IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 September 2023, accepted 27 September 2023, date of publication 2 October 2023, date of current version 5 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3321082

SURVEY

An Overview of Game Theory Approaches for Mobile Ad-Hoc Network's Security

HADJER MESSABIH[1], CHAKER ABDELAZIZ KERRACHE[1], YOUSSRA CHERIGUENE[1], CARLOS T. CALAFATE[2], (Senior Member, IEEE), AND FATIMA ZOHRA BOUSBAA[1]

[1]Laboratoire d'Informatique et de Mathématiques, UniversitéAmar Telidji de Laghouat, Laghouat 03000, Algeria
[2]Computer Engineering Department (DISCA), Universitat Politècnica de València, 46022 Valencia, Spain

Corresponding authors: Hadjer Messabih (h.messabih@lagh-univ.dz) and Carlos T. Calafate (calafate@disca.upv.es)

This work was supported in part by the Research and Development from MCIN/AEI/10.13039/501100011033 under Project PID2021-122580NB-100, and in part by European Regional Development Fund (ERDF) A way of Making Europe.

ABSTRACT The issue of cybersecurity has gained significant prominence in the context of safeguarding the privacy and integrity of information, especially with the increasing prevalence of interconnected devices such as Mobile Ad-hoc networks (MANETs). Due to their nature, particularly in light of the unavoidable security flaws that arise from the complexity of current and future systems and services, it is crucial to explore how to prevent cyberattacks efficiently. On the other hand, game theory is one of the most significant methods used in this field. Yet, survey articles that consider game theory for security in MANETs are less common. Therefore, in this paper, we survey the articles related to game theory for security in MANETs, presenting an overview of the basic MANETs concepts and their main vulnerabilities. Also, we will propose a taxonomy for recent works, highlighting the limits of the existing works, and outlining some potential future directions for cybersecurity in Ad-hoc networks.

INDEX TERMS Cybersecurity, game theory, intrusion, malicious, mobile ad-hoc networks (MANETs).

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) have emerged as a crucial component of connectivity, transcending the constraints imposed by traditional infrastructure-based networks [1], [2]. MANETs possess exceptional adaptability as they facilitate the formation of networks among devices without relying on centralized infrastructure. This unique characteristic renders them highly suitable for various scenarios, including but not limited to disaster response, Internet of Things (IoT) deployments [3], vehicular networks [4], [5], and smart cities [6], [7]. However, the rapid expansion of MANETs, and their wide range of potential uses, also brings up several cybersecurity issues that require thorough investigation [6], [8], [9]. Furthermore, due to the dynamic and unstable nature of the topology of MANETs, as well as their limited resources, these networks more often encounter challenges related to delays and packet loss compared to stationary networks [10].

Additionally, among the reasons for continuous intermissions of communications are security breaches which decrease the efficiency of any network [6], [8], [11]. Such a setback can be caused by the lack of centralized management and monitoring, open access medium, the lack of physical organization members of MANETs, and dynamically changing topologies, which raises the security challenge of MANETs [6], [11].

This raises significant issues regarding the integrity and confidentiality of the transmitted data. As a result, MANETs become prone to malicious attacks, intrusions, and security breaches [6], [12].

The security of MANETs is a significant obstacle that impedes the seamless functioning of the network [13]. With the expectation of a significant increase in the utilization of MANETs in diverse fields in the near future, it is crucial to emphasize the importance of enhancing their security measures and guaranteeing the robustness of these networks

The associate editor coordinating the review of this manuscript and approving it for publication was Chuan Heng Foh.

against emerging cyber risks. There are some open issues and fundamental limitations of MANET security aspects that have been discussed in the literature. For instance, the authors in [14] discuss critical security requirements for networks.

Among the complex security issues in MANETs, profiling the behaviour of nodes [15], and differentiating between ''good'' and ''bad'' nodes, stands out due to the heterogeneity of devices integrating a MANET (e.g. laptops, tablet PCs, smartphones). There are four distinct types of MANET nodes based on their behavioural characteristics [6], [15], [16]:

- The first type is an honest node which is interested in establishing communication with other nodes with the aim of forwarding data packets.
- The second type is the unintentional misbehaving nodes, i.e. an erroneous node that has circuitry issues and defective hardware design.
- The third type is the selfish node which tends to refuse to forward the data packet to the destination nodes in order to save its resources.
- The last type includes malicious intentional misbehaving nodes which have harmful intentions to disrupt traffic and steal confidential data.

There are various consequences that result in the eventual behaviour of malicious nodes, such as network crashes [17]. Nonetheless, identifying malicious nodes in MANETs poses a significant challenge due to the difficulty in detecting malicious attacks. This is primarily attributed to the lack of adequate security systems in MANET policies [17]. The identification of illicit behaviour is hindered by secondary challenges, such as the absence of a systematic network surveillance process. This is often due to the lack of a centralized system, particularly in large-scale environments [17].

A group of works in the literature [6], [18], [19], [20] categorizes attacks into two distinct classes: the first class includes external attacks such as DoS (Denial-of-Service), congested links, as well as false routing information attacks, while the second class refers to internal attacks; an example are malicious nodes mimicking regular nodes to access confidential information. Furthermore, cybersecurity attacks in MANETs can be classified into passive and active attacks. In the former, there is no disruption in the protocol operation, yet there is an attempt to learn important information by eavesdropping on network traffic; in the latter class, active attacks, the attacker attempts to disrupt protocol operations by injecting arbitrary packets with the aim to acquire authentication, restrict availability, or draw packets that are meant to be delivered to other nodes [21]. Another group of works categorized the attacks in MANETs based on various criteria like source/domain, nature/behaviour of the attack, the number of attackers involved, their processing capacity, and the attacks corresponding to different MANET layers [14]. Additionally, in the literature, alternative categorizations of MANET attacks have been suggested by Kavitha and Mukesh [22], consisting of two distinct classes: the first class pertains to a data traffic attack that involves the intentional obstruction of data packets passing through nodes, resulting in either the dropping of claimed packets or the delay of their forwarding. The first category of attacks includes the black-hole attack, cooperative black-hole attack, gray-hole attack, and jellyfish attack. The second category pertains to control traffic attacks, which comprises the worm-hole attack, HELLO flood attack, bogus registration attack, man-in-the-middle attack, rushing attack, cache poisoning attack, cooperative blackmail attack, and Sybil attack. A summary of the aforementioned classifications is highlighted in Fig.1. Furthermore, a description of various attacks based on the distinct MANET layers is given in Table.1.

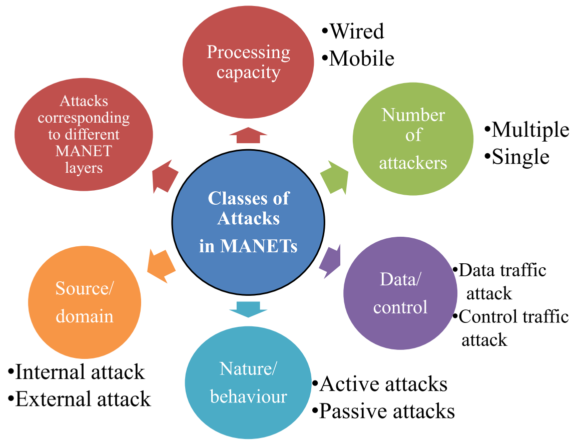

FIGURE 1. Classification of attacks in MANETs.

TABLE 1. Attacks on various MANET layers [14].

Layer	Attack
Physical	Jamming, interceptions, eavesdropping, active interference, malicious message injecting
Data Link	Traffic analysis, monitoring, SYN flooding, TCP ACK storm
Network	Spoofing, wormhole, grey hole, Byzantine, black-hole, resource consumption, flooding, location disclosure attacks, Sybil, routing attacks, sinkhole
Application	Repudiation, malicious code, data corruption
Transport	Session hijacking, TCP ACK storm, SYN flooding, jellyfish
MultiLayer	DoS, replay, man-in-the-middle, impersonation

There are several problems that arise as a consequence of attacks on different layers, as summarized in [14], [23], and [24] including time delay, data loss, full/partial network paralysis, compromised QoS (Quality-of-Service), as well as misuse of services.

As a result, various security methodologies have been developed for MANETs in prior academic studies. As such, authors in [17] grouped them into five groups as follows: 1) Cryptographic approaches that are conducted in either a symmetric or an asymmetric manner, thereby preserving the confidentiality and integrity of the original data by adopting various algorithms, e.g. SHA (Secure Hash Algorithm), MD5 (Message Digest 5), MAC (Message Authentication Codes), and digital signature., 2) trusted third party, 3) intrusion detection systems whose goal is to watch over malicious activities and identify potential threats (e.g. credit-based methods and reputation-based methods), 4) secure protocols, and 5) other security techniques (e.g. security using genetic algorithms, security using artificial neural networks, security using support vector machines, security using swarm intelligence, and security using game theory). Alternative classifications have been proposed in the literature [14], which categorize security approaches in MANETs into two distinct classes. As we have shown in Fig.2: preventive mechanisms are employed as the first line of defense for authenticating the data source and verifying the integrity of data, while reactive mechanisms such as intrusion detection methods act as the second defense line. Their principal aim is pinning down any abnormal actions during the exploit before real damage is carried out to the resources.

Game theory can be defined as a mathematical model that analyses interactive decisions in a particular situation that can be called a game [6]. There are different classes of game theory based on significant features and properties like symmetric, static, comprises perfect information, or imperfect [25].

Fig.3 explains the main features of non-cooperative and cooperative games. There are various interactions between attackers and defenders in network security. Game theory plays an important role to model these interactions and predict its outcome, as shown in Fig.4.

A. PREVIOUS SURVEYS AND CONTRIBUTIONS

Numerous surveys have been conducted in the realm of security within MANETs (see [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37]); additionally, there are different surveys concerning game theory in the field of network security as [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], and [48]. However, there is currently a lack of research that specifically focuses on the applications of game theory in the field of MANET security.

To the best of our knowledge, there exists one survey that studies game theory in the field of MANET security [49]; nonetheless, this work mostly mentions routing attacks and lacks technical detail. Therefore, our focus is directed toward the examination of papers that arise from a merger of the three primary domains.

Our study involves a systematic search for research papers that specifically address the application of game theory in the context of MANET Security, within the time frame from 2016 to 2023. A total of 300 articles were identified and reviewed pertaining to security in MANETs. However, in the specific domain of game theory for MANET security, a smaller subset of 44 articles were found and analyzed. In this survey, our study presents a comprehensive analysis of 44 significant articles that specifically address the application of game theory in enhancing the security of MANETs, where a summary of the findings is presented in this survey.

This article presents a comprehensive analysis of the current research on the application of game theory techniques for enhancing the security of MANETs. Furthermore, it also examines certain constraints of the existent literature and delineates some prospective possibilities that could be explored in the near future. Fig.5 demonstrates the types of papers with their distribution according to years.

In addition, this article offers a thorough overview of the fundamental principles of game theory to ensure that individuals with varying levels of expertise can comprehend the content presented. The paper's remainder is structured as follows: Section II is dedicated to studying pertinent literature in the field of security in MANETs that relied on game theory. A summary of existing review works is presented in Section III. A detailed discussion of the limitations of existing review works has been put in Section IV. Section V presents open issues and future research directions. Finally, the main conclusions of the paper are presented in Section VI.

II. RELATED WORKS

Game theory has been applied in various fields, and gained significant success in many areas including cybersecurity. Upon conducting an analysis of the literature pertaining to game theory for securing MANETs, we have developed a classification scheme based on the types of game theory employed, and the specific problems addressed. This classification is presented in Fig.6. Furthermore, related works can be grouped into five categories: malicious nodes mitigation, selfish nodes mitigation, hybrid selfish and malicious nodes mitigation, intrusion detection, and attacks detection.

Meanwhile, every category comprises numerous subclasses. The following sections will provide a detailed explanation of each of these classes.

A. MALICIOUS NODES MITIGATION

This class entails the presentation of various articles pertaining to the identification of malicious nodes in diverse scenarios. MANETs comprise four distinct node types, namely the malicious node, selfish node, erroneous node, and regular node, as documented in [6] and [15]. However, the authors categorized them using varying methods. In order to clarify the concept, we have introduced a class that encompasses four subcategories based on the node behaviour suggested by the authors.

1) MALICIOUS BEHAVIOUR DETECTION

The detection of malicious nodes is a targeted effort to identify nodes that are deliberately engaging in malicious activities or exhibiting malicious behaviour. The identification of malicious nodes is of utmost importance in upholding the security and coherence of the network, and in safeguarding it against diverse cyber threats. Several articles have been dedicated to the detection of malicious nodes in MANETs. One such work, as described in [50], focuses on the development of a secure routing protocol using the game theory model in MANETs. They divide the nodes into regular and malicious, which are used in their approach based on a dynamic Bayesian signaling game. In particular, authors rely on the Perfect Bayesian Equilibrium (PBE)

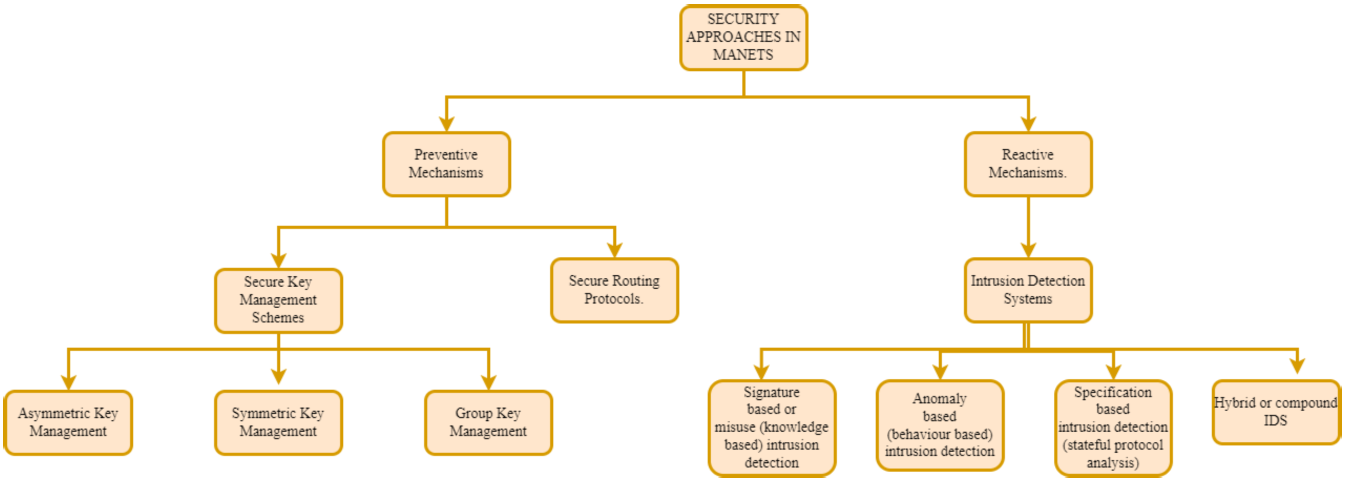
SECURITY APPROACHES IN MANETS
Preventive Mechanisms
Reactive Mechanisms.
Secure Key Management Schemes
Secure Routing Protocols.
Intrusion Detection Systems
Asymmetric Key Management
Symmetric Key Management
Group Key Management
Signature based or misuse (knowledge based) intrusion detection
Anomaly based (behaviour based) intrusion detection
Specification based intrusion detection (stateful protocol analysis)
Hybrid or compound IDS

FIGURE 2. **Security approaches in MANETs.**

to solve incomplete information by combining strategies and payoff of players that constitute an equilibrium. This approach minimizes the utility of malicious nodes, and it motivates better cooperation between nodes by using the reputation system. This game also revealed the best actions of individual strategies for each node and determined the malicious behaviour of a node. The results indicated that the suggested approach produced a relatively low routing overhead. Additionally, it achieved a favorable routing latency in the presence of different fractions of misbehaving nodes. However, the act of maximising throughput results in an increase in bandwidth use.

In [51], an approach is presented for malicious node detection using game theory. Their goal is recognizing, punishing, or expelling malicious nodes. The sending and receiving results and neighbours' responses to inquiries are saved in the nodes' recording table, and used in the next decision-making. These interactions are continued to be stored at appropriate times to be used to identify malicious nodes. They used a dynamic game model, especially a non-cooperative Bayesian game model with incomplete information. The findings indicate that, when the density of malicious nodes approaches 20%, and the game is played more than four times between neighbouring nodes, the suggested technique was able to enhance the detection rate of harmful nodes.

A security-aware routing scheme using a repeated game model (SAR-RG) in MANETs for enhancing secure routing is proposed in [52]. The objective of this approach is to identify malicious nodes in order to prevent packet loss and DoS attacks within the network. A repeated game model was employed. The first step of this algorithm involves formulating the connectivity of the network. Subsequently, the system verifies the identity of the user who has recently transmitted the game and penalizes the player who deviated from the norm. An effective routing model enables the attainment of energy efficiency. The results show that the suggested approach exhibits a reduced time requirement for identifying the malicious node, and demonstrates better performance in about 90% of the detector nodes. The accuracy of the system increases when 60% of the nodes are malicious, whereas the defense rate numbers decline as the number of malicious nodes increases.

The authors in [53] proposed a multi-attacker collusion approach to represent the unpredictable behaviour of nodes in cooperating, reporting, declining, or attacking other nodes to achieve effective modeling of mobile nodes in MANETs. The results showed that the proposed approach attained Perfect Bayesian Equilibrium successfully from both a security and a QoS viewpoint. The key limitation of works in [51] and [53], is the lack of diverse parameters.

2) MALICIOUS NODES MITIGATION WITH RESOURCE PRESERVATION

The resource limitations of MANETs are a common occurrence, largely attributable to their distinctive attributes. In order to reduce the negative effects of malicious nodes on a network, while concurrently guaranteeing optimal utilisation of network resources, several articles have been identified that concentrate on this particular research direction. For instance, the authors in [54] proposed a game theoretic framework to predict malicious behaviours within a MANET to analyze the best security alternatives that preserve the resource consumption of network entities. Furthermore, they relied on an evolutionary game theoretic approach for securing energy-constrained MANETs. In these games, each entity can learn about the behaviour of its opponent over time, allowing the adjustment of its strategy. They consider MANETs composed of malicious and regular nodes, with a distributed IDS composed of Host IDSs installed on each regular node. The main results of their game model are the elaboration of the Evolutionary Stable Strategies (ESSs), which is a stronger concept of equilibria, and the illustration

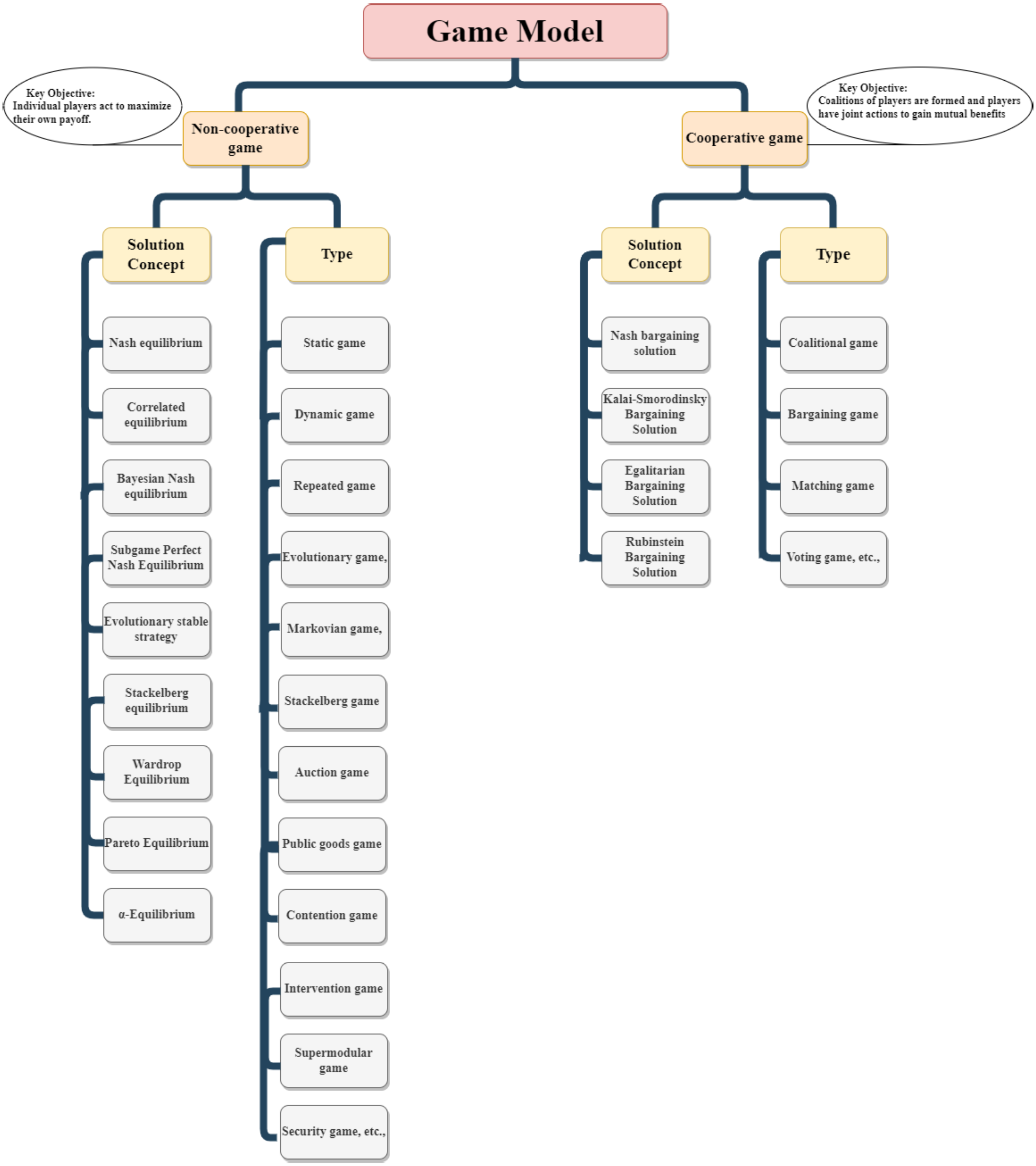

FIGURE 3. Main features of Non-cooperative and cooperative games.

of the evolution process, based on the replicator dynamic. The results of the replicators dynamic implementation showed the impact of the game settings on the convergence of the population strategies towards stable states and energy preservation.

An improved mean field game theoretic (IMFGT) approach for security was proposed in [55]. It is applicable for multiple defenders and multiple attackers. Furthermore, aside from its applicability in a centralised setting, their approach can also be employed in a dynamic environment.

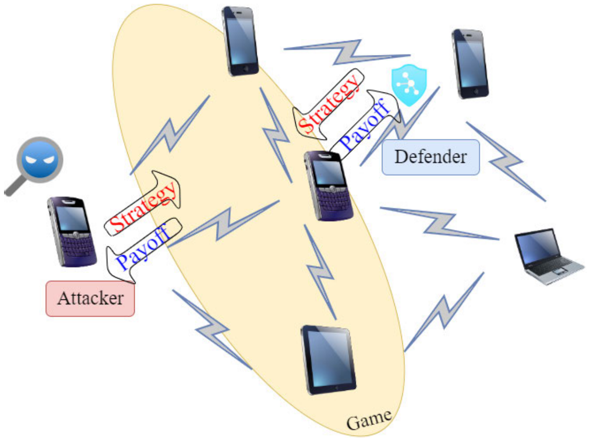

FIGURE 4. Game theory for network security.

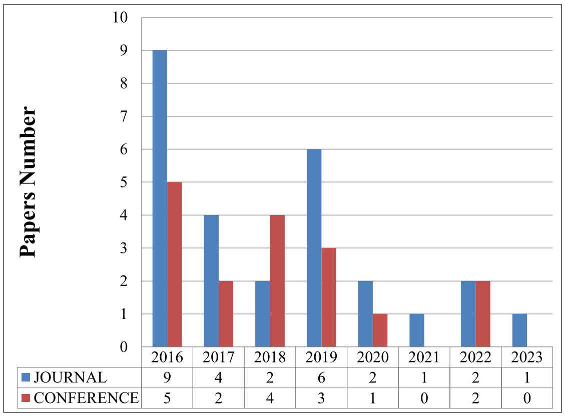

FIGURE 5. Papers distribution according to years.

System resources are taken into consideration. The authors also considered energy consumption in their approach. The results obtained from the IMFGT demonstrated superior performance compared to the current MFGT technique. Nevertheless, the authors fail to provide a thorough presentation of the analyses supporting this strategy. Among the drawbacks of works in [54] and [55] is the lack of simulation results.

B. SELFISH NODES MITIGATION

Selfish nodes in MANETs are characterised by their tendency to prioritise their own interests over the optimal functioning of the network. The nodes show selfish behaviour by intentionally prioritizing their own resources over network efficacy. The existence of self-interested nodes presents significant challenges to MANETs, which have an impact on network efficiency, and overall communication efficacy. Many approaches and algorithms have been suggested for identifying and alleviating the influence of self-interested nodes, with the objective of preserving the collaborative character and effectiveness of the network. Therefore, we present a selection of articles pertaining to the identification of selfish nodes in diverse scenarios. The classification comprises two distinct sub-classes, which are presented in the next subsections.

1) SELFISH NODES AVOIDANCE

Various strategies have been suggested to mitigate the selfish behaviours of nodes and promote network cooperation and efficacy, including measures aimed at avoiding their participation. The authors in [56] proposed a selfish node detection and prevention scheme, called SENDER. Their scheme contains two phases: a detection phase and a prevention phase. In the detection phase, they count the number of receiving and forwarding packets for each node and use an adaptive threshold algorithm to detect whether those nodes demonstrate selfish behaviour or not. In the prevention phase, a repeated game approach was utilised to prevent selfish behaviour by forcing the nodes to forward data packets in a MANET. The results showed that the proposed approach achieved increased throughput and a minimal delay.

A different approach involves the implementation of incentives, whereby nodes are motivated to engage in collaborative efforts through the provision of rewards or benefits for their involvement in network-related endeavours. This incentivizes nodes to exhibit cooperative behaviour. For instance, the authors in [57] proposed a credit-based system that used the advantages of the non-cooperative game and cooperative game theory to avoid selfishness among nodes. They analyzed the underlying behaviour of nodes in a MANET through game theory. The credit-based system is the main approach to avoid selfishness among nodes because the incentive is paid to encourage the node to provide services. An incentive scheme is designed to make the Pareto equilibrium overlap with the Nash equilibrium. The results showed effectiveness in cooperation among nodes avoiding selfish behaviour.

A slave-mode selfish and dynamic punishment scheme is proposed in [58] to avoid selfish behaviours MANETs, motivating selfish nodes to cooperate through a cooperative repeated game. The simulation result of their approach showed an improved MANET performance and a decrease in the number of selfish nodes. The detection rate of selfish nodes is seen to rise as the coalition sizes grow, resulting in enhanced network performance and decreased system latency.

One significant constraint of the approaches discussed in [56], [57], and [58] is the restricted scope of parameters.

On the other hand, the authors in [59] proposed a mechanism to control power consumption and the selfish nature of nodes which is based on cooperative game theory. Their aim is to minimize power loss during data transmission by choosing the best path and defining a stable incentive allocation mechanism through the coalition game among relay nodes to reduce selfishness. The results indicate that the use of methods that control selfish behaviour has a significant impact in optimising the utilisation of power resources in individual mobile nodes. The observed scenario

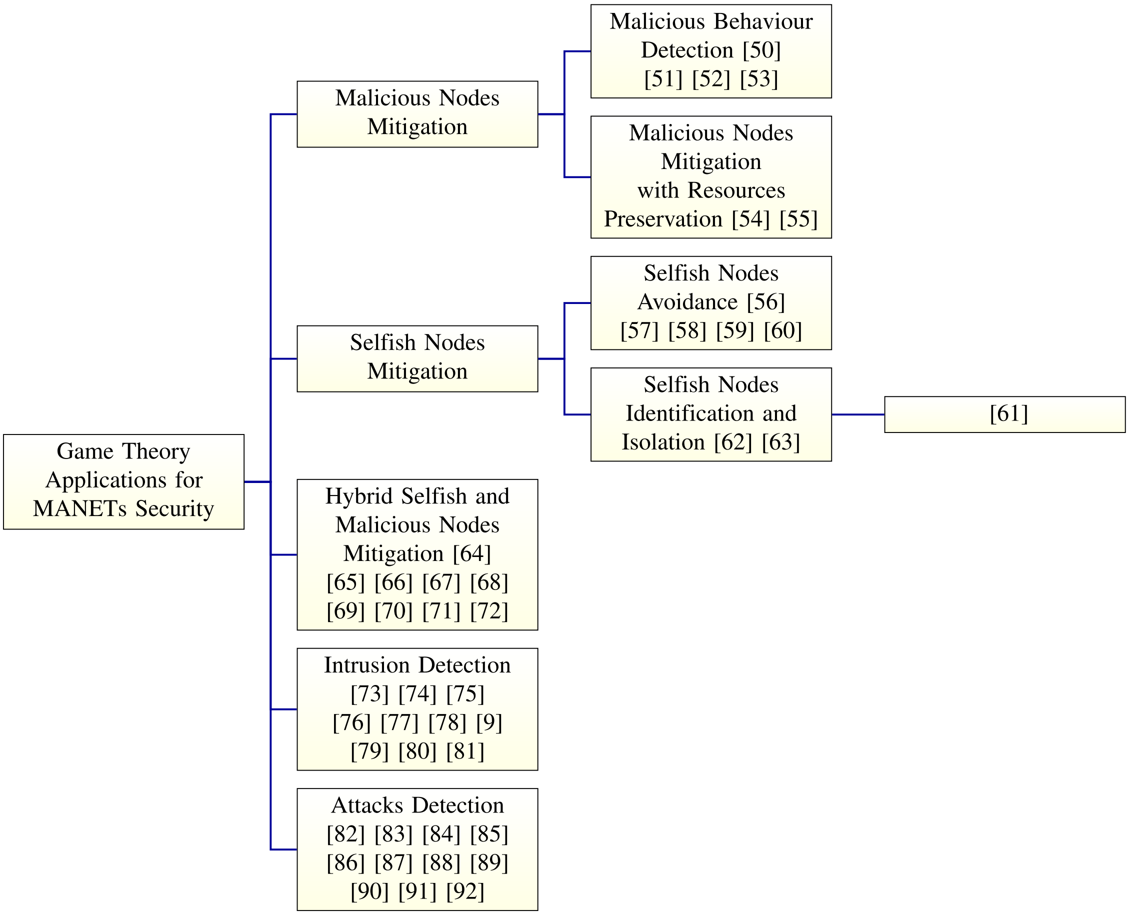
Game Theory Applications for MANETs Security
Malicious Nodes Mitigation
Malicious Behaviour Detection [50] [51] [52] [53]
Malicious Nodes Mitigation with Resources Preservation [54] [55]
Selfish Nodes Mitigation
Selfish Nodes Avoidance [56] [57] [58] [59] [60]
Selfish Nodes Identification and Isolation [62] [63]
[61]
Hybrid Selfish and Malicious Nodes Mitigation [64] [65] [66] [67] [68] [69] [70] [71] [72]
Intrusion Detection [73] [74] [75] [76] [77] [78] [9] [79] [80] [81]
Attacks Detection [82] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92]

FIGURE 6. Classification of security in MANETs using game theory.

demonstrated a trade-off between power consumption and network efficacy, specifically in relation to throughput.

Furthermore, a Hedonic Coalition Formation Game model, as developed in [60], has been suggested as an additional coalition game to address the issue of selfishness. The integration of it was included in the OLSR (Optimised Link State Routing) protocol. The findings indicate that the suggested model exhibits superior performance compared to the traditional OLSR protocol. Specifically, the proposed model achieves a reduction of around 22% in MPR (multi-point relay) nodes, hence extending the network's lifespan. Additionally, the packet delivery ratio is enhanced by 4% when compared to the classical OLSR protocol.

2) SELFISH NODES IDENTIFICATION AND ISOLATION

While selfish node avoidance is a strategic approach that seeks to preclude the involvement of selfish nodes in the network, the strategy of identifying selfish nodes within a network is aimed at detecting those nodes that have joined it with selfish intentions. Upon detection, a self-interested node may be subject to punitive measures or even exclusion from the network. As such, the main goal of the authors in [61] is to identify and isolate selfish nodes that refuse to forward the packets to conserve energy. Their work focused on integrating an Audit-based Misbehaviour Detection (AMD) scheme and an incentive-based reputation scheme with a game theoretical approach called Supervisory Game to analyze the selfish behaviour of nodes in MANET environments. In addition to selfish node detection and isolation in the networks, their approach also identified benevolent nodes and malevolent ones. The results indicate that, in the suggested approach, and when confronted with a large set of malicious nodes, the network keeps a reduced latency, control overhead, and packet loss, while achieving an increased packet delivery ratio. In general, it has resulted in a substantial reduction in the costs associated with identifying nodes that engage in malicious behaviour inside the network. However, one significant drawback of these findings is the inefficient use of bandwidth, and the subsequent increase in network congestion.

The authors in [62] used perfect information game theory to identify selfish nodes and isolate them from the network. Perfect information game theory is a non-cooperative game theory that focuses on agents who make their own individual decisions without a coalition. They found the performance of the network with and without using the game theory approach for static and dynamic Ad-hoc networks. In both types of networks, the results showed that the proposed approach increased the throughput in the presence of selfish nodes, and also decreased the end-to-end delay, which improved the performance of the ad-hoc network. The main limitation of this solution is its unscalability where the achieved results are only for a reduced density and communication load. In addition, the proposed solution also increases the bandwidth consumption.

Furthermore, another approach proposed in [63] introduces a non-cooperative game-based approach for detecting and isolating selfish nodes from the network. The underlying idea of their technique involves first identifying nodes that are suspected of being selfish, followed by a verification process to determine their selfishness and subsequent isolation. The process of verification involves the transmission of a test packet to nodes that are under suspicion. The evaluation is based on their reaction (or lack thereof). In the event of non-response, individuals will be designated and subjected to isolation from the network. However, one major drawback is the lack of numerical results.

C. HYBRID -SELFISH AND MALICIOUS- NODES MITIGATION

The simultaneous mitigation of selfish nodes and malicious nodes in MANETs necessitates the implementation of a range of strategies to address the difficulties presented by both types of nodes. This methodology acknowledges the possibility of the presence of nodes within the network that may exhibit diverse levels of self-interest, ranging from entirely self-centered to overtly malicious behaviour. For instance, the authors in [64] developed an algorithm based on the static and repeated game approach to enforce cooperation between nodes by calculating a Cooperation Rate (CR) for each node in order to avoid selfish and malicious nodes during the routing process. Their research is focused on MANETs using Optimized Link State Routing Protocol (OLSR) which is a proactive protocol. Especially, their strategy has been evaluated using OLSR messages (HELLO and TC), and different network processing (forwarding and routing). The CR represents the value that indicates how many times a node cooperates or not during the game (or during the network lifetime). Through this value, each node can evaluate the behaviour of another node before sending a packet. The results showed that the use of the proposed approach can improve parameters such as throughput, end-to-end delay, total packets forwarded, and packets received.

A new game theoretic method was proposed in [66] based on the AODV routing protocol to detect the selfish nodes and avoid the malicious nodes of the MANET. Their scheme guarantees secure routing and constructs an alternate backup route for guaranteed packet transmission. It is based on the Packet Forward Rate (PFR) during path establishment to detect selfish nodes and uses the CSN-NRN mechanism during data packet transmission. They used Route Density Factor (RDF) to select paths for data transmission. However, the analysis and arguments of this solution are not presented by the authors.

Furthermore, a cooperative game presented in [72] focuses on the bargaining game, which aims to address the issue of selfish nodes via the optimization of resource allocation and data packet forwarding. The presence of collaborating malicious nodes inside the network is also disclosed, and a potential solution for their coexistence is proposed.

A Bayesian game with imperfect information was proposed in [65] to detect malicious and selfish nodes. The only thing that distinguishes their approach is the intention of exploiting malicious and selfish nodes for the benefit of the network. In most cases, a malicious node is isolated upon detection. However, there may be situations in which the malicious nodes can coexist in the network. They rely on the fact that a malicious node does not know if it has been identified. Hence, the node will continue to provide useful network functions under the assumption that it is avoiding detection. Thus they can exploit the node to improve network throughput as long as the benefits to the network outweigh the damage. A malicious node is isolated and banned from the network when the damage it inflicts on the network outweighs the involuntary benefit it provides. In the case of a selfish node, it is banned when the likelihood that it will participate in network activity drops below a particular threshold. The results showed that the proposed approach improves network performance while conserving power resources. In particular, the coexistence with malicious nodes that seldom attack ameliorates throughput, and using benevolent nodes to determine the types of nodes in the network within a reasonable timeframe leads to conserving power.

Nodes that exhibit improper behaviour have the potential to adversely affect the efficiency, fairness, and reliability of the network. There are a handful of works that focus on misbehaviour detection; for instance, the work in [68] focused on integrating a misbehaviour node detection scheme and an incentive-based reputation scheme with a game theoretical approach called Supervisory Game to analyze the selfish behaviour of nodes in the MANETs environment. The main advantage of integrating these approaches is to significantly reduce the misbehaviour node detection cost in the network. Selfish nodes gain their payoff when they relay packets for other nodes, and reluctant nodes are punished and gradually isolated from the network. Nodes have to cooperate with others and relay packets for other nodes to maximize their bonus values. The simulation results show that the proposed mechanism ensures mutual cooperation among selfish nodes, achieving an increase in network throughput and packet delivery rate which improve the overall performance of the network. In addition, it reduces the cost of detecting misbehaving nodes in the network.

The authors in [69] used game theory for detecting misbehaviour. Their proposed game model exploits the concept of Bayes' theorem, belief system, and neighbour monitoring to profile the nodes according to the behaviour they exhibit in the network. Their work concentrated on modelling the behaviour of nodes in MANETs, including regular, malicious, as well as selfish nodes. They defined selfish nodes as regular nodes that encounter power, bandwidth, or other resource limitations that caused them to act selfishly. The results showed that the proposed Perfect Bayesian Equilibrium outperformed both pure and mixed strategies in terms of regular node utility and malicious node utility when applying both collaborative and non-collaborative games. The key limitation of the mentioned solutions in [65], [68], and [69] is the use of minimum parameters.

In [67] authors proposed a Bayesian Signaling (BS) game model that explores malicious behaviours and actions in MANETs. Moreover, the proposed scheme employs the reputation system stimulating enhanced collaboration between nodes while restricting the utility of malicious nodes. In their study, the exceptional actions exhibited by selfish nodes are revealed, and the mitigation of malicious nodes' behaviour is achieved by the adoption of the BS game model. The findings demonstrated that the suggested approach yielded a higher rate of identifying malicious nodes and detecting attacks, while concurrently enhancing throughput and reducing the occurrence of false positives.

Another group of works focuses on the non-cooperative games approach, for instance, a reputation-based scheme with a non-cooperative game is proposed in [71] to detect selfish nodes and prevent identity attacks. The results showed that the proposed approach reduced the throughput consumed by malicious nodes while increasing throughout for good nodes in the network. Furthermore, a Bayesian game approach is proposed in [70] to enhance MANET security. They took into consideration regular, selfish, and malicious nodes which form the static and dynamic game. The principle of their system depends on a periodic evaluation of the nodes to their neighbors by using a belief updating process. By updating their payoffs, they can identify malicious nodes and reduce their payoff. Simulation results showed increasing throughput and packet delivery ratio, along with a decreasing routing overhead and propagation delay.

D. INTRUSION DETECTION

The present categorization is centered on techniques and frameworks that identify and counteract unapproved access activities, and security violations within the MANET. In order to detect and respond to potentially malicious activities, it is common to deploy Intrusion Detection Systems (IDS). Several articles based on intrusion detection in various scenarios were found in the literature. For instance, the authors in [73] proposed a distributed IDS to provide network security while preserving the resources of the network nodes (e.g. energy). It consists of two principal activation modes as follows: the first mode is a collaborative activation mode with a high detection rate and a significant resource expenditure, and the second mode is a non-collaborative activation mode with a lower detection rate and resource expenditure. The choice between activating them is made according to the estimated threat. They used a repeated Bayesian game to model their IDS activation mechanism between a potentially malicious sender node and a defense coalition. The results showed that the proposed approach offers a superior combination of attack detection accuracy and energy expenditure when compared to the benchmark methods.

In [74], the authors developed an energy-efficient IDS that uses a game theory approach based on Bayesian Hybrid Detection (BDH) to evaluate the different vulnerabilities and the most susceptible behaviour of the malicious nodes. A BHD allows the defender to adjust itself based on opponent observation. Their approach consists of two components which are low IDS and high IDS. They are assigned for energy-efficient nodes and to control energy spent on IDS. The updated system is another component of the BHD approach which is implemented using the genetic algorithm. The findings indicate that, using the suggested method, the success rate of defense nodes in identifying malicious nodes is more closely aligned with the success rate of attackers. Furthermore, the BDH system exhibits an efficient processing time, which indicates a higher degree of reliability in the context of intrusion detection.

Bayesian Correlated Equilibrium based IDS is a solution that incorporates two main processes - cluster head selection and hybrid IDS - and that was proposed for MANETs [75] in order to improve the IDS strategy; this solution achieved a high detection accuracy while reducing the power consumption of the nodes. In their approach, authors start by electing the cluster head for each cluster using the Vickrey–Clarke–Groves (VCG) technique. Then, a hybrid IDS model is initialized in the Cluster Head to detect intrusions in the network. Furthermore, the hybrid IDS consists of both lightweight and heavy modules. The lightweight module is less powerful and uses simple analytical rules based on threshold values to detect intrusions. On the contrary, the heavy module is more powerful and uses complex association mining rule techniques to detect anomalies. They used a non-cooperative incomplete information static Bayesian game to model the interaction between the cluster head and the potential malicious node. When the malicious node cannot be detected by a lightweight module, the heavy module is activated on the basis of the correlated equilibrium technique. Such a technique is used to lower the risk of high computational costs caused by the earlier methods. The findings demonstrate a superior network speed, a higher packet delivery ratio, and an increased detection rate.

The authors in [76] proposed a Bayesian game theory based MANET IDS scheme comprising a cluster leader election process and a hybrid IDS. They used the Vickrey–Clarke–Groves mechanism to elect the cluster leader, which provides the intrusion detection service to all other cluster nodes for a predefined period of time. The hybrid MANET IDS used comprises one lightweight module and one heavyweight module. In the beginning, only the lightweight module is activated. When the first module detects a malicious node, then the heavyweight module is activated. The decision to activate the heavyweight module is determined by the Nash Equilibrium of the non-cooperative game played between the elected leader node and the node being monitored. The results showed that the suggested methodology effectively decreased the power consumption and the false alarm rate. Furthermore, it maintained an increased detection rate of various types of attacks: Route compromise, Traffic distortion, and Black-hole attacks.

In [77] the authors proposed a system to prevent intrusion in MANETs using a Bayesian model based MAC Identification from multiple nodes in the network.

The authors in [78] reviewed different intrusion detection techniques which used machine learning approaches. They mentioned some IDS schemes that used single Machine learning techniques, such as genetic algorithms, support vector machine, neural networks, fuzzy logic, and data mining. In addition, they mentioned hybrid classifier techniques that combine one or two machine learning techniques. The latter is proposed to build a better intrusion detection system that has two functional components. The first component produces intermediate results, and the second one generates end results. Their proposed IDS solution is a hybrid IDS technique that combines a genetic algorithm and Bayesian game theory. However, the analysis and discussion of this solution are not presented by the authors.

The authors in [9] proposed an anomaly-based intrusion detection system for detecting malicious packet-dropping attacks on the AODV protocol at the network layer. The approach focused on a host-based misuse detection system using the neighbor monitoring technique, along with game theory approaches to recognize the malicious nodes and provide security to the network. The architecture of their system is composed of four modules as follows: the neighbor monitoring module, neighbor trust module, game engine module, and packet forwarding module. The general principle of their system is as follows: every node in the network monitors the behaviour of its neighbor, updates the trust value for each of its neighbors, and uses Game theory for decision-making purposes which consists of a reactive strategy to provide the best move, and a proactive strategy to predict the neighbor's future behaviour. Their system has achieved an increase in the packet delivery ratio with the existence of malicious nodes. The results show that the packet delivery rate is increased in the presence of malicious nodes when compared to the original AODV protocol.

Furthermore, the Dynamic Mean Field Game Theoretic approach, as proposed in [79], has been suggested as a means of addressing security concerns in MANETs. On the other hand, an Intrusion Detection System that incorporates game theory and K-means clustering while considering power consumption is proposed in [80]. The incentive mechanism for Cooperative Intrusion Detection was formulated as an evolutionary game by the authors in [81]. This game achieves an optimal solution to aid nodes in making decisions regarding their participation in the detection.

E. ATTACKS DETECTION

While the intrusion detection approach is a preventive approach that obstructs novel attacks prior to their manifestation and aims to reduce false positives in the network, the attack detection class instead involves the identification and subsequent mitigation of ongoing security breaches, being considered a reactive measure. This section comprises a selection of articles pertaining to attack detection in various scenarios. For instance, the authors in [82] proposed a reactive scheme against MAC layer misbehaviour, with a minimum of changes to the IEEE 802.11 protocol. Their reaction is in the form of an iterative and cooperative game played by different honest nodes to reduce their contention window parameters until their throughput exceeds that of the greedy node. Hence, honest nodes always compare their throughput with that of the greedy node; if exceeding it, nodes continue the transmission without any reaction; otherwise, nodes decrease the minimum and maximum values of their contention window (CWmin and CWmax). However, this approach takes the reaction delay to achieve the game equilibrium, which consists of exceeding the greedy throughput. To mitigate this, they proposed a hybrid reaction strategy by introducing polynomial regression to obtain the empirical curves of the throughput according to the contention window. Results showed that the proposed method was able to bypass the MAC layer misbehaviour attack.

A reputation-based coalition game-theoretic approach is proposed in [83] to detect and exclude insider jamming attacks on MANETs. In this approach, the nodes rely heavily on the availability of transmission rates and a reputation for each individual node in the coalition to detect the presence of an internal jamming node. The reputation of a node is the collection of ratings maintained by other nodes about the given node. The nodes implement a reputation mechanism based on transmission rates. They exclude the attackers from the coalition by rerouting their paths and randomly changing their transmission channel. The results showed that the proposed approach improved network throughput and delay when increasing coalition sizes.

The authors in [84] seek to provide safe and speedy multimedia communication from the source node to the destination using the AODV protocol. To this end, they proposed an algorithm to detect SYN flooding attacks at an early stage. It also finds malicious nodes which try to affect the multimedia communication in MANETs by introducing unnecessary delays. Their mechanism not only detects the attack but also detects the source of the attack and the elements causing delays. They used non-cooperative nonzero-sum game theory to form a game between the malicious node and the multimedia server node. They used the dominant strategy in order to find the Nash Equilibrium (NE) in a nonzero-sum game. The results showed that the proposed detection mechanism offers a stable packet delivery ratio between 90% and 100% with a very reduced additional

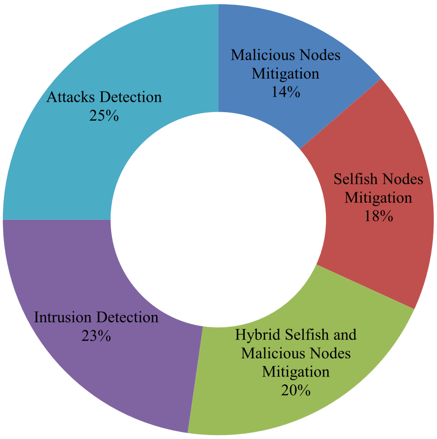

FIGURE 7. Popular detection classes in our taxonomy.

overhead even in the presence of high number of malicious nodes.

In [85], the authors proposed the IFGSPN approach to model an expected attacker-defender interaction in a MANET. They combined theoretical stochastic games, intuitionistic fuzzy logic, and generalized stochastic Petri nets (GSPN) in their approach. Their game is a complete information and zero-sum stochastic type of game.

The authors in [86] used a complete information non-cooperative game to describe the interaction between attacker and defender, which is utilized in the assessment risk of an ad-hoc network. Their approach takes into account the behaviour of the attacker and defender, and introduces the concept of node weight, which is used to distinguish the influence difference of node weight. Their game realized Nash equilibrium, thus leading to a defense strategy and risk evaluation for the network. The findings indicated that nodes with lower weights tend to have lower potential danger. The principal goals of the authors in [87] include securing the data packets and understanding the unpredictable behaviour of the attacker. This is achieved by developing a mechanism of embedding a secret digital code that is resistant to collusion. They used game theory to model the multiple-collusion attacker scenario. In addition, they used game theory to predict nodes' behaviour and to choose an optimal strategy based on auxiliary information to face their opponent. Moreover, this approach is an extension of the previous game model that they proposed in [92] for malicious behaviour detection. The results showed that the proposed approach reduced processing time, decreased resource utilization, and reduced transmission cost in MANETs.

The authors in [88] analyzed the functioning mode of another approach called CORE. In addition, they proposed a new algorithm, named XCORE, to improve the vulnerabilities of CORE. This algorithm takes into consideration different types of attacks such as black-hole cooperative, blackmail, overflow attacks, and selfish behaviour. They used game theory to model their approach. Their model came to an equilibrium situation named Nash's balance. The analysis and arguments of this solution are not presented by the authors.

In addition, a static game theoretic approach was proposed in [89] for security and QoS co-design in MANET. The main goal of their approach is to model the interactions between the attacker's attacking target selection and the source's relay selection. Furthermore, a reputation-based coalition game is proposed in [90] to detect the presence of smart jammer nodes when they are passively eavesdropping and collecting information about the network prior to launching the jamming attack. Another work [91] involves a distributed game theory-based multiagent anti-jamming (DMAA) algorithm as a solution against intelligent jammers. They used a Markov game, and consider the jamming pattern to include sweep jamming and intelligent jamming.

III. SUMMARY AND COMPARISON

In this section, we present the main details of our taxonomy. Our goal is to carry out a systematic review allowing the collecting and indexing of a collection of guides to describe published scientific knowledge on security problems in MANETs that are solved using game theory strategies. In this regard, we grouped significant information into two tables. It is very important to have knowledge about the simulator used, performance metrics, and the attack types of our taxonomy. As a result, we summarized it in Table.2. Our study relates to security problems that used game theory; therefore, we seek to highlight the principal characteristics of game theory as form modeling, game model, game type, concept solution, and information type in Table.3.

We summarize general information about the application of game theory for security in MANETs in the following elements below: detection type, simulator tools, attack types, game elements, game forms, game models, game types, and game solution concepts. And we compare classes that used game theory for security in MANETs in Table.4.

A. DETECTION CLASSES IN MANETS

The pie chart in Fig.7 demonstrates the popular detection genres in the last few years. Overall, attack detection and intrusion detection are the most interesting research, obtaining a percentage of 25% and 23% for each class, respectively. Moreover, we find that malicious nodes mitigation and selfish nodes mitigation are the least popular, obtaining a percentage of only 14% and 18% for each class, respectively. Hybrid selfish and malicious nodes mitigation class is slightly popular for the research domain, with a percentage of 20%.

B. SIMULATOR TOOLS USED

With the spread of different simulation tools, it is important to know which tools are used to resolve MANET security problems based on game theory.

The pie chart in Fig.8 displays simulator tools used in the last few years. Overall, NS-2 is the most popular tool used, with a percentage of 40%, while NS-3, JAVA, DS, VPNPTool,

TABLE 2. Attacks types, Tools used, and performance metrics of works that used game theory for security in MANETs.

		Attack type	Simulator used	Performance metrics
Malicious Nodes Mitigation	[50]	Not specified	NS-2	Throughput, routing overhead, routing latency, average utility, strategy of nodes.
	[51]	Not specified	Java	Detection rate, false positive rate.
	[54]	Not specified	Not specified	Evolution of the malicious/regular populations.
	[53]	Malicious multi-attacker Node collusion (DDoS or black-hole)	MATLAB	Regular node utility, malicious node utility, belief, and uncertainty.
	[55]	Multiple attackers	Not specified	Average consumed energy, average remaining energy.
	[52]	Preventing packet drop and DoS attack (caused by flooding packets)	NS-2	Packet drop rate, average utility, detection accuracy, successful defense rate, energy consumption, and routing latency.
Selfish Nodes Mitigation	[56]	Selfish behaviour	NS-2	Throughput, delay.
	[62]	Selfish behaviour	NS-2	Average delay, control overhead, packet delivery ratio, packet loss.
	[57]	Selfish behaviour	Not specified	Convergent.
	[63]	Selfish behaviour	NS-2	Throughput , end-to-end delay.
	[58]	Selfish behaviour	NS-2	Network performance, system delay.
	[59]	Selfish behaviour	OMNET++	Residual energy, end-to-end delay, throughput.
	[60]	Selfish behaviour	NS-3	Packet delivery ratio, Nodes lifetime, MPR nodes
	[61]	Selfish behaviour	No used simulator	Not implemented.
Hybrid Selfish and malicious nodes Mitigation	[64]	Selfish behaviour + malicious node	NS-3.17	Throughput, packet forwarded, packet received, end-to-end delay.
	[66]	Selfish behaviour + malicious node (black-hole attack)	No used simulator	Packet forward rate, route density factor.
	[68]	Selfish behaviour (misbehaving nodes)+ black-hole	Network Simulator	Packet delivery ratio, delay in packet delivery and network throughput.
	[65]	Selfish behaviour + attacks in a variety of forms (i.e. DoS at different network layers, packet dropping, and routing disruption at the network layer).	DS simulator	Throughput, conserving power.
	[69]	Selfish behaviour + malicious node	Not specified	Utility.
	[67]	Selfish behaviour + malicious node	Not specified	Average utility, false positive rate, detection rate, throughput.
	[70]	Selfish behaviour + malicious node	Not specified	Throughput, packet delivery ratio, routing overhead, propagation delay.
	[71]	Selfish node + Sybil attacks	NS-2	Throughput, evil drop rate, dropped packets.
	[72]	Selfish behaviour + malicious node	Not specified	Not specified
Intrusion Detection	[75]	Not specified	Not specified	Packet delivery ratio, detection rate, throughput, delay.
	[76]	Routing attacks, DoS attacks, packet dropping, packet spoofing	NS-2	Packet delivery ratio, detection rate.
	[77]	MAC identification	NS-2	Delay , average bits transfer.
	[73]	DoS	NS-2	Attack detection accuracy, resources consumption of nodes (residual energy and used memory).
	[78]	Not specified	No used simulator	Not implemented.
	[74]	Not specified	MATLAB	Payoff index, system stability index (SSI), processing vs. accuracy index level.
	[9]	Malicious packet dropping attack	NS-2.28	Packet delivery fraction, routing load, false positives.
	[79]	Black-hole and gray hole attacks	OMNET++	Throughput, packet delivery rate and average cost.
	[80]	Not specified	Not specified	Packet delivery ratio, battery power consumption, and control packet overhead.
	[81]	Not specified	Not specified	Evolution process, cost vs cooperation probability, number of completed tasks.
Attacks Detection	[82]	DoS attacks such as the greedy behaviour (MAC layer misbehaviour).	NS-2	Throughput.
	[83]	Insider Jamming Attacks	NS-2	Throughput, delay.
	[84]	SYN Flooding Attack	NS-2	Packet delivery ratio, control overhead, delay, throughput, jitter.
	[90]	Insider Jamming Attacks	NS-2	Detection accuracy, detection delay, percentage of false positives, and the detection time of the insider jammer.
	[85]	Not specified (Sybil attack, Selfish attack, RREQ flooding attack, and Black-hole attack)	VPNPTool	Certainty, uncertainty, hesitation.
	[86]	Not specified	Not specified	Detection rate, penalty loss.
	[88]	Cooperative black-hole attacks, blackmail, overflow, and selfish behaviour.	No used simulator	Not implemented.
	[87]	Prevention of the multi-collusion attack	MATLAB	Processing time, resource utilization, transmission cost.
	[89]	Not specified	Not specified	Throughput
	[91]	Sweeping jammer, intelligent jammers	Not specified	Cumulative rewards, normalized rates, channel number, performance.

OMNET++, and Network Simulator are the least popular, with a percentage of 3%. MATLAB is not a popular tool either, with a percentage of only 9%. There are some works that did not specify the tools used, scoring a percentage of

TABLE 3. Game Theory properties which used for security in MANETs.

		Game Model	Form modeling	Game type	Concept solution
Malicious Nodes Mitigation	[50]	Non-cooperative	Matrix	Dynamic bayesian signaling game	Perfect bayesian equilibrium
	[51]	Non-cooperative	Matrix	Dynamic bayesian game	Nash equilibrium
	[54]	Non-cooperative	Matrix	Evolutionary game	ESSs
	[53]	Non-cooperative	Not specified	Bayesian game	Perfect bayesian equilibrium
	[52]	Non-cooperative	Extensive	Dynamic repeated game	Subgame perfect equilibrium
	[55]	Not specified	Not specified	Mean field game	Not specified
Selfish Nodes Mitigation	[63]	Non-cooperative	Extensive	Not specified	Nash equilibrium
	[56]	Non-cooperative	Matrix	Repeated games	Not specified
	[57]	Non-cooperative and Cooperative	Matrix	Not specified	Nash equilibrium & Pareto optimal
	[58]	Cooperative	Not specified	Coalition Repeated game	Not specified
	[62]	Not specified	Not specified	Supervisory game	Not specified
	[59]	Cooperative	Not specified	Coalition game	Not specified
citesahnoun2018coalition	Cooperative	Not specified	Coalition game	Not specified	Not specified
	[61]	Non-cooperative	Matrix	Not specified	Nash equilibrium
Hybrid Selfish and Malicious Nodes Mitigation	[64]	Non-cooperative	Matrix	Static and repeated game	Nash equilibrium
	[69]	Non-cooperative	Not specified	Bayes' theorem.	Perfect bayesian equilibrium.
	[67]	Non-cooperative	Matrix	Bayesian signaling game	Bayesian equilibrium
	[66]	Cooperative	Matrix	Cooperative	Not specified
	[65]	Non-cooperative	Extensive, matrix	Dynamic bayesian game	Bayesian nash equilibrium
	[68]	Not specified	Not specified	Supervisory game	Not specified
	[70]	Non-cooperative	Extensive, matrix	Bayesian game (static and dynamic)	Not specified
	[71]	Non-cooperative	Matrix	Repeated game	Nash equilibrium
	[72]	Cooperative	Not specified	Bargaining game	Nash equilibrium
Intrusion Detection	[75]	Non-cooperative	Matrix	Static bayesian game	Bayesian correlated equilibrium
	[76]	Non-cooperative	Matrix, extensive	Static bayesian game	Bayesian nash equilibrium
	[77]	Non-cooperative	Not specified	Bayesian game	Not specified
	[73]	Non-cooperative	Not specified	Repeated bayesian game.	Perfect bayesian equilibrium.
	[78]	Non-cooperative	Not specified	Bayesian game	Not specified
	[74]	Non-cooperative	Not specified	Bayesian game	Not specified
	[9]	Non-cooperative	Matrix	Reactive and proactive game	Nash equilibrium
	[79]	Not specified	Extensive	Dynamic mean field game	Not specified
	[80]	Not specified	Not specified	Not specified	Not specified
	[81]	Non-cooperative	Not specified	Evolutionary game	ESS
Attacks Detection	[82]	Non-cooperative	Extensive	Subgame theory	Subgame perfect equilibrium
	[84]	Non-cooperative	Matrix	Nonzero sum game	Nash equilibrium
	[85]	Non-cooperative	Matrix	Zero-sum stochastic games	Nash equilibrium
	[86]	Non-cooperative	Matrix	Zero-sum	Nash equilibrium
	[88]	Non-cooperative	Matrix	Selfish games	Nash's balance
	[87]	Non-cooperative	Not specified	Bayesian signalling game	Perfect nash equilibrium
	[83]	Cooperative	Not specified	Coalition game	Not specified
	[90]	Cooperative	Not specified	Coalition game	Not specified
	[89]	Non-cooperative	Matrix	Static game	Nash equilibrium
	[91]	Non-cooperative	Not specified	Markov game	Not specified

24%. On the other hand, other works did not implement their proposal, representing 9% in total.

C. ATTACKS TYPES ADDRESSED

It is important to know which type of attack is addressed by game theory strategies in the context of MANETs. The pie chart in Fig.9 illustrates attack types in the studied works in this survey.

Overall, the selfish attack is the main target of research, with a percentage of 31%, while attack types such as routing attacks, flooding, blackmail, overflow, and Sybil are the least addressed in research, with a percentage of only 3%. There are some works that did not specify the attack types that were handled with a percentage of 25%. Regarding selfish attacks, certain articles solely consider this aspect, as was presented in the selfish nodes mitigation class. There are other articles that take into consideration selfish attacks along with other attack types, as we presented in the class of hybrid selfish and malicious nodes mitigation. The authors in [64], [67], [69], and [70] addressed selfish attacks and another attack type, but they did not specify which other attack was contemplated. The works in [66] and [68] handled selfish and black-hole attacks. The work in [71] handled selfish attacks and Sybil attacks. DoS Subclass attacks are not as popular in literature as black-hole attacks, being that black-hole attacks achieve a percentage of 10%. On the other hand, DoS attacks are slightly more popular, achieving a percentage of 18%. In the DoS Subclass sector, most works surveyed (8%) had processed DoS attacks in general. Insider jamming attack is a type of DoS attack that some works considered (5%). SYN flooding and greedy attacks are other types of DoS attacks that were addressed by about 3% of the surveyed works.

D. GAME THEORY ELEMENTS

The primary objective of our study is to conduct a literature survey of works that employed game theory as a means

TABLE 4. Comparison between classes used game theory for security in MANETs.

	Malicious Nodes Mitigation	**Selfish Nodes Mitigation**	**Hybrid Selfish and Malicious Nodes Mitigation**	**Intrusion Detection**	**Attacks Detection**
Detection Types	14%	18%	20%	23%	25%
Simulator tools	• **NS-2:** [50], [52]. • **JAVA:** [51]. • **MATLAB:** [53]. • **Not specified:** [54], [55].	• **NS-2:** [56], [62], [58] , [63]. • **OMNET++:** [59]. • **NS-3:** [60]. • **Not specified:** [57], [61]	• **NS-2:** [71]. • **DS simulator:** [65]. • **NS-3:** [64]. • **Not specified:** [66], [69], [70], [67], [72].	• **NS-2:** [73], [76], [9], [77]. • **OMNET++:** [79]. • **MATLAB:** [74]. • **Not specified:** [75], [80], [81], [78]	• **NS-2:** [82], [83], [90], [84]. • **MATLAB:** [87]. • **VPNPTool:** [85]. • **Not specified:** [88], [86], [89], [91].
Attack types	• **DoS/DDoS:** [53], [52]. • **Black-hole attacks:** [53]. • **Not specified:** [50], [51], [54].	**Selfish behaviour.**	• **Selfish behaviour:** [64], [67], [70], [69], [66], [68], [71], [65], [72]. • **Black-hole attacks:** [66], [68]. • **Sybil attacks:** [71].	• **DoS:** [73], [76]. • **MAC identification attacks:** [77]. • **Packet dropping:** [9], [76]. • **Not specified:** [74], [75], [78], [80], [81].	• **Insider Jamming attacks:** [83], [90]. • **SYN flooding attacks:** [84]. • **Greedy attacks:** [82]. • **Overflow attacks:** [88], [85]. • **Multi-collision attacks:** [87]. • **Jamming attacks:** [91]. • **Not specified:** [86], [89].
Game theory forms	• **Matrix form:** [50], [51], [54]. • **Extensive form:** [52]. • **Not specified:** [53], [55].	• **Matrix form:** [56], [57]. • **Extensive form:** [63]. • **Not specified:** [58], [62], [59].	• **Matrix form:** [64], [67], [66], [71]. • **Two forms:** [65]. • **Not specified:** [68], [69].	• **Matrix form:** [75], [9]. • **Two forms:** [76]. • **Not specified:** [73], [74], [77], [78], [80], [81].	• **Matrix form:** [84]–[86], [88], [89]. • **Extensive form:** [82]. • **Not specified:** [83], [87], [90], [91].
Game theory models	• **Non-cooperative game:** [50], [51], [54], [53], [52]. • **Not specified:** [55].	• **Non-cooperative game:** [63], [56], [57], [61] • **Cooperative game:** [58], [59], [57], [60]. • **Not specified:** [62].	• **Non-cooperative game:** [64], [69], [67], [65], [70], [71]. • **Cooperative game:** [66], [72]. • **Not specified:** [68].	• **Non-cooperative game:** [9], [73]–[78], [81]. • **Not specified:** [79], [80].	• **Non-cooperative game:** [82], [84]–[89], [91]. • **Cooperative game:** [83], [90]. • **Not specified:** [79], [80].
Games theory types	• **Bayesian game:** [53], [51], [50]. • **Dynamic repeated game:** [52]. • **Mean field game:** [55]. • **Evolutionary game:** [54].	• **Supervisory game:** [62]. • **Repeated game:** [56]. • **Coalition game:** [59], [60]. • **Not specified:** [63], [57], [61].	• **Bayesian game:** [69], [67], [65], [70]. • **Cooperative game:** [66]. • **Repeated game:** [71], [64]. • **Supervisory game:** [68]. • **Bargaining game:** [72].	• **Bayesian game:** [77], [78], [74], [75], [76], [73]. • **Evolutionary game:** [81]. • **Repeated game:** [73]. • **Reactive and proactive game:** [9]. • **Not specified:** [81].	• **Subgame:** [82]. • **Nonzero-sum game:** [84]. • **Zero-sum game:** [85], [86]. • **Selfish game:** [88]. • **Bayesian signaling game:** [87]. • **Coalition game:** [83], [90]. • **Markov game:** [91].
Game theory solution concepts	• **Perfect Bayesian equilibrium:** [53], [50]. • **Nash equilibrium:** [52]. • **Subgame perfect equilibrium:** [52]. • **Evolutionary stable strategy:** [54]. • **Not specified:** [55].	• **Nash equilibrium:** [63], [57], [61]. • **Pareto optimal:** [57]. • **Not specified:** [56], [59], [62], [60].	• **Nash equilibrium:** [64], [71], [72]. • **Bayesian equilibrium:** [69], [67]. • **Bayesian Nash equilibrium:** [65]. • **Not specified:** [66], [68].	• **Nash equilibrium:** [9]. • **Bayesian equilibrium:** [73]. • **Bayesian Nash equilibrium:** [76]. • **Bayesian correlated equilibrium:** [75]. • **ESSs:** [81]. • **Not specified:** [74], [77], [78], [80].	• **Nash equilibrium:** [84]–[86], [89], [87]. • **Subgame perfect equilibrium:** [82]. • **Nash's balance:** [87]. • **ESSs:** [81]. • **Not specified:** [83], [90], [91].
Players and actions	• **Normal node:** -- **{cooperate, decline}:** [50]. -- **{cooperate, Defect}:** [52]. • **Malicious node:** -- **{attack, no attack}:** [50]. -- **{cooperate, defect}:** [52].	• **Normal node:** -- **{normal, selfish}:** [56]. -- **{cooperate, not cooperate}:** [57]. • **Selfish node:** -- **{trust, isolate}:** [56]. -- **{cooperate, not cooperate}:** [57].	• **Normal node:** -- **{forward, drop}:** [66]. -- **{cooperate, not cooperate}:** [64]. • **Malicious node:** -- **{forward, drop}:** [66]. -- **{cooperate, not cooperate}:** [64].	• **IDS:** -- **{monitor, not monitor}:** [75], [76], [74]. • **Malicious node:** -- **{attack, not attack}:** [75], [76], [74].	• **Normal node:** -- **{decrement parameters, does not decrement}:** [82]. -- **{select, not select}:** [89]. • **Malicious node:** -- **{cheat, not cheat}:** [82]. -- **{attack, not attack}:** [89].

of addressing security concerns in MANETs. Therefore, acquiring comprehensive knowledge regarding game theory is imperative for further understanding.

The foundational components of game theory consist of the identification of players and their corresponding actions. The majority of the literature surveyed employs a two-player framework, wherein participants assume the roles of either an attacking node, a selfish node, or a normal node. In relation to the conduct of the player, it can be observed that each individual player possesses a total of two distinct actions. In our taxonomy, we provide instances of player types and their corresponding actions for each class, as indicated in Table.4.

E. GAME THEORY FORMS

There are two primary forms for the representation of game theory, namely, the matrix form and the extensive form.

Figure 10 illustrates the proportion of form types utilized by the participants of our survey. Typically, a majority of the studies employ a matrix form to represent their game, accounting for 49% of the sampled studies, whereas the utilization of the extensive form is comparatively low, constituting only 15% of the works surveyed. Approximately 36% of the works analyzed did not utilize any specific form.

F. GAME THEORY MODELS

There are two principal models of game theory followed in the works of our survey: the non-cooperative game model, and the cooperative game model.

Fig.11 presents a bar chart that displays the frequency of game model works that fall within each class of our taxonomy. The results indicate that the non-cooperative game model was more prevalent than the cooperative game model. The non-cooperative game model was predominantly utilized

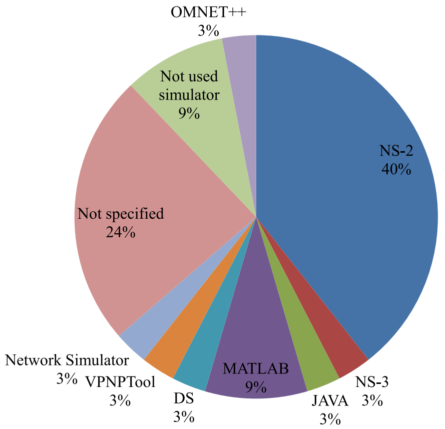

FIGURE 8. Pie chart of simulation approaches for validating the different solutions proposed.

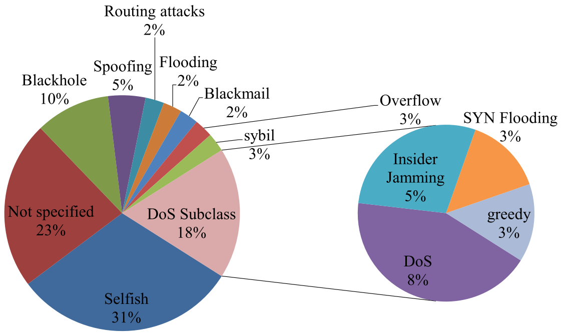

FIGURE 9. Percentage of works addressing different attack types.

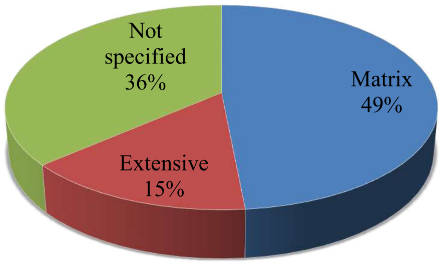

FIGURE 10. Percentage of game theory forms adopted.

in the works belonging to the five categories of our taxonomy. Upon closer examination of the information, it is evident that all of the surveyed works pertaining to the mitigation of malicious nodes and intrusion detection employed the non-cooperative game model. In contrast, the selfish nodes mitigation category employed a non-cooperative game model in four of the studies, and a cooperative game model in four other studies. Conversely, the attacks detection category utilized a cooperative game model in only 2 studies, and a non-cooperative game model in eight others. The hybrid selfish and malicious nodes mitigation class has employed a cooperative game model in two of the studies, and a non-cooperative game model in six other studies.

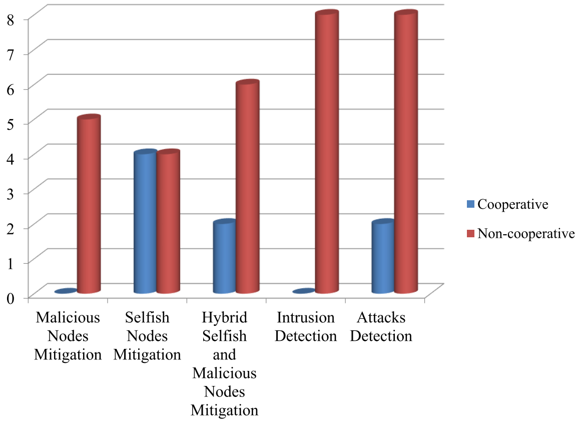

FIGURE 11. Game models adopted by the different surveyed works.

G. GAMES THEORY TYPES

Despite the various categories of games that can be found in the context of cooperative game theory, two sole types of game model are identified: the coalition game, and the bargaining game.The coalition game was the subject of investigation in five of the studies included in our survey analysis, whereas, the bargaining game was used in one study only. The non-cooperative game model encompasses multiple game types.

The pie chart in Fig.12 compares the percentage of seven game types of the Non-cooperative game model which were utilized by the works included in our study. Overall, the researchers solved the problem of security in MANET mostly with three principal game types: Bayesian game, Subgame theory, and Repeated Game. In detail, the Bayesian game was the most utilized game type all over the works. It accounted for nearly half of the total works studied. It is used alone or hybridized with Dynamic, Static, and repeated game types. The second most used game type was the Subgame theory, with 17%. It was utilized as such, or used Bayesian Signaling game, which is considered a type of Subgame theory. The third most used game type was the repeated game, with 13%. It is used alone or hybridized with dynamic, static, and Bayesian game types. Static, non-zero-sum, zero-sum, and evolutionary are the remaining game types used. A static and non-zero-sum game shared almost the same level, at 9% only. A zero-sum is not as popular as an evolutionary game with 4%.

H. GAME THEORY SOLUTION CONCEPTS

Understanding the solution concept is a crucial aspect of game theory. The survey under consideration employs six solution concepts.

The pie chart in Fig.13 describes the information of the different solution concepts that are utilized in the works of our study. The various solution concepts into which this study is distinguished are Bayesian equilibrium, Subgame perfect equilibrium, Nash equilibrium, Bayesian correlated equilibrium, evolutionary stable strategy, and

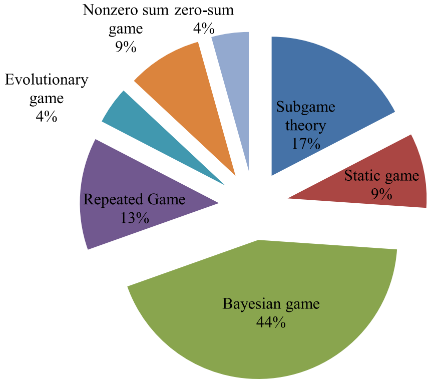

FIGURE 12. Percentage distributed over the game types.

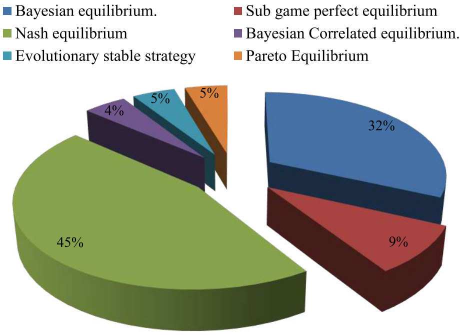

FIGURE 13. Percentage of game theory approaches used in the surveyed literature.

Pareto equilibrium. Nash equilibrium contributes 45% of the total number of works. Bayesian equilibrium constitutes 32% of the total number of works. 9% of the works used Subgame perfect equilibrium. Evolutionary stable strategy and Pareto equilibrium have a contribution are 5%. The remaining 4% of the total number of works comes from Bayesian correlated equilibrium. In the end, it can be concluded that Nash equilibrium and Bayesian equilibrium are the main approaches used by most of the works. On the other hand, Subgame perfect equilibrium, Bayesian correlated equilibrium, evolutionary stable strategy, and Pareto Equilibrium, are not popular in search works.

IV. DISCUSSION

In this section, a discussion study of MANET security using game theory is presented. Table.5 displays the objectives, advantages, and drawbacks of each work, where security in MANETs using game theory is classified according to the type of attack detection. In addition, Table.6 summarizes the main performance metrics of the discussed categories.

By studying these methods, and as presented before, we can discuss the advantages and drawbacks that are present in the different classes where game theoretic methods for MANET security can be classified.

The primary aim of mitigating malicious nodes in a given class is to identify and minimize the presence of any nodes that exhibit malicious behaviour. Furthermore, within this particular classification, there are two distinct subcategories, distinguished primarily by their respective approaches to the conservation of resource utilization. The malicious behaviour detection subclass failed to consider resource conservation, whereas the malicious nodes mitigation with resources preservation subclass prioritized it. Furthermore, the main drawbacks of the mentioned works in this class are:

- Did not take into account selfish nodes.
- Did not take into account imperfect information in their game.
- Considered only incomplete information in their game.
- Did not specify the type of information in some works.

The primary aim of the selfish nodes mitigation class is to prevent or segregate nodes exhibiting selfish behaviour from the network. The primary benefit of this class is the enhancement of MANET performance. The drawbacks of this class can be summarized as follows:

- Did not take into consideration power consumption.
- The occurrence of a significant wastage of MANETs resources as a result of isolated selfish nodes.
- Did not take into consideration the attacks from malicious nodes.
- Did not specify the type of information in most works.

The hybrid selfish and malicious nodes mitigation class aims to identify instances of node misbehaviour, encompassing both malicious and selfish nodes, through an integrated approach. The drawbacks of this class are highlighted as follows:

- The power consumption was not taken into consideration.
- Not applicable to other routing protocols except the specified one.
- Several changes were made to the protocol specification.
- The games they designed were limited to a two-player format.
- Did not specify the type of information in some works.

The primary aim of the intrusion detection class is to present a proficient intrusion detection mechanism that minimizes power consumption. This class offers benefits such as enhanced network intrusion detection capabilities, and reduced power consumption. The drawback of this class is that it does not take into consideration cooperative attacks, and does not specify the type of information in some works.

In the attacks detection class, the main objective is detecting specific attacks. The main advantage of this class is an improved MANET defense strategy. The drawbacks of this class are summarized as follows:

- Not applicable to other attacks.
- Did not investigate a case of cooperative attacks.
- Did not take into consideration selfish nodes.
- Did not take into consideration power consumption.
- Used complete information in some works, while other works did not specify the type of information.

TABLE 5. Review of works that used game theory for security in MANETs.

Ref	Objectives	Solution proposed	Advantages	Drawbacks
[50]	Finding malicious activities and behaviours, and preventing packet-dropping attacks.	Using Dynamic Bayesian signaling game to find malicious activities and behaviours, and incomplete information PBE to prevent packet-dropping attacks.	Revealing the best actions of individual strategies for each node, determining the malicious behaviour of a node, and furnishing secure and reliable communication that makes effective cooperation among nodes.	Did not take into consideration multiple attacks, energy consumption, and selfish nodes.
[51]	Detecting malicious nodes, recognizing, punishing, or expelling.	Using a Dynamic Bayesian game, which is non-cooperative with incomplete information.	Using more strategies in the game for all of the normal and malicious nodes, and storing data in a concise and compact manner to be used in different stages and cooperation of neighbouring nodes.	Did not take into consideration selfish nodes and did not preserve the resources consumption.
[64]	Preventing malicious behaviour and avoiding selfish and malicious nodes during the routing process.	Using Static and Repeated Game Theory with Nash Equilibrium.	Enforcing cooperation between nodes, improving network performances, and preventing malicious nodes.	Not applicable to other routing protocols except OLSR. Introduced many modifications to the OLSR protocol. Used a unique parameter (cooperation rate) to evaluate node behaviour, and did not take into consideration other parameters like the overload of the path, and the energy consumption of the nodes constituting the path.
[54]	Predicting malicious behaviours and preserving resource consumption.	Using evolutionary game theoretic with ESSs in pure strategies.	Allowing a regular node to tune its defensive strategy so as to achieve an effective defense adapted to the attacker's strategy, and taking into consideration energy consumption.	Did not study selfish and erroneous nodes and installed host IDSs on each regular node.
[66]	Detecting selfish nodes and avoiding malicious nodes.	Using Cooperative game theory with a CSN-NRN mechanism.	Guaranteeing secure and uninterrupted data transfer from the source to the destination node in a minimum idle time, and taking into consideration route recovery and the effect of misbehaving nodes in the MANET.	Not applicable to other routing protocols except AODV; introduced many modifications to the AODV protocol, and did not take into consideration the other types of selfish behaviour of AODV nodes that can be detected; did not address the detection of malicious nodes, and their removal from the network.
[53]	Representing the unpredictable behaviour of nodes.	Using Bayesian game with Perfect Bayesian equilibrium.	Effective in the detection of misbehaving nodes, and in taking into account collusion between attacker nodes.	Did not take into consideration energy consumption, and did not study Selfish and erroneous nodes.
[68]	Detecting misbehaviour nodes.	Using a misbehaviour node detection scheme, an incentive-based reputation scheme, and a game theoretical approach.	Reducing the misbehaviour node detection cost in the network, identifying selfish nodes and isolating them, ensuring mutual cooperation among selfish nodes, and increasing network throughput and packet delivery rate.	Not applicable to other routing protocols except DSR. Did not take into consideration consumption power, and lacks malicious nodes analysis.
[55]	Predicting malicious behaviours while preserving resource consumption.	Using an improved mean field game theoretic (IMFGT) approach.	Could be applicable to multiple defenders and multiple attackers; could be used in both dynamic and centralized environments, and takes into consideration consumption power.	Did not explain the working principle, and did not take selfish nodes into consideration.
[65]	Detecting malicious and selfish nodes.	Using a Bayesian game with imperfect and incomplete information and Bayesian Nash Equilibrium.	Efficiency to determine the types of nodes within a reasonable timeframe while conserving power, exploiting malicious and selfish nodes for the benefit of the network, and retention of the malicious nodes to make use of coexistence in some situations.	Did not take into consideration consumption power, and multiple attacker-defender scenarios have not been considered.
[69]	Detecting misbehaving Nodes and selfish nodes.	Using Bayes' theorem, a belief system, neighbor monitoring concept, and Perfect Bayesian equilibrium.	Effective in detecting misbehaving nodes.	PBE strategy suffered slightly when selfish behaviour is exhibited.
[52]	Detecting malicious nodes.	Using dynamic repeated game with Subgame perfect equilibrium.	Showed better efficiency in malicious node detection, improved the security-based routing in MANET, and is effective in terms of power consumption.	Did not take into consideration selfish nodes and energy consumption.
[67]	Exploring malicious behaviours and detecting selfish nodes.	Using Bayesian Signaling game and a reputation system.	Showed better efficiency in malicious node detection	Did not take into consideration power consumption.
[56]	Detecting and preventing selfish behaviour.	Using adaptive threshold algorithm with repeated games theory.	Showed better efficiency in the aspects of throughput and delay in MANETs, and effective detection and prevention of selfish behaviour.	Less efficient when the network topology changes frequently, does not adapt to dynamic network environments, and did not take into consideration power consumption.
[62]	Identifying and isolating selfish nodes.	Using an Audit-based Misbehaviour Detection (AMD) scheme, an incentive-based reputation scheme, and a Game theoretic approach.	Simulation results showed minimum delay, control overhead, packet loss, and an increase in packet delivery ratio with improved network performance.	Huge wastage for a MANET because of isolated selfish nodes.

TABLE 5. ***(Continued.)*** **Review of works that used game theory for security in MANETs.**

[57]	Avoiding selfish behaviour.	Using a credit-based system with game theory.	Showed better efficiency in avoiding selfish behaviour.	Did not take into consideration the vulnerability of the network from the rich credit nodes or attacks from malicious nodes.
[63]	Identifying selfish nodes and isolating them from the network.	Using Non-cooperative game theory with perfect information.	Improving the performance of the Ad-hoc network in both static and dynamic environments.	Huge wastage for a MANET because of isolated selfish nodes; did not take power consumption into account.
[58]	Avoiding selfish behaviour and motivating selfish nodes to cooperate.	Using a cooperative repeated game with imperfect information.	Effective in the detection of selfish nodes, decreasing selfish nodes in a MANET, and improving the performance of MANET.	Did not take into consideration power consumption.
[75]	Improving IDS strategy with high detection accuracy while reducing power consumption.	Using a Non-cooperative static Bayesian game with incomplete information, a Hybrid IDS, and Bayesian Correlated equilibrium.	Improving the detection of intrusions in the network, minimizing power consumption, minimizing intrusion-related traffic in the network, developing an IDS with a high detection rate and accuracy, and prolonging cluster lifetime.	High network overhead due to the VCG mechanism, unfair distribution of processing load among the nodes in a cluster, high time overhead due to the IDS leader election algorithm, not taking into consideration cooperative attacks, and consuming more energy and processing overhead due to the availability of a heavy IDS module and a lightweight module on every node.
[76]	Intrusion detection and minimizing power consumption.	Using a Non-cooperative Bayesian game with incomplete information, Hybrid IDS, and Bayesian Nash Equilibrium.	Minimizing power consumption, achieving a high detection rate, reducing the false alarm rate, prolonging the cluster lifetime, and minimizing intrusion-related traffic in the network.	Incurring in marginal overheads due to cluster leader node election, and failing to detect cooperative attacks.
[77]	Preventing intrusion and improving energy consumption.	Using a Bayesian game with incomplete information.	Providing a lightweight burden to nodes thereby improving energy efficiency; simulated results showed improvement in estimated delay and average bit transfer parameters.	Did not explain the theory side and game theory side.
[73]	Finding an intrusion detection mechanism allowing the reinforcement of network security while preserving the network nodes' resources.	Using repeated non-cooperative Bayesian game with Perfect Bayesian equilibrium.	Effective in the detection of attacks with less power consumption.	Did not consider malicious node coalitions in the proposed approach; design proposed for a specific attack.
[78]	Intrusion detection and treating resource consumption issues.	Using a hybrid IDS technique that combines a genetic algorithm with Bayesian game theory.	Accuracy in the results and prolonged cluster lifetime.	Did not demonstrate the contribution through simulation or experimentation.
[74]	Intrusion detection system.	Using Bayesian game theory, Bayesian Hybrid Detection approach, and Genetic algorithm.	Could detect multiple forms of attacks.	Did not take into consideration cooperative attacks.
[89]	Attack detection in heterogeneous networks.	Using a static game-theoretic approach for security and QoS co-design with Nash equilibrium.	Showed better efficiency in a quantitative framework for relay selection and study of the trade-off between system performance (throughput) and system security requirements.	Did not specify the type of attacker, meaning that both selfish and malicious nodes are categorized as one; did not take into consideration multiple attacks.
[82]	Proposing a novel reaction scheme against the MAC layer misbehaviour while minimizing changes to the IEEE 802.11 protocol.	Using subgame theory with complete and perfect information and Kühn's algorithm.	Effective to bypass the MAC layer misbehaviour attack while minimizing changes to the IEEE 802.11 protocol.	Not applicable to other routing attacks and protocols, and adding a modification to the IEEE 802.11 protocol.
[83]	Detecting and mitigating insider jamming attacks.	Using reputation-based coalition game-theoretic with imperfect information.	Providing a framework to quantify information needed by adversaries to launch insider attacks, improving MANETs' defense against insider attacks, reducing the incorrect classification of legitimate nodes as jammers, and excluding the attackers from the coalition by rerouting their paths and randomly changing their channel of transmission.	Did not use thousands of nodes in simulations and experiments, the attackers' nodes still utilize the network services due to lack of isolation; the case of cooperative attacks that could occur when the excluded nodes form a coalition with the aim of jamming communication in their previous coalition was not studied.
[84]	Detecting the attack and also detecting the source of the attack, and the delay introduced.	Using a non-cooperative nonzero-sum game with Nash Equilibrium.	Detecting the presence of the SYN flooding attack at an early stage, and finding malicious nodes which try to affect the multimedia communication in MANETs by introducing unnecessary delays.	Not tested on other routing protocols except AODV; did not confirm the efficiency by comparing it with other protocols.
[90]	Preventing internal attacks caused by an erstwhile legitimate node.	Using reputation-based coalition game.	Improving the network's defense strategy, and reducing false positives that result from the incorrect classification of unfortunate legitimate nodes as insider jammers.	Did not investigate a case of cooperative attacks that could occur when the excluded nodes form a coalition with the aim of jamming communication in their previous coalition.

TABLE 5. ***(Continued.)*** **Review of works that used game theory for security in MANETs.**

[85]	Describing more accurately the expected behaviour of attackers' interactions with the defense of MANET nodes.	Using theoretical stochastic games with complete information and non-zero-sum games, intuitionistic fuzzy logic, and generalized stochastic Petri nets (GSPN).	Describing in a more realistic way the expected behaviour of attackers, the behaviour of the security system, and dependability being taken into account. Introducing time aspect and intuitionistic fuzzy parameters for characterizing the success probabilities of the attacker's actions, allowing to evaluate some QoS parameters, and helping to estimate expected losses associated with different attack and defense strategies.	Relying on the underlying assumption that the attackers have a complete overview of the security system that might not always be a valid assumption.
[86]	Describing the interaction between attacker and defender.	Using non-cooperative game theory zero-sum with complete information and Nash equilibrium.	Effective in the description of the interaction between attacker and defender.	The utilization of complete information did not correspond with reality.
[88]	Studying attacks and countermeasures.	Using Game theory with Nash's balance.	Taking into consideration different types of attacks and selfish nodes.	Presenting only the theoretical side.
[87]	Understanding the unpredictable behaviour of the attacker.	Using a multistage game with Nash Equilibrium.	Reducing processing time, decreasing resource utilization, and reducing transmission cost.	Did not take into consideration power consumption.
[9]	Intrusion detection.	Using a neighbor monitoring technique and game theory.	Increasing the packet delivery rate by 42% in the presence of malicious nodes, recognizing malicious nodes at the beginning, and eliminating them from the network.	Not applicable to other routing protocols except AODV; requires adding many modifications to the AODV protocol; did not take into consideration other types of attacks.
[59]	Controlling the selfish nature and defining a power control mechanism.	Using a cooperative game and A Stable Payoff Allocation(SPA)" model.	Showing a trade-off between power consumption and the effectiveness of networks in terms of throughput.	Did not take into consideration the vulnerability of the network from the attacks from malicious nodes.
[70]	Malicious and selfish nodes detection.	Using the Non-cooperative Bayesian game approach.	Increasing the throughput and packet delivery ratio, and decreasing the routing overhead and propagation delay.	Did not take into consideration consumption power and multiple attackers scenarios.
[91]	Avoiding attacks when there are intelligent jammers.	Using Markov game and distributed multi-agent anti-jamming algorithm (DMAA).	Simulation results show that the proposed DMAA can make the right decisions to adapt to the policy of the jammer effectively in different situations.	Did not study multi-hop scenarios, and did not take the change of hopping cost into consideration.
[79]	Intrusion detection system.	Using a dynamic mean field game theoretic approach.	Simulation results corroborate that the dynamic mean field game theoretic scheme outperforms the static scheme.	Did not take power consumption into consideration.
[80]	Improving intrusion Detection System and power consumption.	Using Game theory and K-means.	Improving power consumption.	Did not support a heterogeneous network, and did not take into account standards related to quality of service and time.
[81]	Cooperative intrusion detection.	Using an incentive mechanism and an evolutionary game.	Efficiently incentivizing non-malicious nodes to cooperate and decreasing the false detection rate.	Only discussing the situation in which nodes pay more attention to their reputation scores; did not consider nodes with different attitudes on reputation and economic benefits.
[71]	Malicious and selfish nodes detection	Using reputation-based scheme and game theory.	Reducing throughput consumed by malicious nodes and increasing good node throughput in the network.	Did not take into consideration incomplete information.
[60]	Avoiding selfish behaviour, supporting energy-aware and available bandwidth routing.	Using cooperative game and integrating it into OLSR protocol.	Enforcing cooperation between nodes and efficiently prolonging the network lifetime.	Not applicable to other routing protocols except OLSR and introduced many modifications to the OLSR protocol.
[61]	Identifying and isolating selfish nodes.	Using Non-cooperative game theory with ESSDSR algorithm.	Clarity to identify and isolate selfish nodes in a theoretical manner.	Huge wastage for a MANET because of isolated selfish nodes.
[72]	Optimizing resource allocations, coexistence with colluding nodes, and mitigating selfish behaviour.	Using bargaining game with Nash equilibrium.	Efficiently identifying the malicious behavior of colluding nodes.	Did not eliminate malicious nodes and did not take into account standards related to quality of service and time.

V. OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

This survey provides insight into the game theory methodologies currently employed in the realm of security for MANETs, as well as the anticipated research trajectories for addressing security concerns in MANETs through game theory.

Game theory plays an important role in MANET security. All the same, there is little research in this field. In addition, the existing works suffer from numerous problems. In this section, we discuss the limitations of the extensive survey conducted in this work. In addition, based on the conducted survey, we provided a set of promising future research directions.

1) Limitations of current game theory for security techniques in MANETs:
   - Most of the game models integrated in MANET security techniques used two players. Yet, there are

TABLE 6. Performance metrics detailed for works that used game theory for security in MANETs.

		Throughput	Delay	Average Delay	End-to-End delay	System delay	Control Overhead	Convergent	Packet Delivery Ratio	Packet received	Packet loss	Detection Rate	Detection delay	Detection time	Percentage of false positives	Network performance	Accuracy	Resources consumption of nodes (Used memory & Residual energy)	Resource utilization	Conserving power	Average consumed energy	Average remaining energy	Average bits transfer	Jitter	Certainty	Uncertainty	Hesitation	Penalty losse	Processing time	Transmission cost	Payoff index	System stability index	Regular node utility	Malicious node utility	Average Utility	Routing overhead	Routing latency	Strategy of Nodes
Malicious Nodes Mitigation	[53]																									✓							✓	✓				
	[50]	✓																																	✓	✓	✓	✓
	[51]											✓			✓																							
	[52]										✓						✓				✓														✓		✓	
	[54]																																					
	[55]																				✓	✓																
Selfish Nodes Mitigation	[56]	✓	✓																																			
	[57]							✓																														
	[58]					✓										✓																						
	[62]			✓			✓		✓		✓																											
	[63]	✓			✓																																	
	[59]	✓			✓													✓																				
	[60]								✓																													
	[61]																																					
Hybrid Selfish and Malicious Nodes Mitigation	[68]	✓	✓						✓																													
	[69]																																✓	✓				
	[67]	✓										✓			✓																				✓			
	[64]	✓			✓				✓	✓																												
	[66]								✓																													
	[65]	✓																		✓																		
	[70]	✓							✓																											✓		
	[71]	✓									✓																											
	[72]																																					
Intrusion Detection	[73]																✓	✓																				
	[74]																✓												✓		✓	✓						
	[75]	✓	✓						✓			✓																										
	[76]								✓			✓																										
	[77]		✓																																			
	[78]																																					
	[9]								✓						✓																							
	[79]	✓							✓																													
	[80]						✓		✓												✓																	
	[81]																																					
Attacks Detection	[82]	✓																																				
	[83]	✓	✓																																			
	[84]	✓	✓				✓																															
	[85]																								✓	✓	✓											
	[86]											✓																✓										
	[87]																		✓										✓	✓								
	[88]																																					
	[90]												✓	✓	✓																							
	[89]	✓																																				
	[91]															✓																						

cases when a modelization based on solely two players is not sufficient as multiple attackers or collusion between the attackers may arise. Each player is limited to assuming the role of a certain sort of attacker since they are unable to exhibit different behaviours simultaneously. Furthermore, the states of defense exhibit variations depending on the type of attacker, and it is more effective to use collaborative defense strategies among defenders rather than relying just on unilateral defense measures.

- Each player of the game models considered in MANET security techniques has two strategies. Yet, having only two strategies is not enough to model accurately the behaviour of the player. Furthermore, the wide range of actions presents a challenge in terms of the player's behaviours.
- The form model of the game is a crucial component in describing the game, and in illustrating the interactions between players; however, there are numerous works that do not specify the form models in the context of game theory.
- There are quite a large number of game theory strategies besides the types of games used in existing works. None of these additional types are used despite their effectiveness.
- The identification of information type is crucial in assessing the players' knowledge ratio relative to their opponent, as well as the contextual factors; however, most of the MANET security techniques mentioned in this survey failed to specify it.
- In MANETs, there are considerable types of attacks that still need to be modelled by game theory.
- In game theory, there are numerous concepts that have not been applied in MANET security.
- A significant proportion of attention is directed to optimizing the metrics of throughput, delivery packet ratio, latency, and false positives ratio; however, other important QoS metrics were neglected (e.g. bit rate, energy consumption, jitter, network lifetime).
- There is a lack of specific measurements pertaining to game theory that effectively demonstrate the impact of games inside networks. All of the aforementioned studies focus on evaluating the network's performance, which may be influenced by several external variables unrelated to the game itself.
- The majority of implementation outcomes acquired so far need further improvement since they have not yet attained the highest degree of performance.

- There are works that handle malicious nodes and selfish nodes simultaneously, and making no distinction between them despite their different effects.
- There are no uniform metrics used in the existing game theory approaches for MANET security. Various studies have similar objectives, but they use distinct measures to articulate the outcomes of their experimental investigations, which poses a challenge regarding a fair comparison between the approaches. In addition, there are works that use a limited number of metrics.

2) Future research directions:

- Building game models that contain more than two players, and more than two strategies per player. The diversification in the number of players allows for mimicking all the types of nodes that exist in real networks. In addition, the increase in the number of player strategies leads to players that have dynamic behaviour, and it is directly proportional to the opponent's behaviour.
- Taking into account the form models and information type used in the game.
- Application of new types of game theory besides the types of games mentioned before. Fig. 4 demonstrates some game types that exist in both cooperative and non-cooperative games, among which there are those that have not yet been adopted in the MANET security context.
- Taking into consideration new types of attacks besides the types of attacks mentioned before.
- The incorporation of novel solutions and concepts in addition to those previously referenced.
- Mitigate the weaknesses of existing game theory security approaches for MANETs by combining game theory and Artificial Intelligence (AI) methods. In particular, AI is used to increase the accuracy of detection, and to minimize the detection time. In addition, game theory is used for decision-making against opponents to prevent and mitigate harm in the network.
- Utilization of uniform metrics to allow comparison performance between different approaches.
- Hybridization between different types of game theory.

VI. CONCLUSION

The proliferation of mobile devices has led to the increased significance of MANETs, including the subfamilies of MANETs like VANETs (between ground vehicles), and FANETs (between aerial vehicles).

The domain of research pertaining to MANET security is highly sensitive. As a result, game theory has emerged as a significant approach for addressing security challenges in MANETs in recent times. For this reason, this paper provides an overview of MANET security, with a focus on the fundamental concepts and the various attacks that threaten their security. Additionally, the paper discusses existing security measures and the application of game theory in MANET security.

Furthermore, a taxonomy was introduced for the utilization of game theory in secure MANET solutions, which categorizes them into five distinct classes: the first class pertains to the mitigation of malicious nodes, the second class pertains to the mitigation of selfish nodes, the third class pertains to the hybrid mitigation of both selfish and malicious nodes, the fourth class pertains to intrusion detection, and the fifth and final class pertains to the detection and prevention of attacks.

The initial category comprises two subcategories that are differentiated based on the objectives the researchers seek to attain, with a focus on malicious nodes. These subcategories are malicious behaviour detection, and malicious nodes mitigation with resource preservation.

The second category comprises two subcategories based on cases that identify self-interested nodes. This includes two subclasses, namely: the avoidance of selfish nodes, and the identification and isolation of selfish nodes. The objective of the third class is to mitigate the presence of self-interested and malicious nodes concurrently within MANETs. The fourth class presents some articles on intrusion detection in different cases, and the last class displays the works addressing attack detection in different cases.

Throughout this paper we provided an overview of pertinent details, presenting statistics pertaining to the subsequent subjects: detection classes in MANETs, simulator tools, attack types addressed, game theory elements, game theory forms, game theory models, game theory types, and game theory solution concepts. Furthermore, we compared the classes of our taxonomy based on the previous items. Then, we discussed the principal objectives and techniques used and displayed the advantages and drawbacks of existing works in the literature. Additionally, we examined what types of performance metrics are used in game theory security techniques for MANETs to prove their effectiveness and efficiency.

We extensively discussed the limitations observed from game theory concerning the MANET security techniques surveyed in this work. Based on these limitations, we suggested promising future directions for MANET security research based on game theory.

Finally, we concluded with some points that can improve future work, and that we extracted from a comparison of the studied works.

- *Future perspectives:* Although existing efforts addressed significant challenges related to MANET security, room for improvement remains regarding future perspectives that should be considered to design innovations that address MANET security problems using game theory. One of the future work directions is to implement MANET security by using game theory and new technologies. In addition, we plan to extend the resolution of the security problem by combining game theory with machine learning methods while considering the limited constraints of MANETs (i.e. time and energy parameters).

REFERENCES

[1] W.-K. Jia and C.-M. Yu, "WALS: A lightweight stateless label switching framework based on prime theorem for MANETs," *IEEE Internet Things J.*, early access, May 24, 2023, doi: 10.1109/JIOT.2023.3279370.

[2] F. Safari, H. Kunze, J. Ernst, and D. Gillis, "A novel cross-layer adaptive fuzzy-based ad hoc on-demand distance vector routing protocol for MANETs," *IEEE Access*, vol. 11, pp. 50805–50822, 2023.

[3] S. Lu, J. Lu, K. An, X. Wang, and Q. He, "Edge computing on IoT for machine signal processing and fault diagnosis: A review," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11093–11116, Jul. 2023.

[4] M. B. Taha, S. Alrabaee, and K. R. Choo, "Efficient resource management of micro-services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 6820–6835, Jul. 2023.

[5] A. S. Reddy, "Performance of VANET over MANET in mobile computing environment," in *Proc. 7th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jun. 2022, pp. 659–664.

[6] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, A. R. Najeeb, and M. Yaacob, "A survey on MANETs: Architecture, evolution, applications, security issues and solutions," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 12, no. 2, pp. 832–842, 2018.

[7] S. Singh, A. Pise, O. Alfarraj, A. Tolba, and B. Yoon, "A cryptographic approach to prevent network incursion for enhancement of QoS in sustainable smart city using MANET," *Sustain. Cities Soc.*, vol. 79, Apr. 2022, Art. no. 103483.

[8] P. Theerthagiri, "1 An investigation on cooperative communication techniques in mobile ad-hoc networks," in *Computational Intelligent Security in Wireless Communications*. Oxfordshire, U.K.: Routledge, 2023, p. 1.

[9] S. Vijayalakshmi, S. Bose, G. Logeswari, and T. Anitha, "Hybrid defense mechanism against malicious packet dropping attack for MANET using game theory," *Cyber Secur. Appl.*, vol. 1, Dec. 2023, Art. no. 100011.

[10] T. Hai, J. Zhou, Y. Lu, D. Jawawi, D. Wang, E. M. Onyema, and C. Biamba, "Enhanced security using multiple paths routine scheme in cloud-MANETs," *J. Cloud Comput.*, vol. 12, no. 1, p. 68, Apr. 2023, doi: 10.1186/s13677-023-00443-5.

[11] M. Tahboush and M. Agoyi, "A hybrid wormhole attack detection in mobile ad-hoc network (MANET)," *IEEE Access*, vol. 9, pp. 11872–11883, 2021.

[12] R. Sarumathi and V. Jayalakshmi, "A novel trust value based mobile ad hoc networks (MANETs) security," in *Proc. 7th Int. Conf. Comput. Methodologies Commun. (ICCMC)*, Feb. 2023, pp. 933–939.

[13] S. Pandey and V. Singh, "Blackhole attack detection using machine learning approach on MANET," in *Proc. Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Jul. 2020, pp. 797–802.

[14] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, B. R. Pampori, and R. N. Mir, "MANET security appraisal: Challenges, essentials, attacks, countermeasures & future directions," *Int. J. Recent Technol. Eng.*, vol. 8, no. 6, pp. 3013–3024, Mar. 2020.

[15] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, and A. Shah, "Manifestation and mitigation of node misbehaviour in ad-hoc networks," *Wulfenia J.*, vol. 21, no. 3, pp. 462–470, 2014.

[16] F. Pasandideh, J. P. J. D. Costa, R. Kunst, W. Hardjawana, and E. P. de Freitas, "A systematic literature review of flying ad hoc networks: State-of-the-art, challenges, and perspectives," *J. Field Robot.*, vol. 40, no. 4, pp. 955–979, Jun. 2023.

[17] B. U. I. Khan, R. F. Olanrewaju, and M. H. Habaebi, "Malicious behaviour of node and its significant security techniques in MANET—A," *Austral. J. Basic Appl. Sci.*, vol. 7, no. 12, pp. 286–293, 2013.

[18] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks," *IEEE Access*, vol. 10, pp. 14260–14269, 2022.

[19] M. Prasad, S. Tripathi, and K. Dahal, "An enhanced detection system against routing attacks in mobile ad-hoc network," *Wireless Netw.*, vol. 28, no. 4, pp. 1411–1428, May 2022.

[20] S. Thapar and S. K. Sharma, "Attacks and security issues of mobile ad-hoc networks," in *Proc. Int. Conf. Sustain. Comput. Sci., Technol. Manage. (SUSCOM)*, 2019, pp. 1–20.

[21] R. F. Olanrewaju, B. U. I. Khan, F. Anwar, A. R. Khan, F. A. Shaikh, and M. S. Mir, "MANET—A cogitation of its design and security issues," *Middle-East J. Sci. Res.*, vol. 24, no. 10, pp. 3094–3107, 2016.

[22] P. Kavitha and R. Mukesh, "To detect malicious nodes in the mobile ad-hoc networks using soft computing technique," in *Proc. 2nd Int. Conf. Electron. Commun. Syst. (ICECS)*, Feb. 2015, pp. 1564–1573.

[23] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," *Ad Hoc Netw.*, vol. 133, Aug. 2022, Art. no. 102894.

[24] B. M. Esiefarienrhe, T. Phakathi, and F. Lugayizi, "Node-based QoS-aware security framework for sinkhole attacks in mobile ad-hoc networks," *Telecom*, vol. 3, no. 3, pp. 407–432, Jun. 2022.

[25] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, 1st Quart., 2013.

[26] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs," in *Proc. IEEE Jordan Int. Joint Conf. Electr. Eng. Inf. Technol.*, Apr. 2019, pp. 28–33.

[27] M. Karthigha, L. Latha, and K. Sripriyan, "A comprehensive survey of routing attacks in wireless mobile ad hoc networks," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, Feb. 2020, pp. 396–402.

[28] S. S. Kariyannavar, S. Thakur, and A. Maheshwari, "Security in mobile ADHOC networks: Survey," in *Proc. 6th Int. Conf. Inventive Comput. Technol. (ICICT)*, Jan. 2021, pp. 135–143.

[29] E. G. Mwangi, G. M. Muketha, and G. K. Ndungu, "A review of security techniques against black hole attacks in mobile ad hoc networks," in *Proc. IST-Africa Week Conf. (IST-Africa)*, May 2019, pp. 1–8.

[30] M. Vanday Baseri and H. Fatemidokht, "Survey of different techniques for detecting selfish nodes in MANETs," *J. Mahani Math. Res. Center*, vol. 11, no. 2, pp. 45–59, 2022.

[31] S. Kumar, M. Goyal, D. Goyal, and R. C. Poonia, "Routing protocols and security issues in MANET," in *Proc. Int. Conf. INFOCOM Technol. Unmanned Syst.*, Dec. 2017, pp. 818–824.

[32] G. Liu, Z. Yan, and W. Pedrycz, "Data collection for attack detection and security measurement in mobile ad hoc networks: A survey," *J. Netw. Comput. Appl.*, vol. 105, pp. 105–122, Mar. 2018.

[33] R. R. Chandan and P. K. Mishra, "A review of security challenges in ad-hoc network," *Int. J. Appl. Eng. Res.*, vol. 13, no. 22, pp. 16117–16126, 2018.

[34] O. H. Younis, S. E. Essa, and E. S. Ayman, "A survey on security attacks/defenses in mobile ad-hoc networks," *Commun. Appl. Electron.*, vol. 6, no. 10, pp. 1–9, Apr. 2017.

[35] G. Keerthana and P. Anandan, "A survey on security issues and challenges in mobile ad-hoc network," *EAI Endorsed Trans. Energy Web*, vol. 5, no. 20, Sep. 2018, Art. no. 155743.

[36] W. Bouassaba, A. Nabou, and M. Ouzzif, "Review on machine learning based intrusion detection for MANET security," in *Proc. 9th Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Oct. 2022, pp. 1–6.

[37] D. G. Kampitaki and A. A. Economides, "Selfishness in mobile ad-hoc networks: A literature review on detection techniques and prevention mechanisms," *IEEE Access*, vol. 11, pp. 86895–86909, 2023.

[38] H. Shah, V. Kakkad, R. Patel, and N. Doshi, "A survey on game theoretic approaches for privacy preservation in data mining and network security," *Proc. Comput. Sci.*, vol. 155, pp. 686–691, Jan. 2019.

[39] P. Dasgupta and J. B. Collins, "A survey of game theoretic approaches for adversarial machine learning in cybersecurity tasks," *AI Mag.*, vol. 40, no. 2, pp. 31–43, Jun. 2019.

[40] K. Merrick, M. Hardhienata, K. Shafi, and J. Hu, "A survey of game theoretic approaches to modelling decision-making in information warfare scenarios," *Future Internet*, vol. 8, no. 3, p. 34, Jul. 2016.

[41] Y. Wang, Y. Wang, J. Liu, Z. Huang, and P. Xie, "A survey of game theoretic methods for cyber security," in *Proc. IEEE 1st Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2016, pp. 631–636.

[42] C. Kiennert, Z. Ismail, H. Debar, and J. Leneutre, "A survey on game-theoretic approaches for intrusion detection and response optimization," *ACM Comput. Surv.*, vol. 51, no. 5, pp. 1–31, Sep. 2019.

[43] F. Anwar, B. U. I. Khan, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A comprehensive insight into game theory in relevance to cyber security," *Indonesian J. Electr. Eng. Informat.*, vol. 8, no. 1, pp. 189–203, Mar. 2020.

[44] A. E. Chukwudi, E. Udoka, and I. Charles, "Game theory basics and its application in cyber security," *Adv. Wireless Commun. Netw.*, vol. 3, no. 4, pp. 45–49, 2017.

[45] V. Kakkad, H. Shah, R. Patel, and N. Doshi, "A comparative study of applications of game theory in cyber security and cloud computing," *Proc. Comput. Sci.*, vol. 155, pp. 680–685, Jan. 2019.

[46] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S. S. Iyengar, "Game theory for cyber security and privacy," *ACM Comput. Surv.*, vol. 50, no. 2, pp. 1–37, 2017.

[47] M. Zhu, A. H. Anwar, Z. Wan, J.-H. Cho, C. A. Kamhoua, and M. P. Singh, "A survey of defensive deception: Approaches using game theory and machine learning," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2460–2493, 4th Quart., 2021.

[48] A. Sinha, "AI and security: A game perspective," in *Proc. 14th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2022, pp. 393–396.

[49] R. Krishnan, "A survey on game theory approaches for improving security in MANET," *Amer. J. Electr. Comput. Eng.*, vol. 2, no. 1, pp. 1–4, 2018.

[50] B. Paramasivan, M. J. V. Prakash, and M. Kaliappan, "Development of a secure routing protocol using game theory model in mobile ad hoc networks," *J. Commun. Netw.*, vol. 17, no. 1, pp. 75–83, Feb. 2015.

[51] Y. Taheri, H. G. Garakani, and N. Mohammadzadeh, "A game theory approach for malicious node detection in MANETs," *J. Inf. Sci. Eng.*, vol. 32, no. 3, pp. 559–573, 2016.

[52] S. Balaji, E. G. Julie, Y. H. Robinson, R. Kumar, P. H. Thong, and L. H. Son, "Design of a security-aware routing scheme in mobile adhoc network using repeated game model," *Comput. Standards Interface*, vol. 66, Oct. 2019, Art. no. 103358.

[53] B. U. I. Khan, R. F. Olanrewaju, M. Mattoo, A. A. Aziz, and S. A. Lone, "Modeling malicious multi-attacker node collusion in MANETs via game theory," *Middle-East J. Sci. Res.*, vol. 25, no. 3, pp. 568–579, 2017.

[54] M. Bouhaddi, K. Adi, and M. S. Radjef, "Evolutionary game-based defense mechanism in the MANETs," in *Proc. 9th Int. Conf. Secur. Inf. Netw.*, Jul. 2016, pp. 88–95.

[55] M. Sukanya, N. Karthikeyan, and S. Karthik, "The enhanced security scheme for network protection against attacks using improved mean field game theory (IMFGT) in MANET," *Int. J. Printing, Packag. Allied Sci.*, vol. 4, no. 5, pp. 3535–3540, Dec. 2016.

[56] T. Lei, S. Wang, J. Li, I. You, and F. Yang, "Detecting and preventing selfish behaviour in mobile ad hoc network," *J. Supercomput.*, vol. 72, no. 8, pp. 3156–3168, Aug. 2016.

[57] M. T. Singh and S. Borkotokey, "Selfish avoidance payoff allocation in mobile ad hoc network," in *Proc. Int. Conf. Recent Innov. Electr., Electron. Commun. Eng. (ICRIEECE)*, Jul. 2018, pp. 2715–2721.

[58] A. Sharah, M. Alhaj, and M. Hassan, "Selfish dynamic punishment scheme: Misbehavior detection in MANETs using cooperative repeated game," *Int. J. Comput. Sci. Netw. Secur.*, vol. 20, no. 3, pp. 168–173, 2020.

[59] M. T. Singh and S. Borkotokey, "A stable payoff allocation protocol for controlling the selfishness and managing the power consumption in mobile ad hoc networks," *J. Sci. Res.*, vol. 66, no. 2, pp. 52–60, 2022.

[60] A. Sahnoun, A. Habbani, and J. E. Abbadi, "A coalition-formation game model for energy-efficient routing in mobile ad-hoc network," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 1, pp. 26–33, 2018.

[61] G. Narayanan, J. K. Das, M. Rajeswari, and R. S. Kumar, "Game theoretical approach with audit based misbehavior detection system," in *Proc. 2nd Int. Conf. Inventive Commun. Comput. Technol. (ICICCT)*, Apr. 2018, pp. 1932–1935.

[62] S. Mubeen, "Isolating selfish nodes and analyzing performance of adhoc network using perfect information game theory," *Int. J. Knowl. Based Comput. Syst.*, vol. 6, no. 2, pp. 31–37, Dec. 2018.

[63] A. Vij, V. Sharma, and P. Nand, "Selfish node detection using game theory in MANET," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Oct. 2018, pp. 104–109.

[64] H. Amraoui, A. Habbani, A. Hajami, and E. Bilal, "Security-based mechanism for proactive routing schema using game theory model," *Mobile Inf. Syst.*, vol. 2016, pp. 1–17, Jan. 2016.

[65] A. Roles and H. E. Aarag, "Coexistence with malicious and selfish nodes in wireless ad hoc networks: A Bayesian game approach," *J. Algorithms Comput. Technol.*, vol. 11, no. 4, pp. 353–365, Dec. 2017.

[66] D. Das, K. Majumder, and A. Dasgupta, "A game-theory based secure routing mechanism in mobile ad hoc network," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, Apr. 2016, pp. 437–442.

[67] R. F. Olanrewaju, F. Anwar, R. N. Mir, M. Yaacob, and T. Mehraj, "Bayesian signaling game based efficient security model for MANETs," in *Proc. Future Inf. Commun. Conf.*, vol. 2. Cham, Switzerland: Springer, 2020, pp. 1106–1122.

[68] C. Vijayakumaran and T. A. Macriga, "An integrated game theoretical approach to detect misbehaving nodes in MANETs," in *Proc. 2nd Int. Conf. Comput. Commun. Technol. (ICCCT)*, Feb. 2017, pp. 173–180.

[69] R. F. Olanrewaju, A. L. Mechraoui, and B. U. I. Khan, "Game theory probabilistic application to detect misbehaving nodes in ad-hoc networks," in *Proc. 2nd IEEE Int. Conf. Intell. Syst. Eng. (ICISE)*, Kuala Lumpur, Malaysia, 2018, pp. 20–21.

[70] T. Poongothai, K. Jayarajan, and P. S. K. Patra, "Enhancing security in mobile ad hoc networks using non cooperative Bayesian game approach," in *Proc. AIP Conf.*, 2022, p. 020199-020205.

[71] S. Abbas, M. Merabti, K. Kifayat, and T. Baker, "Thwarting Sybil attackers in reputation-based scheme in mobile ad-hoc networks," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 12, pp. 6214–6242, 2019.

[72] L. Y. Njilla, P. Echual, N. Pissinou, and K. Makki, "A game-theoretic approach on resource allocation with colluding nodes in MANETs," in *Proc. Annu. IEEE Syst. Conf.*, Apr. 2016, pp. 1–8.

[73] M. Bouhaddi, M. S. Radjef, and K. Adi, "An efficient intrusion detection in resource-constrained mobile ad-hoc networks," *Comput. Secur.*, vol. 76, pp. 156–177, Jul. 2018.

[74] V. Sangeetha, M. Vaneeta, S. S. Kumar, P. K. Pareek, and S. Dixit, "Efficient intrusion detection of malicious node using Bayesian hybrid detection in MANET," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1022, no. 1, 2021, Art. no. 012077.

[75] S. Sampath and A. Edwin Robert, "Bayesian correlated equilibrium based IDS for MANET," *Indian J. Sci. Technol.*, vol. 9, no. 41, p. 41, Nov. 2016.

[76] B. Subba, S. Biswas, and S. Karmakar, "Intrusion detection in mobile adhoc networks: Bayesian game formulation," *Eng. Sci. Technol., Int. J.*, vol. 19, no. 2, pp. 782–799, Jun. 2016.

[77] B. Kokode, M. Pande, and S. V. Warjurkar, "Intrusion detection in mobile ad-hoc networks using Bayesian game methodology," *Int. J. Future Revolution Comput. Sci. Commun. Eng.*, vol. 3, no. 9, pp. 194–203, 2017.

[78] F. Hamza and S. M. C. Vigila, "Review of machine learning-based intrusion detection techniques for MANETs," in *Computing and Network Sustainability*. Cham, Switzerland: Springer, 2019, pp. 367–374.

[79] K. Chopra, "Mobile ad hoc network security using mean field game theoretic threshold-based scheme," *Recent Adv. Comput. Sci. Commun.*, vol. 15, no. 3, pp. 388–396, Mar. 2022.

[80] P. Pandey and A. Barve, "An energy-efficient intrusion detection system for MANET," in *Data, Engineering and Applications*, vol. 2. Singapore: Springer, 2019, pp. 103–117.

[81] Y. Guo, H. Zhang, L. Zhang, L. Fang, and F. Li, "A game theoretic approach to cooperative intrusion detection," *J. Comput. Sci.*, vol. 30, pp. 118–126, Jan. 2019.

[82] M.-A. E. Houssaini, A. Aaroud, A. E. Hore, and J. Ben-Othman, "A game theoretic approach against the greedy behavior in MAC IEEE 802.11," in *Proc. Int. Symp. Ubiquitous Netw.* Cham, Switzerland: Springer, 2017, pp. 38–47.

[83] A. Al Sharah, T. Oyedare, and S. Shetty, "Detecting and mitigating smart insider jamming attacks in MANETs using reputation-based coalition game," *J. Comput. Netw. Commun.*, vol. 2016, pp. 1–13, Jan. 2016.

[84] K. Geetha and N. Sreenath, "Detection of SYN flooding attack in mobile ad hoc networks with AODV protocol," *Arabian J. Sci. Eng.*, vol. 41, no. 3, pp. 1161–1172, Mar. 2016.

[85] E. Guţuleac, I. Gîrleanu, A. Furtună, and I. Iavorschi, "Uncertainty analysis of attacker-defender interactions in MANET based on game GSPN with intuitionistic fuzzy parameters," in *Proc. Int. Conf. Inf. Technol., Syst. Netw.*, Chişinău, Republic of Moldova, Oct. 2017, pp. 265–277.

[86] X. Gao and Z. Chen, "Risk assessment of ad hoc based on game theory," in *Proc. Int. Conf. Appl. Techn. Cyber Intell.* Cham, Switzerland: Springer, 2020, pp. 256–264.

[87] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, M. L. B. M. Kiah, and R. N. Mir, "Game theory analysis and modeling of sophisticated multi-collusion attack in MANETs," *IEEE Access*, vol. 9, pp. 61778–61792, 2021.

[88] A. Gaye and K. Konate, "The Nash's balance in the theory of games for A secure model mechanism in routing protocol of MANET," *Int. J. Cryptogr. Inf. Secur.*, vol. 9, nos. 1–2, pp. 1–12, 2019.

[89] D. Zheng and S. Hu, "Quality of service (QoS) and security provisioning in cooperative mobile ad hoc networks (MANETs)," 2016, *arXiv:1610.00071*.

[90] T. Oyedare, A. A. Sharah, and S. Shetty, "A reputation-based coalition game to prevent smart insider jamming attacks in MANETs," in *Proc. Int. Conf. Wired/Wireless Internet Commun.* Cham, Switzerland: Springer, 2016, pp. 241–253.

[91] Y. Ma, K. Liu, and X. Luo, "Game theory based multi-agent cooperative anti-jamming for mobile ad hoc networks," in *Proc. IEEE 8th Int. Conf. Comput. Commun. (ICCC)*, Oct. 2022, pp. 901–905.

[92] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A game theory-based strategic approach to ensure reliable data transmission with optimized network operations in futuristic mobile adhoc networks," *IEEE Access*, vol. 8, pp. 124097–124109, 2020.

HADJER MESSABIH received the M.Sc. degree in computer science from the University of Batna, Algeria, in 2015. She is currently pursuing the Ph.D. degree with Laboratoire d'Informatique et de Mathématiques (LIM), University of Laghouat. Her research interests include security, MANETS, and game theory.

CHAKER ABDELAZIZ KERRACHE received the M.Sc. and Ph.D. degrees in computer science from the University of Laghouat, Algeria, in 2012 and 2017, respectively. He is currently an Associate Professor with the Department of Computer Science and the Head of Informatics and Mathematics Laboratory (LIM), University of Laghouat. His research interests include trust and risk management, secure multi-hop communications, vehicular networks, named data networking (NDN), and UAVs.

YOUSSRA CHERIGUENE received the M.Sc. degree in computer science from the University of Laghouat, Algeria, in 2020, where she is currently pursuing the Ph.D. degree with the Informatics and Mathematics Laboratory (LIM). Her research interests include mobile edge computing, unmanned aerial vehicles, and federated learning.

CARLOS T. CALAFATE (Senior Member, IEEE) received the Graduate degree (Hons.) in electrical and computer engineering from the University of Oporto, Portugal, in 2001, and the Ph.D. degree (cum laude) in informatics from the Technical University of Valencia (UPV), Spain, in 2006. Since 2002, he has been with UPV, where he is currently a Full Professor with the Department of Computer Engineering. His research interests include ad-hoc and vehicular networks, UAVs, smart cities and the IoT, QoS, network protocols, video streaming, and network security. He is ranked among the World's Top 2% Scientists, and also among the top 100 Spanish Researchers in the computer science and electronics field.

FATIMA ZOHRA BOUSBAA received the M.Sc. and Ph.D. degrees in computer science (information system engineering specialization) from the University of Laghouat, Algeria, in 2011 and 2020, respectively, where she is currently pursuing the Ph.D. degree with the Doctorate School. Her current research interests include the use of heuristic methods to solve geocast/multicast routing problems, game theory, and UAVs.