sensors

MDPI

Review

Game Theory Meets Wireless Sensor Networks Security Requirements and Threats Mitigation: A Survey

Mohamed S. Abdalzaher [1,2,*], Karim Seddik [3], Maha Elsabrouty [1], Osamu Muta [2], Hiroshi Furukawa [2] and Adel Abdel-Rahman [1]

1 Electronics and Communications Engineering Department, Egypt-Japan University of Science and Technology (E-JUST), Alexandria 21934, Egypt; maha.elsabrouty@ejust.edu.eg (M.E.); adel.bedair@ejust.edu.eg (A.A.-R.)

2 Kyushu University, Fukuoka 819-0395, Japan; muta@ait.kyushu-u.ac.jp (O.M.); furuhiro@ait.kyushu-u.ac.jp (H.F.)

3 Electronics and Communications Engineering Department, American University in Cairo, Cairo 11835, Egypt; kseddik@aucegypt.edu

* Correspondence: mohamed.abdelzaher@ejust.edu.eg; Tel.: +81-80-855-39852 or +2-011-178-25787

Academic Editors: Ignacio Bravo, Esther Palomar, Alfredo Gardel and José Luis Lázaro
Received: 22 May 2016; Accepted: 24 June 2016; Published: 29 June 2016

Abstract: We present a study of using game theory for protecting wireless sensor networks (WSNs) from selfish behavior or malicious nodes. Due to scalability, low complexity and disseminated nature of WSNs, malicious attacks can be modeled effectively using game theory. In this study, we survey the different game-theoretic defense strategies for WSNs. We present a taxonomy of the game theory approaches based on the nature of the attack, whether it is caused by an external attacker or it is the result of an internal node acting selfishly or maliciously. We also present a general trust model using game theory for decision making. We, finally, identify the significant role of evolutionary games for WSNs security against intelligent attacks; then, we list several prospect applications of game theory to enhance the data trustworthiness and node cooperation in different WSNs.

Keywords: game theory; WSNs security; evolutionary game; game-theoretic based trust model; WSNs applications

1. Introduction

Security and authentication in Wireless Sensor Networks (WSNs) face a more challenging environment compared to traditional networks. WSN has an ad-hoc nature in which the nodes can dynamically enter or leave the network, which leads to a variable network topology. Consequently, there is no predefined route for data replication. With the ambiguity of the nodes involved, a critical problem may occur when a malicious intruder attacks the system. In addition, power limitation can turn the node itself to behave selfishly in order to conserve its energy, which increases the risk of network malfunctioning. Therefore, the above-mentioned aspects of the WSNs make the security schemes in WSNs more challenging and vulnerable. For this reason, security in WSNs has gained increasing interest. Some techniques were developed to meet different WSNs security threats mitigation [1–4]. There are other techniques that are used for protection in WSNs that rely on the reputation principle [5–18]. These reputation-based techniques are out of the scope of this survey paper since our main focus in this paper is on game-theoretic-based protection techniques.

Game theory is a modern branch of intelligent optimization [19–27]. It tackles problems where cost functions of different entities are mutually dependent [19,22–27]. Since the rise of game theory in the late 1940s, it has been widely applied to model the behavior in a variety of applications.

In [28], the authors discuss the promising features of game theory approaches for the wireless networks, while in [29,30], different trends of using game theory for WSNs have been reviewed. Recently, with the emergence of infrastructure-less and distributed systems, game theory has found its way in decentralized communication systems [31]. One of the problems in this category is related to security in WSNs. The security situation, which involves an interaction between the defender(s) and attacker(s), can be directly mapped to a game among players in which each player strives to promote its benefit. More particularly, having the action of the attacker(s) or the defender(s) depending on the counter-action of the other party places game theory as a perfect fit for this security model [22,24–26,32].

In this paper, we introduce a brief interpretation of the different game techniques presented in the literature to address WSN security. In addition, an overall view of the desired WSN properties in terms of security fulfillment is presented. We study the game theory based approaches for mitigating different WSN security threats from the state-of-the-art literature on the topic. We classify those approaches into two main categories, namely, cooperative games and non-cooperative games, and each summarizes the involved defense strategies based on game theory. Then, we propose a taxonomy of game theoretic defense strategies taking into consideration the attacked layer, attack features, attack consequences, convenient defense game approach, and game type. Afterward, a general trust model based on the discussed game theory approaches and scenarios is introduced to take into account the variability and features of the attack types. Consequently, we would utilize this model to any network environment (cooperative/non-cooperative game with internal/external attack). Finally, we present some applicable future trends for the interested researchers, showing the capability of facing intelligent attacks [33–36] using the evolutionary game approach [37–39].

The rest of the paper is structured as follows. Section 2 provides a brief overview about game theory. Section 3 outlines game theory classifications, addresses the different game types that are involved in WSN security, and provides the security properties needed for WSN security. Section 4 illustrates the proposed taxonomy of game theory defense strategies for WSN security showing the types of attacks and the types of suitable games to mitigate these attacks. Section 5 presents the proposed general trust model based on the discussed game theory types and attack types in WSNs. In Section 6, the applicable future trends are listed. Section 7 concludes the paper.

2. Game Theory: A Brief Overview

Game theory is an advanced branch of intelligent optimization. The model of game theory represents a game between player groups that choose to behave cooperatively or non-cooperatively and try to promote their benefits (payoffs) through the used strategy(ies) executed through the cumulative players actions. [19,20] survey the fundamental definitions of game parameters, which can be summarized as follows:

Definition 1. *A game is a description of the strategic interaction between opposing, or cooperating, interests where the constraints and payoff for actions are taken into consideration.*

Definition 2. *A player is a basic entity in a game, which is involved in the game with a finite set of players denoted by N that is responsible for taking rational actions denoted by A_i, for each player i. A player can represent a person, machine, or group of people within a game.*

Definition 3. *The Utility/Payoff is the positive or negative reward to a player for a given action within the game denoted by $u_i : A \rightarrow \mathbb{R}$, which measures the outcome for player i determined by the actions of all players $A = \times_{i \in N} A_i$, where the symbol $\times$ denotes Cartesian product.*

Definition 4. *A strategy is a plan of action within the game that a given player can adopt during game play denoted by a strategic game $\langle N, (A), (u_i) \rangle$.*

In the security field, game theory application is not only limited to counteracting the effect of external intruders; it can be used to detect the malicious nodes and reveal the nodes that behave selfishly and overburden the whole network. Generally, Nash equilibrium (NE) is the intelligent solution for the social problems that has become a promising concept for wireless networks and more specifically for WSN security [19–21,29,40,41].

Definition 5. *Nash equilibrium is a profile of optimal actions, $a^* \in A$, such that any player $i \in N$ cannot benefit due to unilaterally deviating from its strategy and choosing another action [21,41]. This can be translated in terms of the utility function as, $u_i\left(a_i^*, a_{-i}^*\right) \geq u_i\left(a_i, a_{-i}^*\right)$ for all $a_i \in A$, where a_i denotes the strategy of player i and a_{-i} denotes the strategies of all players other than player i [19].*

In Section 3, an overview of the different game types is briefly introduced, focusing on the games that can be particularly useful to describe the security situation in WSN.

3. Games Theory for WSNs Security

The different game types that are commonly used to model WSNs security issues can be classified to cooperative games and non-cooperative games as shown in Figure 1. The cooperative games are represented by cooperating nodes aiming at maximizing the whole networks security against different security threats. On the contrary, the non-cooperative games involve the conflicting individual actions for which every node aims at maximizing its own payoff that opposes the others' outcomes. Figure 1 lists the different types of games that have been used to model security problems in WSNs (Figure 1 does not present a classification for games in general, but presents the games that have been used in the literature to model WSNs security problems). In this section, a brief description of the different involved games for mitigating WSNs security threats is provided. Then, the WSN security requirements are discussed.

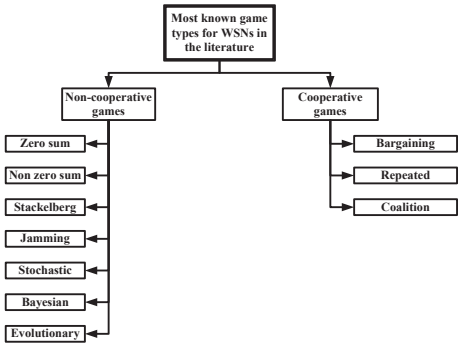

Figure 1. Cooperative and Non-cooperative Game Classification for Addressing WSN Security Issues.

3.1. Cooperative Games

The common types of cooperative games that are used to resolve different WSN security issues are presented as follows.

3.1.1. Bargaining Game

The Bargaining game represents a problem between two competitors (agents) who should cooperate; in other words, the bargaining or Nash bargaining game is modeled based on the bargaining interaction concept between two players, who request a fraction of the same benefits [21,42–45]. It can be used to model resource allocation in wireless communication networks, in which the agents aim to exploit the same spectrum, which should be fairly allocated. In Nash bargaining game, if the total requests by the two players are greater than the available resources, both requests are discarded. Conversely, if their requests are less than the available resources, both requests are

accomplished. Pareto-inefficient is a result of non-cooperating players, which is solved by a Nash bargaining solution [46].

3.1.2. Repeated Game

The repeated game is fundamentally considered as an interaction between two individual players who repeatedly play the game [19,21,47–49]. This game is also known as iterated game [47] which consists of some repetitive stages. Each stage has two players at which the current action is taken into consideration in the subsequent actions of the other players. The repeated games can be classified into two categories: finitely repeated games and infinitely repeated games [47]. In the finitely repeated games, the time period is fixed and thoroughly known. This category has a drastic defect which permits the player to act selfishly and NE equals the *minmax* payoff. Consequently, the punishment is not sufficient in this case. The infinitely repeated game represents the most popular notion in which the game is probably played for infinite times. The punishment is defined in this case as reducing the payoff that the non-cooperating player earns based on his reputation. The reputation is computed based on the players' interactions.

3.1.3. Coalition Game

The coalition game is a result of cooperation among a set of players acting as one player against the others aiming at maximizing the mutual outcome [21,28,50,51]. This coalition mutual benefit called coalition value. Coalition games are classified into two forms, namely, strategic form and partition form [28]. In the former case, the coalition value depends on the number of participant players in the coalition regardless of their network establishment. Conversely, in partition form, the establishment represents the intrinsic role for the coalition value [28].

3.2. Non-Cooperative Games

The common types of non-cooperative games that are used to mitigate different WSN security problems are presented as follows.

3.2.1. Zero-Sum Game

The zero-sum game is one of the types of non-cooperative games between two players. One player is considered a maximizer that strives to maximize its gain while the other is considered to be the minimizer that aims to minimize its losses [52,53]. Consequently, it seems as a two-side conflict game or a one-side win game, at which the total utility/payoff of both players remains constant during the course of the game, $\sum_{i=1}^{2} u_i(s) = 0 \; \forall \; \mathbf{s} \in S$, where **s** is a strategy profile [21]. Apparently, **constant-sum game** could be transformed to an equivalent zero-sum game; and zero-sum game is a special case of constant-sum game given that the players add up their gains or losses to a constant value for any strategy profile [21].

3.2.2. Nonzero-Sum Game

Nonzero-sum game is played between two or more players where the sum of players' utilities is not constant during the course of the game [19,54]. In nonzero-sum games, all players are considered maximizers or minimizers which have no constraints on the total utility as in the zero-sum game [54]. Consequently, all the participants can gain or lose together [21].

3.2.3. Stackelberg Game

The Stackelberg game is used to model two competitive players [21,47]; one is a game initiator (leader) who chooses an action from a set A_1 then the second player traces the leader's action and chooses an action from a set A_2. This scenario is widespread in securing different WSNs where the defender acts as a leader and the attacker plays the role of the follower [2,55–57].

3.2.4. Jamming Game

The jamming game represents a scenario between the WSN defender player against the jamming attack. The attack aims to disrupt the transmitted data stream [58,59]. The jamming game is fundamentally inspired from the zero-sum game framework in which the two players aim at maximizing their conflicting utilities. Consequently, the resultant of the two utilities are zero. Interestingly, the jamming game is used to treat the complexity constraints of implanted biomedical sensors as in [60,61]. Furthermore, underwater sensor network is one of the booming applications that utilize the concept of jamming game [59].

3.2.5. Stochastic Game

The stochastic game is one of dynamic games that are played in a sequence of stages [21,62]. The stage is formulated based on a probabilistic transitions by one or more players [21,62–65]. The new state of the game is random which depends on the previous players' actions [21,62].

3.2.6. Bayesian Game

The Bayesian game falls under the non-cooperative game framework, in which the players have some information shortage while executing their actions. In other words, Bayesian game could be suitable for modeling the incomplete information interactions between players. Accordingly, a player can estimate the other players' payoffs [19,21]. Moreover, a game theoretic approach based on Bayesian game has been developed to do intrusion detecting for wireless nodes in [66].

3.2.7. Evolutionary Game

The evolutionary game is fundamentally applied for the biological networks in which the players can combine pure and mixed strategies with rational behavior to enhance some population characteristics [21]. Moreover, different WSNs applications have been modeled using evolutionary game in [67–75].

3.3. Security in WSNs: Requirements

WSNs have emerged in the recent years because of their features and the applications that they can be used in. Due to these substantial reasons some requirements should be maintained for WSNs security as follows [76,77]:

- **Confidentiality:** A transmitted data to a specific sensor node must not be understood by any other node in WSNs.
- **Integrity:** The transmitted and received data must not be maliciously altered by the participant sensor nodes in WSNs.
- **Authentication:** A sensor node uses the data authentication to verify that the received data is actually sent by the claimed sender in WSNs.
- **Authorization:** The authorization is used to guarantee that the authorized sensor nodes are only able to perform certain operations in WSNs.
- **Availability:** The WSN services must be available whenever the WSN users need them.
- **Freshness:** The data produced by the WSN sensor nodes must be neoteric.
- **Forward and backward secrecy:** Forward secrecy is used to prevent a sensor node that has left a WSN from reading any future data. Backward secrecy means preventing a new comer to a WSN from reading any previous data.

4. Game Theory Defense Strategies Against WSN Attacks

In this section, we propose a study of the state-of-the-art on different game trust models for WSNs security. More concretely, we propose a classification of the game theory defense strategies for confronting the WSN attacks. The classification will be carried out based on the attack type, the

attacked layer, the attack being passive or clear, the attack being internal or external, the attack feature, the attack consequences, the suitable defense strategy based on game theory, and the game type.

4.1. WSN Attack Types vs. Corresponding Layer

WSNs are suffering from several attack types that target different layers. In [33,34,76,78,79], WSN attacks are classified based on the layer attacked and the countermeasures which can be summarized as follows. The physical layer (L1) is prone to jamming and tampering attacks in which the attacks target L1 features. The data link layer (L2) attacks (e.g., sniffing, collision, exhaustion, unfairness, stealthy, etc.) aim for deteriorating the layer facilities such as media access techniques. The network layer (L3) can be affected by certain attacks such as spoofed altered relayed information, Sybil, wormhole, etc. More specifically, these attacks aim to corrupt the network layer routing protocols. Finally, the transport layer (L4) would be infected by some attacks (e.g., desynchronization, flooding, etc.) that aim at disrupting the layer functions such as the end-to-end protocols.

4.2. Internal and External Attacks

In this section, the WSN attacks are categorized into internal and external attack [33] based on an extensive review of the literature. Internal WSN nodes that act selfishly or maliciously are considered as internal attacks, while the external attack is performed by some external entities aiming at deteriorating the WSNs functionality.

4.3. Clear and Passive Attacks

We present a study of the previous work that involved the clear and passive attacks taking into consideration the role of game theory.

4.3.1. Clear Attack

The clear attack is capable of disrupting the traffic stream. It can transmit, respond, modify, and/or delete specific messages inside the stream due to the manipulation that the attacker applies. This attack can impersonate one end of a conversation or a third party. Consequently, it can prevent the infected sensor node from communicating with others.

The following papers consider the clear attack types in WSNs. In [80], the authors propose a defense attack strategy which concentrates on the jamming attack. An intrusion detection system is introduced against the attacks based on the NE concept that represents a defense strategy against the most vulnerable sensor nodes [41,81]. In [2], the attack targets the data trustworthiness of the sensor network which is mitigated by a game theoretic approach to protect the sensor nodes based on a trust score of the data item observed by those nodes. Consequently, the higher the data items trust scores are, the more trustful the nodes are. In [53], a deleterious attack scenario is considered, where a node turns malicious and then drops selected packets from a traffic stream.

Interestingly, clear attacks can cause some manipulations to the whole sensor network. Therefore, a great deal of information is needed for the defense mechanisms to be able to mitigate this type of attacks. For example, a malicious sensor node has the ability to drop incoming packets or issue route error messages to misdirect the path (e.g., blackhole attack) as presented in [82]. Also, in [83], the authors propose a game-theoretic approach to confront the attack impact of dropping the passing messages within a cluster.

4.3.2. Passive Attack

The passive attack has the ability to capture the transmitted traffic without disturbing the network. In other words, it eavesdrops the incoming traffic stream without modification. The inherent risk of this attack is that the attack targets the sensitive data (e.g., the encryption codes). Moreover, this attack can represent selfish sensor nodes which strive to save their power as maximum as possible. For example,

the selfish nodes go to sleep mode without a permission from the network administration, whether these nodes are involved in cooperative or non-cooperative games. Furthermore, the malicious nodes that aim at saving their power consumption by ignoring packet forwarding to their neighbors are also considered passive attack.

The following papers consider different types of WSN passive attacks. In [84], a bargaining game is introduced to confront the passive attack due to the selfish behavior of some of visual event-driven sensors. This represents a highly sensitive and vulnerable application in which the selfish nodes tend to conserve their power. In addition, in [42], the authors propose Nash bargaining games, which lead to the system Pareto optimality aiming at optimizing the network reliability. In [85], the authors consider a form of passive attack where a selfish sensor saves its power by going to sleep mode without a permission, by deceiving the network intrusion detection system (IDS). In [77], a game theoretic approach is proposed to address the passive DoS attack that causes malfunction of the forwarding mechanism of sensor nodes at which the nodes agree to forward packets but fail to do so. Furthermore, in [76], a win-lose scenario is used to model the relationship between the system and the attacker using a zero-sum game to secure the forward data path in which the attack strives to drop the passing packets. In addition, a sampling mechanism, inspired from the learning automata methodology, is applied in this game-theoretic context to treat the passive attack impact based on the reward and punishment technique [86].

4.4. Cooperative and Non-Cooperative Games

In the following discussion, we summarize the different game defense strategies against different attack types in WSNs. A game can be chosen to be cooperative or non-cooperative game according to the attack type and the expected penalty.

4.4.1. Cooperative Games

The cooperative games can be used to model strategies that require cooperation among the participant WSN nodes to combat the different attacks. The utility function in the cooperative games is commonly represented by three main parameters, namely, cooperation, reputation, and security level between the cooperating nodes. More concretely, the NE is used as a promising notion to reach the optimal solution in different WSNs [83]. Cooperative game theories for WSNs security can be summarized as follows.

- **Bargaining Game**: A bargaining game is presented in [42] through the cooperating nodes, resulting in a Nash Bargaining Solution and Reliability in Wireless Body Sensor Networks (WBSNs). This seeks to promote the cooperation between the nodes to maximize the performance in a multi-hop WBSN and hence, the utility function distinguishes the allocated bandwidths. Three main parameters should be taken into consideration: dynamic nature, quality-of-service (QoS), and fairness of resource allocation. In [44], the power allocation problem is addressed using bargaining NE leading to cooperative relaying. The proposed model aims at achieving the optimal signal-to-noise ratio (SNR) in WSNs. In [45], the authors propose the bargaining game to attain the optimal energy management policy for a solar-powered sensor node. The proposed model obtains the optimal sleep and wake up mode for the participant sensor nodes based on the bargaining NE by treating the selfish nodes that conserve energy through blocking packets with high probability. The players' utility function is denoted by the combination between the probability of an active mode, a sleep mode, a listen mode, a packet block, and a packet drop for the two competitive players.
- **Repeated Game**: In [49], the authors propose a game theoretic approach based on repeated game to investigate the selfish nodes throughout in CSMA/CA network. The model stimulates the selfish nodes to cooperate leading to the Pareto optimality NE. In this model, the utility

function is presented as the difference between the throughput and a punishment factor of the participant nodes.

In [85], the authors propose a specific technique controlled by the network base station to be able to detect and prevent the selfish behavior of nodes. This technique works in parallel with the Core Mesh Routing Protocol (CMP) without disrupting its functionality using a game-theoretic approach based on a repeated game to detect and prevent the selfish behavior. This game uses the power consumption as an indicator of the game utility/payoff function. Increasing the utility is considered as a positive signpost of honesty and trustworthiness and vice versa if selfish behavior is presented. Consequently, the base station investigates the utility function to ensure that whether the node is capable of going to sleep or not. The utility concentrates on the transmission cost which is based on the forwarded data. Hence, the node with the increased utility/payoff has a higher chance of going to sleep.

In [77], a repeated game is presented targeting a defense against passive DoS attack. This model applies a defense strategy at the routing layer to promote cooperation through rewarding the cooperating nodes and accumulating reputation values over time, while punishing non-cooperative passive attackers. To reach this goal, each node plays a repeated game executing series of Nash Equilibria on a utility function that balances between cooperation gain represented by the reputation value and the cost of forwarding packets to check the routing security.

- **Coalition Game**: In [84], a defense strategy is introduced to predict the attacks and their effect using cooperating camera sensors. The model is based on a threshold for the probability of error of the captured scene. This approach provides a solution for false alarm, energy conservation, early attack prediction, and selfish behavior detection.

4.4.2. Non-Cooperative Games

The non-cooperative games have been proposed to describe and model the competition between the benevolent nodes and selfish/malicious nodes. In the following we list some of the WSN security problems, which can be modeled by non-cooperative games.

- **Zero-sum Game**: In [76], a game-theoretic approach based on zero-sum game was presented seeking routing secured against external intruders. The authors have developed the utility function as a combination of the energy consumption, probability of malicious nodes, and probability of dropped packets between check nodes (one or more through the forward path) to maximize the probability of attack detection. Intrusion detection framework for smart phone systems is proposed in [41] at which two players play a non-cooperative constant-sum game with complete information to achieve NE that leads to a defense strategy for the security server. In this game, the defender wishes to enhance the security level but the attacker wants to deteriorate it. The model gathers data and checks if the security server monitors attack or not, then calculates the payoff per each case using node ID as a node identity.

  Furthermore, in [87], the authors propose an intrusion packet detection at which the classical zero-sum game is chosen as a natural model for the behavior of the attacker/defender strategies. The utility functions for both the attacker and defender take into consideration the probability of detection. In [53], a zero-sum game is proposed to mitigate the selective forwarding attack in which the infected nodes turn malicious and select some packet to drop based on a stochastic formulation. The model utility function is the difference between the defense energy budget supplied by the IDS for all participant nodes and the attack energy budget applied to turn those nodes into malicious. In [52], the authors formulate a zero-sum game aiming at maximizing the transmission capacity in underwater sensor network based on the mitigation of jammers. The utility function of this game is maximized to achieve the optimal SNR based on two observers sensor nodes against the effect of the disruption caused by the jammer.

- **Nonzero-sum Game**: In [82], a nonzero-sum game is proposed to detect the malicious nodes and their effect (e.g., dropping packets and routing error message to misdirect the path) due to the DoS attack impact. Two defense strategies are developed. The first strategy is based on dynamic source routing that aims at maximizing the payoff. The second strategy focuses on reputation and cooperation between neighbors which also aims at maximizing the payoff and enhancing the defense strategy. However, the developed algorithms suffer from unnecessary added cost in the utility function of the defender, and this cost is mainly related to continuous defending of nodes even when no attack is encountered. In [81], the authors introduce a defense strategy based on a nonzero-sum game and achieve NE using a Markov decision process to predict the most vulnerable sensor node. In [54], the proposed defense strategy aims at detecting and correcting the malicious sensor nodes that drop packets based on a nonzero-sum game using periodic collusion-resistant punishment mechanism. The model stimulates the detected malicious node(s) to react benevolently.
- **Stackelberg Game**: In [2], the attack-defense interactions are modeled using a Stackelberg game, and the NE condition is derived which is sufficient to ensure that the sensed data are truthful within a nominal error bound. The defense strategy gives an authority to the defender to be the decision maker. The model is based on a thresholding defense strategy against the attacks. The thresholding is correlated to the trust score of the data items observed by the sensor nodes to detect the effect of the followers (attacker). In [56], the authors propose a Stackelberg game for detecting the reactive jamming attack in wireless networks aiming at maximizing the signal-to-interference-noise ratio (SINR). The reactive jammer seeks to inject noise like legitimate signal at receiver. The utility function is represented by the resulting SINR, while a linear power penalty is used as a punishment for jammer and legitimate nodes. In [57], a Stackelberg game is developed to confront the external attacks manipulations based on energy defense budget against the corresponding energy attack budget. The utility function represents the resultant of the defense and attack energy budgets.
- **Jamming Game**: In [58], the authors propose a jamming game that is fundamentally inspired from the zero-sum game framework due to the uniqueness of NE. More concretely, the authors study the jamming impact on the Orthogonal Frequency Division Multiplexing (OFDM) system when the jammer is situated close to the base station. The utility function is the combination of the power level of the uncontrolled environmental noise at i-th state, the costs of power usage for transmitter and jammer, and fading channel gains for transmitter and jammer. In [59], a jamming game is proposed to mitigate the DoS attack (jamming attack) in underwater sensor network. The legal player utility function is maximized based on a combination of its power level, SINR, and transmission costs. The game model is classified into two cases. In the former case, the game is presented as a static jamming game that owns a single NE. In the latter case, the game is represented by a dynamic jamming game which is derived based on a Markov decision process. In other work, the jamming game is used to treat the complexity constraints of implanted biomedical sensors [60,61]. In these models, the utility function is presented in two cases. In the former case, the authors study a fixed strategy in which the jammer may or may not jam the i-th player. In the latter case, a mixed transmission strategy is used for the i-th player.
- **Stochastic Game**: In [64], the authors propose a new framework for wireless nodes virtualization in which the service providers and network operators are responsible for the QoS and spectrum management, respectively. The proposed model can handle the unknown dynamics in traffic characteristics and channel conditions. In addition, the network operator is responsible for calculating the NE based on the conjectural price of the communicating nodes leading to the optimal resource management.
- **Bayesian Game**: In [66], a Bayesian game is proposed to analyze the interactions between pairs of attacking/defending nodes. The Nash equilibrium is studied for the attacker/defender game through two scenarios, namely, static and dynamic. In fact, the dynamic Bayesian model

represents the more realistic approach that allows the network defender to continuously update his decision for the existing malicious nodes. Furthermore, the dynamic scenario provides energy-efficient monitoring strategies for the defender. A new approach is suggested called Bayesian hybrid detection that adopts lightweight monitoring and heavyweight monitoring mechanisms. The lightweight monitoring is utilized to estimate the adversary's actions, while the heavyweight monitoring acts as a last resort of defense.

- **Evolutionary Game**: In [67], the authors propose a data aggregation model called evolutionary game-based data aggregation model (EGDAM) in WSNs. The model uses a weighting method based on the pixel-level fusion between homogeneous sensor nodes to adapt the unreliable information from the nodes. In [68], an evolutionary game is used to maintain the cooperation in static and mobile multi-class WSNs, with each class managed by a different authority. Two scenarios are considered for the packet forwarding. In the former scenario, the packet forwarding is between mobile classes in which the game formulation is based on iterated prisoner dilemma. In the later scenario, the packet forwarding is between spatially dispersed stationary classes.

  In [69], building reliable and survivable networks with fault tolerance is reviewed based on bio-robustness of different biological scales, i.e., gene, molecular networks, immune systems, population, and community. In [70], dynamic hybrid fault models are proposed to achieve the reliability and fault tolerance for WSNs based on the evolutionary game. The dynamic models provide real-time prediction and fault-tolerance. The dynamics of the proposed models are involved into the time-dependent failure rate and time-dependent failure modes. The utility function of the proposed evolutionary game is formulated as reliability or survivability of the WSN in which a sensor node can be sacrificed to achieve the optimal network sustainability. The same concept of dynamic hybrid fault models has been extended [74] and extensively studied in [73].

  In [72], the WSN sensors are mapped as a biological population using evolutionary game in which the payoff function is represented by reliability of players. The dragonfly adult concept has been studied in [75] to guarantee optimal channel time sharing in WSNs using evolutionary game. Consequently, selfish behavior of nodes can be treated. The utility function is called fitness function that is represented by the sensors' targets. In [71], the authors propose a defense strategy for WSNs aiming at reaching a stable state between the defender and the attacker using evolutionary game. More specifically, the sensor nodes can be active and dynamic to adjust their defense strategy. The payoff function is represented by a combination of some parameters of defender and attacker, e.g., reward of successive forwarded packets, security measuring cost, successful attack, failure attack, attacking cost, and probability of successful attack attempts.

4.5. Defense Strategies Classification

Table 1 proposes a classification that addresses the WSN attacks [33] based on an extensive review of the state-of-the-art game-theoretic approaches to deal with WSNs security. In Table 1, the first column lists the WSN attacks. In the first row, we categorize these attacks based on the attacked layer [76] (i.e., physical layer (L1) attacks, data link layer (L2) attacks, network layer (L3) attacks, and transport layer (L4) attacks); this classification takes into account both the features and consequences of those attacks. Afterward, the attack is classified as internal or external; the internal attack (In) represents an internal node acting selfishly or turning malicious, while the external attack (Ex) is caused by an external attacker. Then, we pinpoint whether the attack is passive (P) or clear/active (Clr). Further, suitable defense strategy (suitable game) is presented that mitigates the attack manipulations based on both the attack type and games features as proposed in the literature. Finally, the game type is identified.

Table 1. WSN attack classifications and defense strategies based on game theory.

Attack Type	Attacked Layer	P/Clr Attack	Ex/In Attack	Attack Feature	Attack Consequences	Defense Strategy	Game Type
Jamming [55,56,59,88–90]	L1 [76,78,79]	Clr	Ex	Interfere with radio frequencies	Disrupt whole/ portion of the network	Stackelberg [55,56]/ Repeated [88]/ Evolutionary [89]/ Jamming [59,90]	NC/C/NC/NC
Tampering [91]	L1 [76,78,79]	Clr	Ex/In	Extract cryptographic keys	Create/replace existing node	Repeated [91]	C
Sniffing [92–94]	L2 [95]	Clr	Ex	Overhear essential data from neighboring nodes	Penetration network secrecy	Stackelberg [92]/ZS [93,94]	NC
Collisions [89]	L2 [76,78,79]	P	In	Simultaneous transmission on the same frequency	Change in portion of data, Checksum mismatch at receiver	Evolutionary [89]	NC
Exhaustion [96]	L2 [76,78,79]	Clr	In/Ex	Naive implementation may continuously attempt to retransmit the corrupted packets	Resource exhaustion	Repeated [96]	C
Unfairness [42,97]	L2 [78,79]	P	In	Considered weak DoS, Intermittent exploiting the resources	Miss transmission deadline for other nodes in a real-time MAC protocol	Repeated [97]/Bargaining [42]	C
Stealthy [98,99]	L2 [78]	Clr	In	Compromise a node and inject false data through that node.	Make the network accept false data	ZS [98]/ NZS [99]	NC
Energy Drain [76,98]	L2 [78]	Clr	In/Ex	Request from neighboring node to respond after massive traffic transmission	Paralyze the whole network	ZS [76,98]	NC

Table 1. *Cont.*

Attack Type	Attacked Layer	P/Clr Attack	Ex/In Attack	Attack Feature	Attack Consequences	Defense Strategy	Game Type
Conflicting behavior [100–102]	L3 [103]	Clr	In	Perform differently with different nodes	Decrease trust value of nodes by conflicting their reputation	Repeated [100–102]	C
Blackhole [82,104]	L3 [103]	Clr	In/Ex	Attract the whole traffic to be routed through it by advertising itself as the shortest route and drop all received message	Block the traffic to the sink, Expand crisis by easily combining with other extra attacker	Repeated [82,104]	C
Spoofed, altered, replayed information [66,89]	L3 [76,78,79]	Clr	In/Ex	Disrupt the network traffic	Create routing loop, Extend or shorten source route, Error message generation	Bayesian [66] Evolutionary [89]	NC
Selective forwarding [53,76,87,89]	L3 [76,78,79]	Clr	In/Ex	Transmit certain packets and drop others	A malfunction occurs in transmission process	NZS [53]/ ZS [76,87]/ Evolutionary [89]	NC
Sinkhole [82,105]	L3 [76,78,79]	Clr	In	Compromise a node and then attract the surrounding nodes to use it as next node	Lose huge number of packets, Retransmit lost packets, Increase delay, Exhaust nodes	NZS [82]/ Evolutionary [105]	NC
Sybil [66,89,106]	L3 [76,78,79]	Clr	In	One node presents more than one ID	Exhaust nodes' power	Stochastic [106]/ Bayesian [66]/ Evolutionary [89]	NC
Wormhole [82]	L3 [76,78,79]	Clr	In	Low-latency that links between two portions of the network where the messages replayed	Paralyze the whole network, Network traffic jamming	NZS [82]	NC

Table 1. *Cont.*

Attack Type	Attacked Layer	P/Clr Attack	Ex/In Attack	Attack Feature	Attack Consequences	Defense Strategy	Game Type
Hello flood	L3 [76,78,79,107]	Clr	Ex	Use high powered-transmitter to deceive neighbors that it has the trajectory towards the base station	The neighbor believe that attacker, Control the data flow	ZS * /NZS *	NC
Acknowledgment spoofing [66,89]	L3 [76,78,79]	Clr	In	Spoof the ACKs of overhead packets destined for neighboring nodes in order to provide false information to those neighboring nodes	Disrupt and confuse routing mechanism	Stochastic [66]/ Evolutionary [89]	NC
Badmouthing [108]	L3 [109]	Clr	In	Propagate negative reputation information about good nodes	Block valid path by confusing reputation system	Repeated [108]	C
Goodmouthing (opposite Badmouthing behavior)	L3 [109]	Clr	In	Propagate positive reputation information about bad nodes	Block valid path by confusing reputation system	Repeated *	C
Whitewashing	L3 [109]	Clr	In	Re-enter the network with new ID and fresh reputation	deteriorate the defense of reputation mechanism	Evolutionary *	NC
Flooding [77,110,111]	L4 [76,78,79]	Clr	Ex	An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit	System traffic congestion, Cause channel capacity deterioration	Repeated [77,110,111]	C

Table 1. *Cont.*

Attack Type	Attacked Layer	P/Clr Attack	Ex/In Attack	Attack Feature	Attack Consequences	Defense Strategy	Game Type
Desynchronization	L4 [76,78,79]	Clr	Ex	Refers to the disruption of an existing connection	Repeatedly spoof messages to an end host, causing that host to request the retransmission of missed frames	Repeated *	C
Intelligent behavior [112]	-	Clr	In	Selectively provide services good or bad, high or low values of recommendation according to threshold of trust rating	Disrupt trust system order indistinguishably, Increase the cost of reputation evaluation	Stochastic [112]	NC
DoS [77,82,104,110,113,114]	L1-L4 [76,78]	Clr	In/Ex	Prevent any part of WSNs from functioning correctly or in a timely manner	Split the network grid and take control of part of the network by inserting a new sink node jam and tampering network	Repeated [77,104,110]/ NZS [82,113,114]	C/NC
ON-OFF	-	Clr	In	Behave well or badly by exploiting the dynamic properties of trust through time-domain inconsistent behaviors	Remain undetected while causing damage	Evolutionary *	NC

Clr... Clear, P... Passive, ZS... Zero-sum, NZS... Non Zero-sum, C... Cooperative, NC... Non-cooperative, In... Internal, Ex... External; * · · · based on the attack and game features.

5. Game Theory-Based General Trust Model

The trustworthiness mechanisms are considered the foremost concern of the WSNs security specialists. Therefore, different network security frameworks are discussed in the literature [3,4,33,115]. Figure 2 shows the general process of a trust model, similar to the model considered in [116]. This trust model is divided into four main stages. The first stage involves gathering the information from the traffic stream, then followed by the second stage that applies the suitable trust model. Afterward, the analyzed data throughout the trust model is checked using the intrusion detection system within the third stage. The fourth stage is in charge of punishing or rewarding the infected or benevolent packets, respectively. This general mechanism aims at attaining energy efficient networks against the intrusion impact using the general principle of learning automata by sampling the incoming packets [86,117]. The same principle can be used to enhance WSNs security using game theory [87].

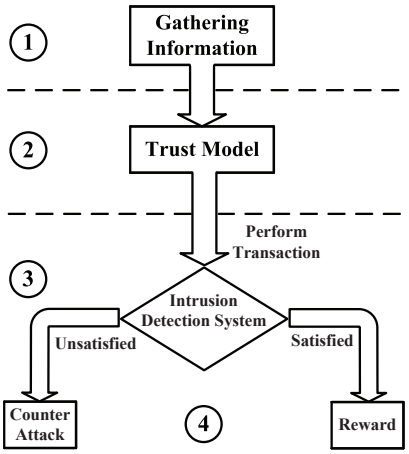

Figure 2. General Trust and Reputation Model Mechanisms.

In designing the game model, the nature of WSN should be taken into account. Maintaining the same data transfer from multiple nodes, keeping low power consumption, accommodating large number of nodes, and providing timely decision are of paramount importance to the WSN operation. In fact, the reputation is the essential factor that the different game theoretic approaches rely on to establish robust trust models against the WSN threats scenarios. In the first scenario, the model targets the selfish nodes. In the second scenario, the model addresses the malicious nodes that are considered a harm for the WSN. Finally, in the most harmful scenario, the WSN suffers from selfish and malicious nodes for which an intelligent model is desired.

In this paper, we discuss a general trust model based on game theory to mitigate the WSNs security threats leading to detecting the malicious nodes and those nodes that act selfishly. Figure 3 illustrates the data flow of the general trust model in which the selected game is used to face the designated attack based on the observed information from the whole network. Apparently, this general system collects the needed information to select the best game that fits the detected attack and the mentioned classifications in Section 4. After this, the captured data are analyzed to pinpoint the network features, attack type, and appropriate defense strategy that will be applied, whether in a cooperative or non-cooperative game.

It can be obviously seen that two possible directions are available to apply the game-theory-based defense strategy. The cooperative process is shown as follows: the cooperating WSN nodes calculate three main parameters, namely, cooperation, reputation, and security level for every participant node. Then, these parameters are listed in an information list $N(i)$. Afterward, every node is checked if it acts selfishly or maliciously. Consequently, the node is rewarded or punished. On the one hand, if the node is rewarded (benevolent node), the NE existence is checked. A timer is used as a threshold for the NE existence to reduce the risk in the real-time sensitive applications. This time out is application

dependent. Then, if NE exists, the optimal solution is achieved; otherwise, the node will be applied again to the suitable defense strategy based on game theory. On the other hand, if the node is selfish or malicious, it will be exposed to a punishment check. Consequently, if it is the first time the node acts selfishly or due to a hardware malfunction reason, a time out will be given to the node then the node status will return again to the neighbor list $N(i)$. Finally, if the node recursively behaves selfishly, the node turns malicious, or the time out expires, the node will be excluded from routing. The above is executed till reaching the NE based on the application sensitivity leading to the optimal solution.

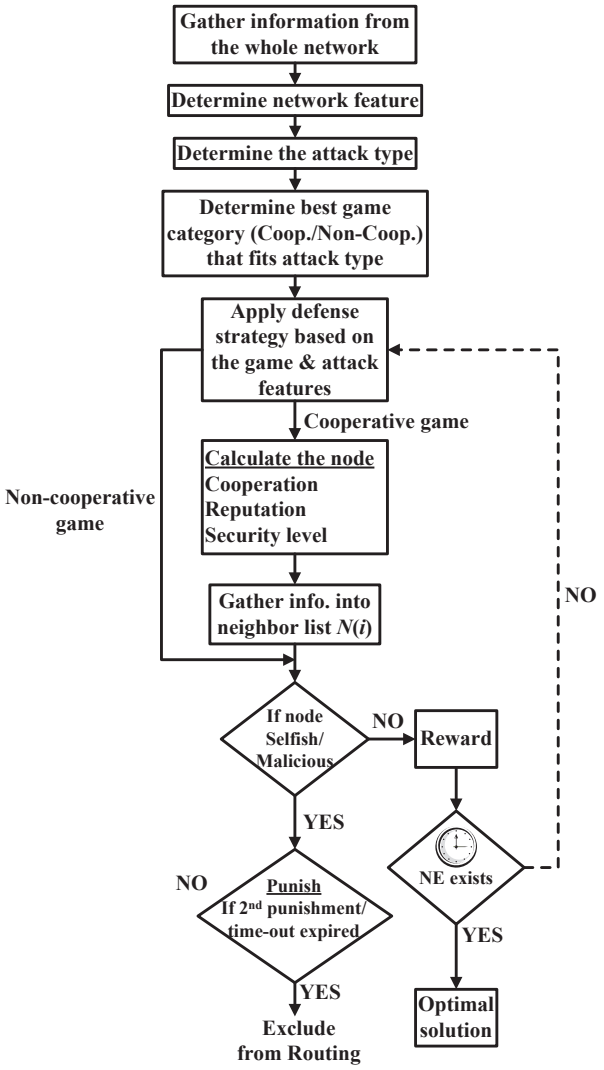

Figure 3. Proposed Game Theory Trust Model.

The non-cooperative stages are presented starting with the suitable non-cooperative game against the existing attack. Apparently, the same steps are executed as in the cooperative process but starting from the check step that determines whether the node is benevolent, malicious, or even selfish. In addition, the non-cooperative process omits two steps. The first step is calculating the cooperation, reputation, and security level parameters. The second step is collecting the neighbor list. In centralized networks, the proposed general trust model could be deployed part of a software-defined networking (SDN) at the network controller. On the contrary, the model duties could be allotted to some of the cooperating nodes in decentralized networks. More concretely, the network operator, the service provider, the cloud provider, or a combination of them, based on the network communication structure and connectivity, could control this model.

6. Applicable Future Trends

The most known cooperative game models for WSNs security are based on centralized authentication. More specifically, these models are used to handle the traffic motion, maintain the benevolent nodes, and punish the selfish or malicious nodes using the cooperating nodes. However, as there are many benefits of using the centralized authentication, there are also some problems that may cause a risk for the network security such as the resources deterioration of the centralized security node. In [31], a solution is proposed, called group authentication, to reduce the risk on the centralized node. The proposed mechanism aims at distributing the security task among different correlated nodes. Therefore, the cooperating nodes are supposed to achieve the security targets in WSNs [32]. Consequently, many benefits can be addressed in WSNs as follows: reducing the whole network delay, increasing the throughput, enhancing the detection probability of the selfish/malicious nodes, saving the power consumption, decreasing the number of error messages, promoting the WSNs performance and robustness against the effect of attacks, etc.

Among the different game types, evolutionary game presents a valuable approach in which the players are rationally adapting their actions based on the iterative development of the game [21,37,39,118]. The evolutionary game has the ability to deal with the interaction among rational biological agents in a population. In addition, evolutionary game can be classified into static and dynamic hypotheses [21]. In the static hypothesis, the evolutionary game utilizes the evolutionarily stable strategies (ESS) [21]. In the dynamic hypothesis, the replicator dynamics have been involved to model the adaptation of the strategies of the players [21]. The evolutionary game framework has some advantages over the classical non-cooperative game such as equilibrium selection, bounded rationality, and dynamic behavior of players [21]. Consequently, we envision that evolutionary game models can be used to mitigate the intelligent attacks in WSNs leading to robust systems.

6.1. Evolutionary Game for WSNs Security

WSNs rational attacks [33,34] can cause a harmful problem due to the intelligent manipulations based on some unfixed strategy. Consequently, this issue needs an intelligent defense behavior to deal with this situation. The evolutionary game can intelligently use the mixed strategy against the intelligent attack manipulations [19,21]. In other words, the evolutionary game has the ability to change the defense strategy during the game progress against malicious attacks in WSNs [37,38]. More concretely, the strategies of players are non-deterministic in which the player can select different pure strategies with a certain probability [21,48] such as the Hawk and Dove problem [21,39,118]. In addition, we can use the dynamic evolutionary game that follows the Snowdrift game [39,118,119] which proposes a different point of view away from the other biologically based games. Dynamic evolutionary game is slightly different from the Hawk and Dove game which supports both the assigned cooperator and the other players [39,118,120]. Consequently, if the evolutionary game was generally used in the general trust model in Figure 3, it would introduce an adaptable solution for the intelligent attack dilemma.

In biological terms, the biological organisms combat each other aiming at maximizing their benefit. In particular, bacteria strive to infect/control the benevolent cells [120,121]. Similarly, the intelligent attacker in WSN aims at turning the benevolent nodes to malicious or selfish nodes based on unfixed strategy as a chameleon. Consequently, WSN nodes can be modeled as biological organisms using the evolutionary game that presents a promising solution for mitigating such situations [67–75]. The evolutionary game features can be summarized as follows.

- The evolutionarily stable strategies (ESS) or evolutionary equilibrium assists in the NE perfection, specifically when multiple Nash equilibria exist.
- The evolutionary game modeling is suitable for human scenarios with agents that may not have hyper-rational or strong rational behavior.

- The evolutionary game is based on an evolutionary process due to its dynamic nature, which organizes the dynamics of interactions among agents in the population. In other words, the strategy adaptation continues over time. On the contrary, most of the traditional non-cooperative games are evolved in a static setting [21].

6.2. Intelligent Attacks

For researchers who are interested in the recent intelligent WSNs attack types [33–36], these attacks and the corresponding features would be listed in Table 2.

Table 2. WSN intelligent attacks.

Attack Type	Features
Badmouthing attack	Grants negative feedback on a node in order to disrupt its reputation.
Goodmouthing attack	Grants positive feedback about a malicious entity.
ON-OFF attack	Occurs when an adversary attempts to initiate a security attack or a mixture of attacks based irregular manner in order to make its reputation acceptable.
Sybil attack	Occurs when a node in a network claims multiple identities.
Whitewashing attack	Exists when an attacker resets a poor reputation by re-entering the system with a new identity.
Stealthy attack	Operates quietly, hides the evidence of its actions, disrupts the traffic stream from arriving the destination through malicious behavior at third party node.
Conflicting behavior attack	Deteriorates the reputation of good nodes by performing differently for different peers.
Intelligent behavior attack	Uses different behaviors based on unfixed strategy to manipulate good nodes.

6.3. Attractive WSNs Applications

In this section, we list some of the applicable recent trends of WSNs for the interested researchers. These applications can be listed as cognitive radio sensor networks (CRSNs), wireless underground or underwater sensor networks (i.e., under water sensor networks, Earthquake observation, agriculture applications, military uses, etc.), smart grid networks, power grid networks, energy harvesting, wireless body area networks (WBAN), and cyber physical systems (CPSs). The above applications present some security threats and game-theory-based approaches can prove to be beneficial to address these threats.

6.3.1. Cognitive Radio Sensor Networks (CRSNs)

In [122], recent applications of the CRSNs have been studied in which the different schemes in CRSNs can be classified into centralized, distributed, and cluster-based. More specifically, performance enhancement is the main concern (i.e., interference avoidance, throughput maximization, QoS assurance, fairness and priority consideration, etc.). The papers that concentrate on the WSN security aspects would be summarized as follows. In [123], the authors use the interference of secondary users (SUs) to improve the secrecy capacity of the primary user (PU) in CRSN. In [124], the CR security threats have been reviewed and are classified into two main categories, namely, cognitive capability, and reconfigurability. The SU is used as a relay to improve the PHY security by which PU can enhance the secrecy rate based on game theory [125]. In [126], a sequential detection mechanism is proposed in which the SU is sequentially computing the likelihood ratio to determine whether or not to stop listening. A Stackelberg game is formulated aiming at maximizing energy saving in CR networks taking into consideration the users' selfishness and intellectualism in [127]. In [128], two cooperation schemes are proposed to secure the PU transmission. In the former scheme, the PU selects two individual SUs to cooperate with, called relay-jammer scheme. One of the SUs acts as a relay and

the other is a friendly jammer. In the later scheme, the PU cooperates with a cluster of sensor nodes whereas the scheme is called cluster-beamforming.

6.3.2. Wireless Underground or Underwater Sensor Networks

The applications wireless underground sensor networks include acoustic signals such as Earthquake disaster observation, underwater sensor networks (UWSNs), agriculture applications, military uses, etc [129–131]. In [52], a Bayesian zero-sum game approach is proposed to confront the jammers intervention in order to disrupt the acoustic signals of UWSN. The model aims at maximizing the channel underwater capacity in the presence of different types of noise and jammer. In [59], a jamming game is proposed to model the interactions between jammers and underwater sensors. More specifically, the model concentrates on the reactive jammers that determine their jamming power based on the ongoing sensors' traffic stream. This jammer type is more severe than responsive jammer (i.e., constant jammers). In other words, the model proposes a learning-based anti-jamming enhancement method whereas every sensor decides its own transmit power regardless of the channel gain of the jammers.

6.3.3. Smart Grid Networks

Recently, smart grid networks have been combined with cognitive radio (CR) networks. In [132], the authors propose a trustful system for energy management in smart home, called smart home energy management (SHEM) to enhance delay sensitive data transmissions. The system uses the CR technology due to the promising features as reliable opportunistic data transmissions and strategic decision making. The proposed model is examined by being applied to model spectrum sensing data falsification (SSDF) attack behaviors.

6.3.4. Energy Harvesting

Energy harvesting is a very booming research area in WSNs because of the limited energy nature of sensor nodes [133]. In [134], a distributed MAC protocol is proposed, called Self-Learning Energy Harvesting and Spectrum Access in Cognitive Radio Sensor Networks (S-LEARN) that combines the WSN sensor nodes and the CR technology. The proposed protocol allows the sensor nodes in CRSN to get the necessary power to transmit data packets from the small amount of power the nodes can harvest wirelessly from the environment. In [135], the random behavior of energy harvesting and energy consumption in dense small cell networks have been mathematically modeled and analyzed based on a probabilistic framework. In addition, a bandit-theoretical formulation has been developed for the cooperating users when no information is supported. Bandit is a class of online optimization problems in which no prior information is provided to an agent [135]. The agent selects a finite set of arms in successive trials and every arm produces some reward. The agent captures only the reward of the played arm and not the other arms' rewards. Bandit is categorized based on the generated rewards of arms, e.g., adversarial bandits, stochastic bandits, etc. A problem occurs due to the tradeoff between taking actions that yield immediate large rewards and taking actions that might result in larger reward only in the future. A solution is proposed called policy or allocation rule that pinpoints which arm should be employed at successive rounds [135].

6.3.5. Wireless Body Area Networks (WBANs)

Wireless body area networks are of the essential real time applications. More concretely, WBAN is used to monitor human being health (i.e., temperature, blood pressure, ECG, life activity, etc.) [42]. In [136], a game theoretic approach has been proposed to resolve Socially-aware Interference Mitigation (SIM) issue in Body-to-Body networks (BBNs). The model is classified into two main channel allocation mechanisms. In the former mechanism, the BBN stage for inter-WBANs' communications is addressed. In the latter mechanism, WBAN stage for intra-WBAN communications is considered. Moreover, in [137], transmission scheduling is studied throughout a large number of gateways

connected to one base station of medical centers taking into account the QoS requirements for the different gateways. In addition, a game theoretic approach is proposed to guarantee optimal strategy between the competitive gateways that can lead to an efficient Wardrop equilibrium.

6.3.6. Cyber Physical Systems (CPSs)

Cyber Physical Systems represent the new generation of complex sensor networks that combine physical subsystems and cyber components [25,138]. Recently, CPSs have been evolved in most of control systems that rely on feedback such as power networks, social networks, smart transportation systems, sensor networks, smart buildings, etc. In [138], several future directions for sensor networks have been studied that serve CPSs based on two baselines, namely, security and privacy. Jamming attack is one of the treats of CPSs that has been mitigated by game theory models [80]. In [25], the strategic interactions between an attacker and a defender are studied using game theory in which both cyber and physical components are considered. The authors have developed and validated this model with UltraScience Net infrastructure, which was built to support high-performance network experiments. Interestingly, CPSs could be developed to combat the homeland security issues [22,23,139] based on different authorities combination to support extensive analysis leading to a robust system.

7. Conclusions

In this paper, we have addressed the important and challenging problem of assuring trustworthiness of sensor data in the presence of both selfish behavior and malicious adversaries in WSNs. We have carried out an extensive overview of the state-of-the-art of many game theoretic approaches that are utilized to design defense strategies to protect sensor nodes from attacks and to guarantee a high level of trustworthiness for sensed data. We have presented a classification for the different attack types, based on their features, and we have presented the different types of games that have been used in the literature to mitigate these attacks. We have also presented some potential future, active research trends for using game theory.

In addition, we have presented the concept of evolutionary game using a group policy/authentication to resist the intelligent attacks which do not use pure strategies. We expect astounding results after applying this model, such as reducing the number of dropped packets, promoting the efficiency, increasing the security level, managing the interactions between nodes, rapid attack detection, regenerating (based on the evolutionary nature of the game) and intelligent strategies against new manipulations of attacks, with the aim of producing powerful trust model based on game theory.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BBNs	Body-to-Body networks
C	Cooperative
CPS	Cyber Physical System
CR	Cognitive Radio
CRSN	Cognitive Radio Sensor Network
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CMP	Core Mesh Routing Protocol
Clr	Clear
DoS	Denial of Service
ESS	Evolutionary Stable Strategies
Ex	External
EGDAM	Evolutionary Game based Data Aggregation
In	Internal
IDS	Intrusion Detection System
NE	Nash Equilibrium

NZS	Nonzero-sum
NC	Non cooperative
OFDM	Orthogonal Frequency Division Multiplexing
PU	Primary User
P	Passive
QoS	Quality of Service
SDN	Software-defined Networking
SHEM	Smart Home Energy Management
SIM	Socially-aware Interference Mitigation
SINR	Signal to Interference Noise Ratio
S-LEARN	Self-Learning
SNR	Signal to Noise Ratio
SSDF	Spectrum Sensing Data Falsification
SU	Secondary User
UWSNs	Underwater Sensor Networks
WBAN	Wireless Body Area Network
WSNs	Wireless Sensor Networks
ZS	Zero-sum

References

1. Mármol, F.G.; Pérez, G.M. Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommun. Syst.* **2011**, *46*, 163–180.
2. Lim, H.S.; Ghinita, G.; Bertino, E.; Kantarcioglu, M. A game-theoretic approach for high-assurance of data trustworthiness in sensor networks. In Proceedings of the 28th International Conference on Data Engineering (ICDE), Arlington, VA, USA, 1–5 April 2012; pp. 1192–1203.
3. Rani, V.U.; Sundaram, K.S. Review of trust models in wireless sensor networks. *Int. J. Comput. Inf. Syst. Control Eng.* **2014**, *8*, 371–377.
4. Lopez, J.; Roman, R.; Agudo, I.; Fernandez-Gago, C. Trust management systems for wireless sensor networks: Best practices. *Comput. Commun.* **2010**, *33*, 1086–1093.
5. Pingel, F.; Steinbrecher, S. Multilateral secure cross-community reputation systems for internet communities. In *Trust, Privacy and Security in Digital Business*; Springer: Milano, Italy, 2008; pp. 69–78.
6. Ganeriwal, S.; Balzano, L.K.; Srivastava, M.B. Reputation-based framework for high integrity sensor networks. *ACM Trans. Sens. Netw.* **2008**, *4*, 15.
7. Boukerch, A.; Xu, L.; El-Khatib, K. Trust-based security for wireless ad hoc and sensor networks. *Comput. Commun.* **2007**, *30*, 2413–2427.
8. Zhang, J.; Shankaran, R.; Orgun, M.A.; Varadharajan, V.; Sattar, A. A trust management architecture for hierarchical wireless sensor networks. In Proceedings of the 35th Conference on Local Computer Networks (LCN), Denver, CO, USA, 10–14 October 2010; pp. 264–267.
9. Alzaid, H.; Foo, E.; Nieto, J.G. RSDA: Reputation-based secure data aggregation in wireless sensor networks. In Proceedings of the Ninth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), Otago, New Zealand, 1–4 December 2008; pp. 419–424.
10. Li, X.; Zhou, F.; Du, J. LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 924–935.
11. Shao, N.; Zhou, Z.; Sun, Z. A lightweight and dependable trust model for clustered wireless sensor networks. In *Cloud Computing and Security*; Springer: Beijing, China, 2015; pp. 157–168.
12. Chen, D.; Chang, G.; Sun, D.; Li, J.; Jia, J.; Wang, X. TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Comput. Sci. Inf. Syst.* **2011**, *8*, 1207–1228.
13. Ozdemir, S. Functional reputation based reliable data aggregation and transmission for wireless sensor networks. *Comput. Commun.* **2008**, *31*, 3941–3953.
14. Chae, Y. Redeemable Reputation Based Secure Routing Protocol for Wireless Sensor Networks. PhD Thesis, University of Rhode Island, Kingston, RI, USA, 2012.
15. Xiang, G.; Jianlin, Q.; Jin, W. Research on trust model of sensor nodes in WSNs. *Procedia Eng.* **2012**, *29*, 909–913.
16. Bao, F.; Chen, I.R.; Chang, M.; Cho, J.H. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE Trans. Netw. Serv. Manag.* **2012**, *9*, 169–183.

17. Srinivasan, A.; Teitelbaum, J.; Wu, J. DRBTS: Distributed reputation-based beacon trust system. In Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, IN, USA, 29 September–1 October 2006; pp. 277–283.
18. Dogan, G.; Avincan, K. MultiProTru: A kalman filtering based trust architecture for two-hop wireless sensor networks. *Peer-to-Peer Netw. Appl.* **2016**, 1–14, doi:10.1007/s12083-016-0446-3.
19. Wang, B.; Wu, Y.; Liu, K.R. Game theory for cognitive radio networks: An overview. *Comput. Netw.* **2010**, *54*, 2537–2561.
20. Roy, S.; Ellis, C.; Shiva, S.; Dasgupta, D.; Shandilya, V.; Wu, Q. A survey of game theory as applied to network security. In Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS), Kauai, HI, USA, 5–8 January 2010; pp. 1–10.
21. Han, Z. *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*; Cambridge University Press: Cambridge, UK, 2012.
22. Shan, X.; Zhuang, J. Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender–attacker game. *Eur. J. Oper. Res.* **2013**, *228*, 262–272.
23. Shan, X.; Zhuang, J. Subsidizing to disrupt a terrorism supply chain [mdash] a four-player game. *J. Oper. Res. Soc.* **2013**, *65*, 1108–1119.
24. Xu, J.; Zhuang, J. Modeling costly learning and counter-learning in a defender-attacker game with private defender information. *Ann. Oper. Res.* **2016**, *236*, 271–289.
25. Rao, N.S.; Poole, S.W.; Ma, C.Y.; He, F.; Zhuang, J.; Yau, D.K. Defense of Cyber Infrastructures Against Cyber-Physical Attacks Using Game-Theoretic Models. *Risk Anal.* **2015**, *36*, 694–710.
26. Guan, P.; Zhuang, J. Modeling Resources Allocation in Attacker-Defender Games with "Warm Up" CSF. *Risk Anal.* **2015**, *36*, 776–791.
27. Shan, X.; Zhuang, J. Modeling Credible Retaliation Threats in Deterring the Smuggling of Nuclear Weapons Using Partial Inspection-A Three-Stage Game. *Decis. Anal.* **2014**, *11*, 43–62.
28. Akkarajitsakul, K.; Hossain, E.; Niyato, D.; Kim, D.I. Game theoretic approaches for multiple access in wireless networks: A survey. *Commun. Surv. Tutor.* **2011**, *13*, 372–395.
29. Shi, H.Y.; Wang, W.L.; Kwok, N.M.; Chen, S.Y. Game theory for wireless sensor networks: A survey. *Sensors* **2012**, *12*, 9055–9097.
30. Benmammar, B.; KRIEF, F. Game theory applications in wireless networks: A survey. In Proceedings of the 13th International Conference on Software Engineering, Parallel and Distributed Systems (SEPADS'14), Gdansk, Poland, 15–17 May 2014; pp. 15–17.
31. Harn, L. Group authentication. *IEEE Trans. Comput.* **2013**, *62*, 1893–1898.
32. Shen, S.; Yue, G.; Cao, Q.; Yu, F. A survey of game theory in wireless sensor networks security. *J. Netw.* **2011**, *6*, 521–532.
33. Yu, Y.; Li, K.; Zhou, W.; Li, P. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *J. Netw. Comput. Appl.* **2012**, *35*, 867–880.
34. Sun, Y.L.; Han, Z.; Yu, W.; Liu, K.R. A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. *INFOCOM* **2006**, *6*, 1–13.
35. Sun, Y.; Han, Z.; Liu, K.R. Defense of trust management vulnerabilities in distributed networks. *Commun. Mag.* **2008**, *46*, 112–119.
36. He, D.; Chen, C.; Chan, S.; Bu, J.; Vasilakos, A.V. ReTrust: Attack-resistant and lightweight trust management for medical sensor networks. *IEEE Trans. Inf. Technol. Biomed.* **2012**, *16*, 623–632.
37. Komathy, K.; Narayanasamy, P. Trust-based evolutionary game model assisting AODV routing against selfishness. *J. Netw. Comput. Appl.* **2008**, *31*, 446–471.
38. Kamhoua, C.; Pissinou, N.; Miller, J.; Makki, S.K. Mitigating routing misbehavior in multi-hop networks using evolutionary game theory. In Proceedings of the Globecom Workshops (GC Wkshps), Miami, FL, USA, 6–10 December 2010; pp. 1957–1962.
39. Tembine, H.; Altman, E.; El-Azouzi, R. Delayed evolutionary game dynamics applied to medium access control. In Proceedings of the International Conference on Mobile Adhoc and Sensor Systems (MASS), Pisa, Italy, 8–11 December 2007; pp. 1–6.
40. Zhang, Y.; Guizani, M. *Game Theory for Wireless Communications and Networking*; CRC press: Boca Raton, FL, USA, 2011.

41. Yang, F.; Zhou, X.; Jia, G.; Zhang, Q. A non-cooperative game approach for intrusion detection in smartphone systems. In Proceedings of the Eighth Annual Communication Networks and Services Research Conference (CNSR), Montreal, QC, Canada, 11–14 May 2010; pp. 146–151.
42. Pal, R.; Gupta, B.; Cianca, E.; Patel, A.; Kaligotla, S.; Gogar, A.; Wardana, S.; Lam, V.T.; Ganguly, B. Playing 'games' with human health the role of game theory in optimizing reliability in wireless health networks. In Proceedings of the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), Rome, Italy, 7–10 November 2010; pp. 1–5.
43. Colell, A.M. Bargaining games. In *Cooperation: Game-Theoretic Approaches*; Springer: Berlin, Germany, 1997; pp. 69–90.
44. Zhang, G.; Gu, J.; Liu, P.; Ding, E. Cooperative communication strategy for wireless sensor networks based on cooperative game theory. *J. Wuhan Univ. Technol.* **2010**, *32*, 133–136.
45. Niyato, D.; Hossain, E.; Rashid, M.M.; Bhargava, V.K. Wireless sensor networks with energy harvesting technologies: A game-theoretic approach to optimal energy management. *IEEE Wirel. Commun.* **2007**, *14*, 90–96.
46. Vane, H.R.; Mulhearn, C. *The Nobel Memorial Laureates in Economics: An Introduction to Their Careers and Main Published Works*; Edward Elgar Publishing: Northampton, MA, USA, 2005.
47. Osborne, M.J.; Rubinstein, A. *A Course in Game Theory*; MIT Press: Cambridge, UK, 1994.
48. Liu, K.R.; Wang, B. *Cognitive Radio Networking and Security: A Game-Theoretic View*; Cambridge University Press: Cambridge, UK, 2010.
49. Čagalj, M.; Ganeriwal, S.; Aad, I.; Hubaux, J.P. On selfish behavior in CSMA/CA networks. In Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005), New York, NY, USA, 13–17 March 2005; Volume 4, pp. 2513–2524.
50. Saad, W.; Han, Z.; Debbah, M.; Hjørungnes, A.; Başar, T. Coalitional game theory for communication networks. *Signal Proc. Mag.* **2009**, *26*, 77–97.
51. Khayatian, H.; Saadat, R.; Mirjalily, G. Distributed power allocation based on coalitional and noncooperative games for wireless networks. In Proceedings of the 5th International Symposium on Telecommunications (IST), Tehran, Iran, 4–6 December 2010; pp. 367–372.
52. Vadori, V.; Scalabrin, M.; Guglielmi, A.V.; Badia, L. Jamming in Underwater Sensor Networks as a Bayesian Zero-Sum Game with Position Uncertainty. In Proceedings of the Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
53. Reddy, Y.B.; Srivathsan, S. Game theory model for selective forward attacks in wireless sensor networks. In Proceedings of the 17th Mediterranean Conference on Control and Automation (MED), Thessaloniki, Greece, 24–26 June 2009; pp. 458–463.
54. Estiri, M.; Khademzadeh, A. A game-theoretical model for intrusion detection in wireless sensor networks. In Proceedings of the 23rd Canadian Conference on Electrical and Computer Engineering (CCECE), Calgary, AB, Canada, 2–5 May 2010; pp. 1–5.
55. Karapistoli, E.; Economides, A.A. Defending jamming attacks in wireless sensor networks using stackelberg monitoring strategies. In Proceedings of the IEEE/CIC International Conference on Communications in China (ICCC), Shanghai, China, 13–15 October 2014; pp. 161–165.
56. Tang, X.; Ren, P.; Wang, Y.; Du, Q.; Sun, L. Securing wireless transmission against reactive jamming: A stackelberg game framework. In Proceedings of the Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
57. Abdalzaher, M.S.; Seddik, K.; Muta, O.; Abdelrahman, A. Using Stackelberg game to enhance node protection in WSNs. In Proceedings of the 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2016; pp. 853–856.
58. Altman, E.; Avrachenkov, K.; Garnaev, A. A jamming game in wireless networks with transmission cost. In *Network Control and Optimization*; Springer: Berlin, Germany, 2007; pp. 1–12.
59. Xiao, L.; Li, Q.; Chen, T.; Cheng, E.; Dai, H. Jamming games in underwater sensor networks with reinforcement learning. In Proceedings of the Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
60. Moussavinik, H.; Byun, S.S.; Balasingham, I. On the steady state in multiuser multiband IR-UWB without NBI detection. In Proceedings of the 6th International Symposium on Wireless Communication Systems (ISWCS), Siena, Italy, 7–10 September 2009; pp. 522–525.

61. Moussavinik, H.; Byun, S.S.; Balasingham, I. Towards robustness in multiband/multiuser IR-UWB: Overcoming unknown NBI via FEC and subband scheduling. In Proceedings of the 11th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Ireland, 15–18 February 2009; Volume 3, pp. 1947–1949.
62. Shapley, L.S. Stochastic games. *Proc. Natl. Acad. Sci. USA* **1953**, *39*, 1095–1100.
63. Susu, A.E.; Acquaviva, A.; Atienza, D.; De Micheli, G. Stochastic modeling and analysis for environmentally powered wireless sensor nodes. In Proceedings of the 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops (WiOPT), Berlin, Germany, 1–3 April 2008; pp. 125–134.
64. Fu, F.; Kozat, U.C. Stochastic game for wireless network virtualization. *IEEE/ACM Trans. Netw. (ToN)* **2013**, *21*, 84–97.
65. Nguyen, K.C.; Alpcan, T.; Başar, T. Stochastic games for security in networks with interdependent nodes. In Proceedings of the 9th International Conference on Game Theory for Networks (GameNets), Istanbul, Turkey, 13–15 May 2009; pp. 697–703.
66. Liu, Y.; Comaniciu, C.; Man, H. A Bayesian game approach for intrusion detection in wireless ad hoc networks. In Proceedings of the ACM Workshop on Game Theory for Communications and Networks, Pisa, Italy, 11–13 October 2006.
67. Lin, J.; Xiong, N.; Vasilakos, A.V.; Chen, G.; Guo, W. Evolutionary game-based data aggregation model for wireless sensor networks. *IET Commun.* **2011**, *5*, 1691–1697.
68. Crosby, G.V.; Pissinou, N. Evolution of cooperation in multi-class wireless sensor networks. In Proceedings of the Local Computer Networks (LCN), Dublin, Ireland, 15–18 Octpber 2007; pp. 489–495.
69. Ma, Z.S.; Krings, A.W. Bio-robustness and fault tolerance: A new perspective on reliable, survivable and evolvable network systems. In Proceedings of the Aerospace Conference, Big Sky, MT, USA, 1–8 March 2008; pp. 1–20.
70. Ma, Z.S.; Krings, A.W. Dynamic hybrid fault models and the applications to wireless sensor networks (WSNs). In Proceedings of the 11th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Vancouver, BC, Canada, 27–31 October 2008; pp. 100–108.
71. Qiu, Y.; Chen, Z.; Xu, L. Active defense model of wireless sensor networks based on evolutionary game theory. In Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), Chengdu, China, 23–25 September 2010; pp. 1–4.
72. Ma, Z.; Krings, A.W. Insect population inspired wireless sensor networks: A unified architecture with survival analysis, evolutionary game theory, and hybrid fault models. In Proceedings of the International Conference on BioMedical Engineering and Informatics (BMEI), Sanya, China, 27–30 May 2008; Volume 2, pp. 636–643.
73. Ricardo, V. Fault-Tolerant Wireless Sensor Networks Using Evolutionary Games. PhD Thesis, University of New Mexico, Albuquerque, NM, USA, 2012.
74. Ma, Z.S.; Krings, A.W. Dynamic hybrid fault modeling and extended evolutionary game theory for reliability, survivability and fault tolerance analyses. *IEEE Trans. Reliab.* **2011**, *60*, 180–196.
75. Ma, Z.S.; Krings, A.W.; Hiromoto, R.E. Dragonfly as a model for UAV/MAV flight and communication controls. In Proceedings of the Aerospace Conference, Big Sky, MT, USA, 7–14 March 2009; pp. 1–8.
76. Reddy, Y.B. A game theory approach to detect malicious nodes in wireless sensor networks. In Proceedings of the Third International Conference on Sensor Technologies and Applications (SENSORCOMM), Athens, Greece, 18–23 June 2009; pp. 462–468.
77. Agah, A.; Asadi, M.; Das, S.K. Prevention of DoS Attack in Sensor Networks using Repeated Game Theory. In Proceedings of the ICWN, Las Vegas, NV, USA, 26–29 June 2006; pp. 29–36.
78. Wang, Y.; Attebury, G.; Ramamurthy, B. A survey of security issues in wireless sensor networks. *Commun. Surv. Tutor.* **2006**, *8*, 1–23.
79. Rassam, M.A.; Maarof, M.A.; Zainal, A. A survey of intrusion detection schemes in wireless sensor networks. *Am. J. Appl. Sci.* **2012**, *9*, 1636.
80. Li, Y.; Shi, L.; Cheng, P.; Chen, J.; Quevedo, D.E. Jamming attack on Cyber-Physical Systems: A game-theoretic approach. In Proceedings of the 3rd Annual International Conference on Cyber Technology in Automation, Control and Intelligent Systems (CYBER), Nanjing, China, 26–29 May 2013; pp. 252–257.

81. Agah, A.; Das, S.K.; Basu, K.; Asadi, M. Intrusion detection in sensor networks: A non-cooperative game approach. In Proceedings of the Third International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 August–1 September 2004; pp. 343–346.
82. Agah, A.; Basu, K.; Das, S.K. Preventing DoS attack in sensor networks: A game theoretic approach. In Proceedings of the International Conference on Communications (ICC), Seoul, Korea, 16–20 May 2005; Volume 5, pp. 3218–3222.
83. Agah, A.; Das, S.K.; Basu, K. A game theory based approach for security in wireless sensor networks. In Proceedings of the International Conference on Performance, Computing, and Communications, Phoenix, AZ, USA, 15–17 April 2004; pp. 259–263.
84. Czarlinska, A.; Kundur, D. Reliable event-detection in wireless visual sensor networks through scalar collaboration and game-theoretic consideration. *IEEE Trans. Multimedia* **2008**, *10*, 675–690.
85. Ben Abid, I.; Boudriga, N. Game theory for misbehaving detection in wireless sensor networks. In Proceedings of the International Conference on Information Networking (ICOIN), Bangkok, Thailand, 28–30 January 2013; pp. 60–65.
86. Misra, S.; Krishna, V.P.; Abraham, K.I. Energy efficient learning solution for intrusion detection in wireless sensor networks. In Proceedings of the 2010 Second International Conference on Communication Systems and Networks, Bangalore, India, 5–9 January 2010; pp. 1–6.
87. Kodialam, M.; Lakshman, T. Detecting network intrusions via sampling: A game theoretic approach. In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, INFOCOM 2003, San Francisco, CA, USA, 30 March–3 April 2003; Volume 3, pp. 1880–1889.
88. Slater, D.; Tague, P.; Poovendran, R.; Li, M. A game-theoretic framework for jamming attacks and mitigation in commercial aircraft wireless networks. In Proceedings of the American Institute of Aeronautics and Astronautics, AIAA Infotech at Aerospace Conference, Washington, DC, USA, 6–9 April 2009; pp. 1880–1889.
89. Xiao, L.; Chen, Y.; Lin, W.S.; Liu, K. Indirect reciprocity security game for large-scale wireless networks. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1368–1380.
90. Chen, L.; Leneutre, J. Fight jamming with jamming–A game theoretic analysis of jamming attack in wireless networks and defense strategy. *Comput. Netw.* **2011**, *55*, 2259–2270.
91. Hao, D.; Adhikari, A.; Sakurai, K. Mixed-Strategy game based trust management for clustered wireless sensor networks. In *Trusted Systems*; Springer: Beijing, China, 2011; pp. 239–257.
92. An, B.; Tambe, M. Game theory for security: An important challenge for multiagent systems. In *Multi-Agent Systems*; Springer: Utrecht, The Netherlands, 2011; pp. 17–30.
93. Luo, Y.; Szidarovszky, F.; Al-Nashif, Y.; Hariri, S. A game theory based risk and impact analysis method for intrusion defense systems. In Proceedings of the International Conference on Computer Systems and Applications (AICCSA), Rabat, Morocco, 10–13 May 2009; pp. 975–982.
94. Zhu, Q.; Başar, T. Game-theoretic approach to feedback-driven multi-stage moving target defense. In *Decision and Game Theory for Security*; Springer: Fort Worth, TX, USA, 2013; pp. 246–263.
95. Wang, J.; Smith, G. A cross-layer authentication design for secure video transportation in wireless sensor network. *Int. J. Secur. Netw.* **2010**, *5*, 63–76.
96. Khirwadkar, T.S. Defense Against Network Attacks Using Game Theory. PhD Thesis, University of Illinois at Urbana-Champaign, Champaign, IL, USA, 2011.
97. Konorski, J. A game-theoretic study of CSMA/CA under a backoff attack. *IEEE/ACM Trans. Netw. (TON)* **2006**, *14*, 1167–1178.
98. Czarlinska, A.; Luh, W.; Kundur, D. Attacks on sensing in hostile wireless sensor-actuator environments. In Proceedings of the Global Telecommunications Conference (GLOBECOM), Washington, DC, USA, 26–30 November 2007; pp. 1001–1005.
99. Laszka, A.; Johnson, B.; Grossklags, J. Mitigation of targeted and non-targeted covert attacks as a timing game. In *Decision and Game Theory for Security*; Springer: Fort Worth, TX, USA, 2013; pp. 175–191.
100. Jha, S.; Tripakis, S.; Seshia, S.A.; Chatterjee, K. Game theoretic secure localization in wireless sensor networks. In Proceedings of the International Conference on the Internet of Things (IOT), Cambridge, MA, USA, 6–8 October 2014; pp. 85–90.
101. Vovk, V.G. A game of prediction with expert advice. In Proceedings of the ACM Eighth Annual Conference on Computational Learning Theory, New York, NY, USA, 5–8 July 1995; pp. 51–60.

102. Vovk, V.; Zhdanov, F. Prediction with expert advice for the Brier game. *J. Mach. Learn. Res.* **2009**, *10*, 2445–2471.
103. Perrig, A.; Stankovic, J.; Wagner, D. Security in wireless sensor networks. *Commun. ACM* **2004**, *47*, 53–57.
104. Agah, A.; Das, S.K. Preventing DoS attacks in wireless sensor networks: A repeated game theory approach. *IJ Netw. Secur.* **2007**, *5*, 145–153.
105. Kamhoua, C.A.; Pissinou, N.; Makki, K. Game theoretic modeling and evolution of trust in autonomous multi-hop networks: Application to network security and privacy. In Proceedings of the International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011; pp. 1–6.
106. Shila, D.M.; Anjali, T. A game theoretic approach to gray hole attacks in wireless mesh networks. In Proceedings of the Military Communications Conference (MILCOM), San Diego, CA, USA, 16–19 November 2008; pp. 1–7.
107. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Netw.* **2003**, *1*, 293–315.
108. Lin, W.S.; Zhao, H.V.; Liu, K. Cooperation stimulation strategies for peer-to-peer wireless live video-sharing social networks. *IEEE Trans. Image Proc.* **2010**, *19*, 1768–1784.
109. Chen, R.; Bao, F.; Chang, M.; Cho, J.H. Integrated social and QoS trust-based routing in delay tolerant networks. *Wirel. Pers. Commun.* **2012**, *66*, 443–459.
110. Alpcan, T.; Başar, T. A game theoretic analysis of intrusion detection in access control systems. In Proceedings of the 43rd Conference on Decision and Control (CDC), Atlantis, Paradise Island, Bahamas, 14–17 December 2004; Volume 2, pp. 1568–1573.
111. Fallah, M.S. A puzzle-based defense strategy against flooding attacks using game theory. *IEEE Trans. Dependable Secure Comput.* **2010**, *7*, 5–19.
112. Sallhammar, K.; Knapskog, S.J.; Helvik, B.E. Using Stochastic Game Theory to Compute the Expected Behavior of Attackers. PhD Thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2005.
113. Agah, A.; Basu, K.; Das, S.K. Enforcing security for prevention of DoS attack in wireless sensor networks using economical modeling. In Proceedings of the International Conference on Mobile Adhoc and Sensor Systems Conference, Washington, DC, USA, 7 November 2005; pp. 1–8.
114. Agah, A.; Das, S.K.; Basu, K. A non-cooperative game approach for intrusion detection in sensor networks. In Proceedings of the 60th Vehicular Technology Conference (VTC), Los Angeles, CA, USA, 26–29 September 2004; Volume 4, pp. 2902–2906.
115. Movahedi, Z.; Hosseini, Z.; Bayan, F.; Pujolle, G. Trust-distortion Resistant Trust Management Frameworks on Mobile Ad hoc Networks: A Survey. *Commun. Surv. Tutor.* **2015**, *18*, 1287–1309.
116. Mármol, F.G.; Pérez, G.M. TRMSim-WSN, trust and reputation models simulator for wireless sensor networks. In Proceedings of the International Conference on Communications (ICC), Dresden, Germany, 14–18 June 2009; pp. 1–5.
117. Misra, S.; Krishna, P.V.; Abraham, K.I. A simple learning automata-based solution for intrusion detection in wireless sensor networks. *Wirel. Commun. Mob. Comput.* **2011**, *11*, 426–441.
118. Shen, S.; Huang, L.; Fan, E.; Hu, K.; Liu, J.; Cao, Q. Trust dynamics in WSNs: An evolutionary game-theoretic approach. *J. Sens.* **2016**, *10.1155*, 1–11.
119. Doebeli, M.; Hauert, C.; Killingback, T. The evolutionary origin of cooperators and defectors. *Science* **2004**, *306*, 859–862.
120. Hofbauer, J.; Sigmund, K. Evolutionary game dynamics. *Bull. Am. Math. Soc.* **2003**, *40*, 479–519.
121. Foster, D.; Young, P. Stochastic evolutionary game dynamics. *Theor. Popul. Biol.* **1990**, *38*, 219–232.
122. Ahmad, A.; Ahmad, S.; Rehmani, M.H.; Hassan, N.U. A survey on radio resource allocation in cognitive radio sensor networks. *Commun. Surv. Tutor.* **2015**, *17*, 888–917.
123. Zhang, H.; Wang, T.; Song, L.; Han, Z. Interference Improves PHY Security for Cognitive Radio Networks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 609–620.
124. Fragkiadakis, A.G.; Tragos, E.Z.; Askoxylakis, I.G. A survey on security threats and detection techniques in cognitive radio networks. *Commun. Surv. Tutor.* **2013**, *15*, 428–445.
125. Al-Talabani, A.; Nallanathan, A.; Nguyen, H.X. Enhancing secrecy rate in cognitive radio via game theory. In Proceedings of the Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.

126. Han, L.; Gao, F.; Zhang, K.; Zhang, S. Sequential detection aided modulation classification in cognitive radio networks. In Proceedings of the Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
127. Li, Y.; Cao, B.; Daneshmand, M.; Zhang, W. Cooperative spectrum sharing with energy-save in cognitive radio networks. In Proceedings of the Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
128. Zhang, N.; Lu, N.; Cheng, N.; Mark, J.W.; Shen, X.S. Cooperative spectrum access towards secure information transfer for CRNs. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 2453–2464.
129. Gavrilovska, L.; Krco, S.; Milutinovic, V.; Stojmenovic, I.; Trobec, R. *Application and Multidisciplinary Aspects of Wireless Sensor Networks: Concepts, Integration, and Case Studies*; Springer Science & Business Media: London, UK, 2010.
130. Vadlamani, S.; Eksioglu, B.; Medal, H.; Nandi, A. Jamming attacks on wireless networks: A taxonomic survey. *Int. J. Prod. Econom.* **2016**, *172*, 76–94.
131. Kamath, G.; Shi, L.; Song, W.Z.; Lees, J. Distributed travel-time seismic tomography in large-scale sensor networks. *J. Parallel Distrib. Comput.* **2016**, *89*, 50–64.
132. Premarathne, U.S.; Khalil, I.; Atiquzzaman, M. Trust based reliable transmission strategies for smart home energy management in cognitive radio based smart grid. *Ad Hoc Netw.* **2016**, *41*, 15–29.
133. Seah, W.K.; Eu, Z.A.; Tan, H.P. Wireless sensor networks powered by ambient energy harvesting (WSN-HEAP)-Survey and challenges. In Proceedings of the 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology Wireless (VITAE), Aalborg, Denmark, 17–20 May 2009; pp. 1–5.
134. Hawa, M.; Darabkh, K.A.; Al-Zubi, R.; Al-Sukkar, G. A self-learning MAC protocol for energy harvesting and spectrum access in cognitive radio sensor networks. *J. Sens.* **2016**, *2016*, doi:10.1155/2016/9604526.
135. Maghsudi, S.; Hossain, E. Distributed User Association in Energy Harvesting Small Cell Networks: A Probabilistic Model, Cornell University, 2016. arXiv preprint arXiv:1601.07795. Available online: http://arxiv.org/abs/1601.07795 (accessed on 27 January 2016)
136. Meharouech, A.; Elias, J.; Mehaoua, A. A two-stage game theoretical approach for interference mitigation in body-to-body networks. *Comput. Netw.* **2016**, *95*, 15–34.
137. Yi, C.; Zhao, Z.; Cai, J.; de Faria, R.L.; Zhang, G.M. Priority-aware pricing-based capacity sharing scheme for beyond-wireless body area networks. *Comput. Netw.* **2016**, *98*, 29–43.
138. Zhang, L.; Zhang, H. A Survey on Security and Privacy in Emerging Sensor Networks: From Viewpoint of Close-Loop. *Sensors* **2016**, *16*, 443.
139. Shan, X.; Zhuang, J. Cost of equity in homeland security resource allocation in the face of a strategic attacker. *Risk Anal.* **2013**, *33*, 1083–1099.