Sensor Networks," *International Journal of Security and Networks*, Vol. 6, No. 4, 2011, pp. 201 - 210.

[65] G. Luo and K.P. Subbalakshmi, "KL-sense secure image steganography," *International Journal of Security and Networks*, Vol. 6, No. 4, 2011, pp. 211 - 225.

[66] W. Chang, J. Wu, and C. C. Tan, "Friendship-based location privacy in Mobile Social Networks," *International Journal of Security and Networks*, Vol. 6, No. 4, 2011, pp. 226 - 236.

[67] X. Zhao, L. Li, and G. Xue, "Authenticating strangers in Online Social Networks," *International Journal of Security and Networks*, Vol. 6, No. 4, 2011, pp. 237 - 248.

[68] B. Sun, F. Yu, K. Wu, Y. Xiao, V. C. M. Leung, "Enhancing Security using Mobility-Based Anomaly Detection in Cellular Mobile Networks," *IEEE Trans. Veh. Technol.*, Vol. 55, No. 4, July 2006, pp.1385-1396.

[69] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," *IEEE Wireless Commun. Mag.*, Special Issue on Security in Wireless Mobile Ad Hoc and Sensor Networks, Oct. 2007, pp. 56-63.

[70] B. Sun, K. Wu, Y. Xiao, and R. Wang, "Integration of mobility and intrusion detection for wireless Ad Hoc networks," (Wiley) *International Journal of Communication Systems*, Vol. 20, No. 6, pp. 695-721, Jun. 2007.

[71] B. Sun, Y. Xiao, and R. Wang, "Detection of Fraudulent Usage in Wireless Networks," *IEEE Trans. Veh. Technol.*, Vol. 56, No.6, Nov. 2007, pp. 3912 - 3923.

[72] B. Sun, Y. Xiao, and K. Wu, "Intrusion Detection in Cellular Mobile Networks," *Wireless Network Security*, Springer, 2007, ISBN-10 0-387-28040-5, ISBN-13 978-0-387-28040-5, Chapter 8, pp. 183-210.

[73] F. Hu, Y. Malkawi, S. Kumar, and Y. Xiao, "Vertical and Horizontal Synchronization Services with Outlier Detection in Underwater Sensor Networks," (Wiley) *Wireless Communications and Mobile Computing* (WCMC), John Wiley & Sons, Vol. 8, No. 9, Nov. 2008, pp. 1165 - 1181.

[74] S. Ozdemir and Y. Xiao, "Outlier Detection Based Fault Tolerant Data Aggregation for Wireless Sensor Networks," *Proc. 5th International Conference on Application of Information and Communication Technologies* (AICT2011).

[75] B. Sun, X. Jin, Y. Xiao, and R. Wang, "Enhancing Security using Mobility Profile for Wireless Networks," *Proc. GLOBECOM 2006.*

[76] B. Sun, Y. Xiao, R. Wang, and S. Guizani, "Enhancing Security using Calling Activity for Wireless Networks," *Proc. GLOBECOM 2006.*

[77] B. Sun, N. Chand, K. Wu, and Y. Xiao, "Change-Point Monitoring for Secure In-Network Aggregation in Wireless Sensor Networks," *Proc. IEEE GLOBECOM 2007*, pp. 936-940.

[78] B. Sun, X. Jin, K. Wu, and Y. Xiao, "Integration of Secure In-Network Aggregation and System Monitoring for Wireless Sensor Networks," *Proc. IEEE ICC 2007*, pp. 1466- 1471.

[79] X. Liang and Y. Xiao, "Bio-inspired True Coalition Formation on Intrusion Detection by Mobile Robots," *Proc. CollaborateCom09.*

[80] X. Liang and Y Xiao, "Studying Bio-inspired Coalition Formation of Robots for Detecting Intrusions Using Game Theory," *IEEE Trans. Syst. Man Cybern., Part B*, Special Issue on Game Theory, Vol. 40, No. 3, June 2010, pp. 683-693.

Xiannuan Liang is a graduate student of Dept. of Computer Science at the University of Alabama. He received his BS and MS degrees in mathematics from Jilin University, China, in 2004 and 2007, respectively. Under the supervision of Prof. Yang Xiao with the Department of Computer Science, University of Alabama, his current research areas are sensor networks and wireless networks.

Yang Xiao worked in industry as a MAC (Medium Access Control) architect involving the IEEE 802.11 standard enhancement work before he joined Dept. of Computer Science at The Univ. of Memphis in 2002. Dr. Xiao is currently with Dept. of Computer Science at The Univ. of Alabama. He was a voting member of IEEE 802.11 Working Group from 2001 to 2004. He is an IEEE Senior Member. He serves as a panelist for the US National Science Foundation (NSF), Canada Foundation for Innovation (CFI)'s Telecommunications expert committee, and the American Institute of Biological Sciences (AIBS), as well as a referee/reviewer for many national and international funding agencies. His research areas are security and communications/networks. He has published more than 200 refereed journal papers (including 50 IEEE/ACM transactions papers) and over 200 refereed conference papers and book chapters related to these research areas. Dr. Xiao's research has been supported by the US National Science Foundation (NSF), U.S. Army Research, The Global Environment for Network Innovations (GENI), Fleet Industrial Supply Center-San Diego (FISCSD), FIATECH, and The University of Alabama's Research Grants Committee. He currently serves as Editor-in-Chief for *International Journal of Security and Networks* (IJSN) and *International Journal of Sensor Networks* (IJSNet). He was the founding Editor-in-Chief for *International Journal of Telemedicine and Applications* (IJTA) (2007-2009).