IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 July 2023, accepted 10 August 2023, date of publication 14 August 2023, date of current version 18 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3305262

SURVEY

Selfishness in Mobile Ad-Hoc Networks: A Literature Review on Detection Techniques and Prevention Mechanisms

DIMITRA G. KAMPITAKI, (Member, IEEE), AND ANASTASIOS A. ECONOMIDES, (Senior Member, IEEE)
Information Systems IPPS, University of Macedonia, GR-546 36 Thessaloniki, Greece
Corresponding author: Dimitra G. Kampitaki (dkampitaki@uom.edu.gr)

The publication of the article was financially supported by HEAL-Link.

ABSTRACT Constant connectivity is one of the most challenging requirements modern communication networks promise to satisfy. 5G and Beyond applications and the proliferation of Internet of Things (IoT) applications make mobile networks one of the most discussed research topics of the present, while research is already moving towards the design specifications and development of 6G services and solutions. Using multi-hop patterns, mobile nodes can move around always maintaining their connectivity in a pervasive and ubiquitous manner. New possibilities emerge from this progress, whereas long known challenges still exist and evolve. One of them is the selfishness or unwillingness of some nodes to spend resources to serve the communication requests of other nodes, not in a malicious but rather in a self-conservative manner. While intentional misbehavior of nodes is considered a security issue, selfishness is studied separately in the relevant literature and has attracted a lot of research attention. In this review we attempt to present the leading research on the detection techniques and the preventive mechanisms employed by previous studies to address the selfishness problem in mobile ad hoc networks, and to identify the trends during the past few years, focusing primarily on the routing layer. We follow a systematic methodology to identify, select, categorize, and analyze the relevant research and we use a concept-centric approach to present the results forming a comprehensive starting point for future research.

INDEX TERMS Mobile ad hoc networks, routing protocols, next generation networking, mobile communication, 5G and beyond communications, 6G communications.

I. INTRODUCTION

Initially, Ad hoc Networks were deployed to address emergency situations occurring in areas or during times where conventional connectivity was limited or unavailable. The primary objective was to identify swift-to-implement and reliable communication media to facilitate effective communication under such circumstances. Under this scope, Ad hoc Networks [1] were employed. The nodes of an Ad hoc Network formed temporary connections among themselves so they could utilize the wireless medium in an ad hoc manner providing connectivity and services, whenever and wherever they were needed, and terminate communication afterwards. They were further improved to be able to communicate even if some or even all nodes were mobile, forming Mobile Ad hoc Networks (MANETs).

The routing protocols employed in the deployment and functioning of wired networks rely on pre-established routing tables, which are created in advance and persistently maintained throughout the network's lifespan. However, these routing protocols are not efficient or effective in maintaining end-to-end connectivity and providing network services in a fast-changing environment, so new routing protocols were developed to serve the specific needs of MANETs. A simple taxonomy of these routing protocols categorized them as proactive, e.g., Optimized Link State Routing (OLSR) [2],

The associate editor coordinating the review of this manuscript and approving it for publication was Vladimir Poulkov.

and reactive, e.g., Dynamic Source Routing (DSR) [3], while in some implementations, concepts from both categories were used, forming hybrid solutions, e.g., Zone Routing Protocol (ZRP) [4]. In proactive routing protocols, each node forms and maintains a routing table with the routes to every other known node in the network, while in reactive routing protocols the route to a node is created only when it is required. A comprehensive review of routing protocols for MANETs can be found in [5].

As new technologies were introduced and implemented, advanced routing solutions were proposed. Routing protocols evolved trying to overcome specific MANETs challenges, forming a set of sub-fields. There have been approaches that focus on energy efficiency [6], mobility models [7], [8], security issues [9], various Quality of Service (QoS) parameters [10], etc. The literature around the field is vast, and numerous literature reviews and surveys have been published focusing on and analyzing one or more of these aspects, for example [11] surveys energy efficient routing protocols for MANETs. A considerable number of research articles investigates performance evaluations of different MANET routing protocols, under various assumptions and settings. For example, in [12], the performance of various routing protocols is examined when File Transfer Protocol (FTP) traffic exists in the network, and in [13] the routing protocols are compared when the MANET is used for video streaming.

In this study, we focus on the selfishness problem, the definition of which we will specifically examine onwards. Then, we present the various approaches to address the selfishness problem, briefly explaining each one approach and we focus on the most recent and important contributions in the field to identify promising directions and to set a starting point for future research. We aim to address the following research questions, concerning the network layer of MANETs:

RQ1: How is selfishness in MANETs defined in the literature, specifically on the network layer?

RQ2: What are the detection techniques and the solutions proposed to address the selfishness problem in MANETs, specifically on the routing layer?

RQ3: Is there a research field shift during the recent years and towards which direction?

The rest of the study is structured as follows: First, we present the research methodology we used, and then we give the definitions that will help the reader go through the rest of the study having a basic understanding of the field. We examine the different scopes under which selfishness has been defined in the literature and we categorize the aspects of selfishness considered by researchers, thus answering RQ1. Next, we introduce a new taxonomy of the research approaches to the selfishness problem along with a concise presentation of them, thus answering RQ2. Through this process, we identify new concepts that have been introduced and have been applied to the field, thus answering RQ3. The study is concluded with a critical summary of the research on this field and potential directions for future research.

II. MOTIVATION AND CONTRIBUTION

Research on routing protocols and selfishness has been extensive and there are numerous research articles on the field. One of the most popular studies [14] provides a comprehensive overview of research on selfishness up to 2006. After that, there have been some interesting studies, however most of them do not analyze new concepts, but stick to revisiting the ones presented in [14].

Some of the recent literature reviews, e.g., [15], [16], are mostly focused on the early proposed methods, and fail to collect, categorize, and analyze new research. Additionally, they do not employ a systematic way to collect, select and analyze the literature, thus failing to capture the whole research field. This review comes to cover this gap using a comprehensive and systematic methodology for collecting, selecting, and analyzing the literature. Furthermore, many of the existing reviews and surveys, e.g., [17], [18] just provide a list of relevant research and briefly discuss the topic of each article in a paragraph at a time. Although this type of reviews and surveys is easier to conduct, their usefulness is limited. We refrain from that type of review, as we aim at concept-centric and not article-centric analysis. We do not analyze explicitly the methods proposed by each one article, instead we examine the field, we identify the main concepts behind each group of proposed methods, and we discuss them focusing on their features and challenges.

Finally, previous research [15], [16], [17], [18] groups the detection and prevention methods employed to address the selfishness problem, using the characterization given by their authors either as reputation-based, credit-based, etc. We attempt a different taxonomy, based on the concept these methods employ, which we will present at the respective section of this paper. For each proposed method, we record the concepts utilized using the proposed taxonomy.

The main contributions of this review are as follows:

- It provides a categorical approach to the definition of selfishness, facilitating the understanding of the concept.
- It introduces a modular taxonomy accompanied with a comprehensive collection and summary of the research approaches on the prevention, detection, evaluation, and reaction methods of selfishness in MANETs.
- It examines the state-of-the-art research in the field and gives research directions by identifying the research trends.

However, this review does not provide detailed analysis of each method and research paper considered, as this would result in a lengthy article with no added information provided. The reader is encouraged to refer to the original papers cited in this work to acquire detailed descriptions and operation explanation of each method.

III. REVIEW METHODOLOGY

The methodology used to conduct this review is based on the one proposed by Webster and Watson in [19], combined with some of the guidelines provided by the PRISMA

TABLE 1. Inclusion and exclusion criteria.

Inclusion	Exclusion
Studies on mobile ad hoc networks	Studies on other types of networks.
Studies that consider the network layer	Studies that do not consider the network layer (e.g., they study selfishness in the application layer)
Studies that consider selfish nodes and/or other nodes	Studies that consider only malicious nodes (e.g., security-oriented)
Original research papers	Technical reports, review, or survey papers
Studies written in English	Studies written in other languages
Studies included in major scientific databases	Non-published studies that were found online

statement [20] and some guidelines given by Kitchenham in [21]. As suggested in [19], to form a comprehensive literature review we focus on concepts and use an appropriate organizing framework to synthesize and present the literature. We define the concept outline for selfishness, and we adopt a systematic search among the published work. Focusing on the concepts we attempt to present a review of the relevant literature, using the provided checklists and flow diagrams given in [20]. Using the research questions proposed in [21], we guide the process and assess our results.

An important limitation of this work is the inability to retrieve some articles that seem relevant to our topic because they are unavailable online, and despite our efforts it was not possible to retrieve them. These articles were either older publications or published in non-indexed and low-quality publications. However, these articles are a minority, and do not alter the results of this study. Usually, high impact and quality publications tend to be under an open-access policy or by reputable publishers or available through university subscriptions, therefore they are easy to access.

A. SEARCH STRATEGY

To collect the relevant literature, we performed a thorough search among the most popular scientific literature databases, using appropriate keywords. The search was conducted on the databases of IEEE Xplore, Scopus, and Google Scholar, using the keywords MANET, selfish, selfishness, selfish node, detection, routing, and various combinations of them. The results spanned from the year 2000 up until the end of 2022 and included a diverse collection of journal articles and conference publications. We examined the references of these items to ensure that all the important articles were included in the results. After elimination of the duplicates, a collection of 233 articles was gathered.

B. STUDY SELECTION AND ASSESSMENT CRITERIA

We went through each article and noted the title, keywords, abstract and publication discipline, deciding whether to include or exclude it, using the inclusion and exclusion criteria mentioned in Table 1.

First, we read the title and through the abstract of each paper and identified the main topic of each article. We included studies concerning routing in MANETs with selfish nodes and we excluded articles that examine methods applied to other types of networks (e.g., infrastructure-based networks), studied selfishness in other layers than the routing layer or approached networks under a security perspective, that aimed to identify malicious nodes and suppress attacks. Articles that examined the security perspective were the harder to distinguish as selfishness has been addressed to as a security issue by many researchers. However, since selfish behavior is not intentional and selfish nodes do not actively try to harm the network performance, we believe that selfishness has to be examined separately. When the article's main theme was about authentication schemes, public and private keys or specifically considered ''attacks'', ''intruders'', ''anomaly detection'', or ''intrusion detection'', we excluded it as security oriented. Additionally, this study contains only original work articles, whereas technical reports, surveys and review papers were excluded. Finally, some works that were presented first in a conference were excluded if there was a follow-up publication with more complete results by the same authors. Apart from these criteria, we had to exclude some items of low quality, not innovative or irrelevant to the field, or written in other languages than English. Concluding this procedure, the final list consists of 38 articles.

C. DATA EXTRACTION AND SYNTHESIS

As our motivation is to examine the field concept-wise and also to identify the trends of the research in the field, we examined the research articles in a chronological order. The early research articles were examined to extract and identify the main concepts and early methods and the more recent research articles to focus on the recent developments in the field. Having followed the evolution of this field for a long time, we believe that the novel solutions which have been proposed due to the newly employed technologies, have formed a shift of the research field towards another direction in comparison to the earlier proposed methods. Therefore, we went through these items to identify the most prominent research articles and the concepts in them and then we grouped conceptually related approaches. Using concept matrices, we analyzed, coded, and synthesized the literature. In the next section, we present the results of this procedure.

Since the literature is so extensive, we had to form a framework under which the literature would be compiled. Figure 1 illustrates the compiled data for each of the acquired items.

1) PUBLICATION CHARACTERISTICS

We collected data about the year and the type of the publication of each article. Thus, we were able to record when each method was proposed and compare the utilization of each method through time. The recording of the type of publication is additional information, as methods are usually first introduced in conferences and later, they are thoroughly

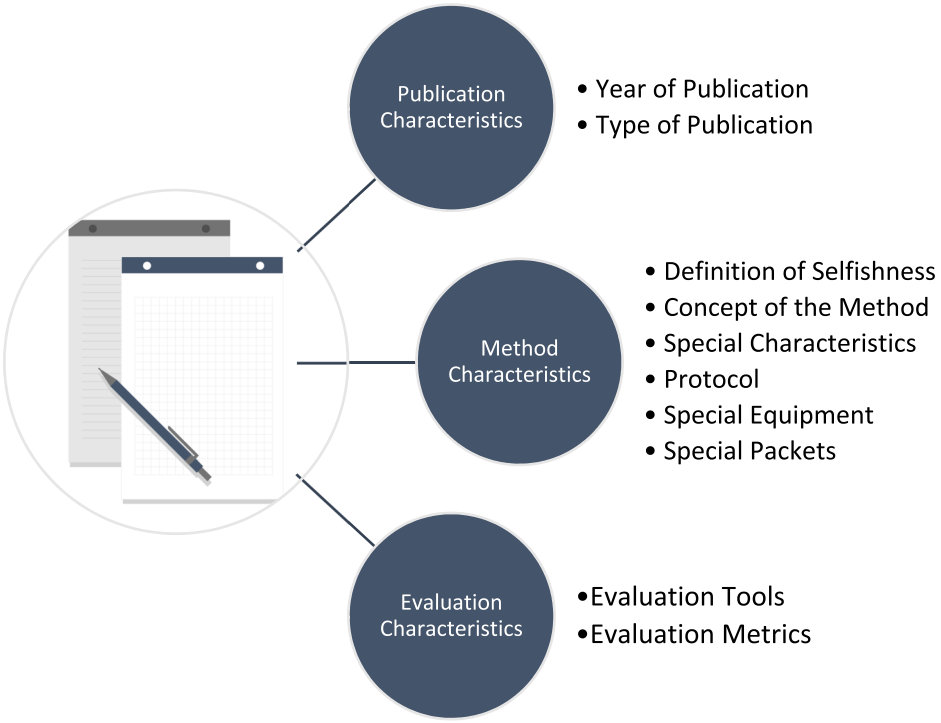

FIGURE 1. Publication features compiled from each item retrieved during the search.

explained and presented in journal publications. Using this data, we were able to outline the evolution of the research of the field through time.

2) METHOD CHARACTERISTICS

The collection and presentation of the method characteristics comprises the main objective of this review. We collected specific information of each proposed method, and we grouped them conceptually. We recorded the definition of selfishness that each proposed method uses, the special characteristics of the proposed methods in terms of detection and prevention of selfishness, the routing protocol that was modified, if so, and the need for special packets or equipment, if any.

3) EVALUATION CHARACTERISTICS

Data about the characteristics of the evaluation of the methods was also collected. We recorded the tools and the metrics that were used to evaluate the performance of each proposed method. Most of the proposed methods use common metrics for network performance evaluation, while the tools are in most cases open-source network simulators.

IV. DEFINITIONS

In this section, we present a summary of the basic definitions, and we discuss the definition of selfishness in the context of wireless networks throughout literature. Thus, we specifically define our field of study and the scope of this review, whereas addressing the RQ1.

A. BASIC DEFINITIONS

An ad-hoc network is a network that is formed without the need for any pre-existing infrastructure. The nodes, besides using the network that is formed by their peers, function as routers to find data delivery paths and as relay nodes to forward data to other nodes. They use the wireless medium and utilize routing protocols to route data between themselves. When the nodes of the ad hoc network are mobile, the network is called a Mobile Ad hoc Network (MANET).

Subcategories of MANETs are considered by defining specific characteristics, for example, a MANET that is formed by vehicles is a Vehicular Ad hoc Network (VANET) [22]. A network that consists of Flying nodes is a Flying Ad hoc Network (FANET) [23]. In case the time frame for the delivery of the packets is unrestricted and the packets are stored by the nodes and are delivered when the nodes have the opportunity, which is commonly addressed in VANETs and FANETs, the network is called Delay Tolerant Network (DTN) [24], a subcategory of which is Opportunistic Network (OppNet) [25]. A network that consists of devices whose mere purpose is to monitor one or more specific parameters (usually environmental) is called a Wireless Sensor Network (WSN) [26]. This type of network evolved partially to Internet of Things (IoT), which is also a particularly important variation of networks that already has a wide range of applications and is expected to be even more used in 6G networks [27]. All these networks are extensions of MANETs and the features and challenges of MANETs operation apply to all of them, whereas each of these networks has its own

additional features and challenges. For example, VANETs are expected to follow specific routes and FANETs have a 3-dimensional area of movement.

Each device that can connect to the network is called a *node*. The nodes in an ad-hoc network communicate in a multi-hop manner, and the routing protocols that are designed specifically for MANETs consider nodes as fully cooperative. A mobile node usually is of small size and therefore has low processing capabilities, low energy capacity, specific and low transmission range, and in many cases low bandwidth is available to them.

A node that needs to send data to another node is the *source node* and the receiver node is the *destination node*. The intermediate nodes between them that are used to forward the packets in a multi-hop pattern are called *relay nodes*. When two nodes reside in each other's transmission range they are called neighbors. All nodes that reside inside the transmission range of a node are called its neighborhood.

A *normal node* is a node that is fully cooperative, forwards every packet it receives, and provides truthful information to the routing protocol and other nodes. A *selfish node* is a node without malicious intent. That means it does not aim to harm the network, instead, its actions (or the absence of them) are taken to serve its own communication needs without sacrificing its resources to serve the needs of other nodes that belong to the network.

A *malicious node* is a node that aims to harm the network performance and it deliberately acts towards that aim. The motive of these actions is not to benefit itself but to harm the network even if that means it will also harm itself in the process. The actions of a malicious node are considered security attacks and are out of the scope of this work. However, since some of the approaches that we examine, either do not distinguish the difference between malicious and selfish nodes or they examine both behaviors in their study, we refer to some of them, too.

MANET routing protocols use several types of control packets for routing purposes. The most commonly used are:

- HELLO – it is transmitted periodically to notify the neighbors of a node of its presence. It can contain various information that has to be known to the neighbors of the node.
- Route Request (RREQ) – It is broadcasted by a source node that needs to reach a destination node and it searches for a path towards it.
- Route Reply (RREP) – It is sent back to the source node when a route to the destination node is found.
- Route Error (RERR) – It is broadcasted when an error occurs through an established route.

These control packets can be modified accordingly to serve the needs of newly designed routing protocols, whereas other routing protocols introduce arbitrarily designed control packets to serve their needs and carry extra information that facilitates their operation.

B. SELFISHNESS DEFINITION

Selfishness has been studied extensively since routing misbehavior was observed in networks. Researchers have attempted to model selfish nodes under different scopes, with similarities and differences between their definitions. In this section, we summarize definitions of selfishness as presented by various researchers and we categorize the way selfishness is defined, thus replying to the RQ1.

As Marti et al. [28] pointed out, misbehaving nodes are nodes that agree at first to forward packets for other nodes, but at the end fail to accomplish that, for various reasons, such as overloading, selfishness, maliciousness, or operation failure. Michiardi and Molva [29] defined two types of selfish behavior that defer in whether the nodes participate or do not participate in routing procedures of the routing protocol; but in both cases they do not forward data packets for other nodes. They also define a third type that falls back into one of the two categories depending on its residual energy.

Selfishness is a deliberate action but not with malicious intent, while overloading and operation failure are unintentional actions. The result, however, of all these types of misbehavior is the degradation of network performance. Security-oriented solutions aim to detect and eliminate malicious attacks, congestion control and fairness algorithms target to solve overloading issues, and operation failure can be minimized during the processes of design and implementation of the devices. Research about selfishness aims to distinguish selfishness from the other types of misbehavior and propose solutions to minimize its impact on network performance.

Selfishness can be defined depending on the way the selfish node expresses it. In Fig. 2, a summary of the diverse ways selfishness is considered in MANETs is depicted. Various combinations of these features have been considered until now, extending or limiting the definitions of Marti et al. [28] or Michiardi and Molva [29].

Selfishness can occur due to many reasons, with a variety of effects on network performance. However, in most cases nodes do not become arbitrarily selfish, instead, there must exist specific conditions under which the selfish behavior is observed. In some studies selfishness, once expressed, became a permanent behavior for the node, while in other studies the nodes stopped being selfish after the conditions that triggered selfishness were eliminated, for example, if the node recovered some energy. Most methods though, consider selfishness as a permanent behavior of the nodes and once the node has been labeled as selfish, they exclude it permanently from all network operations and isolate it by not allowing it to send its packets through the other nodes of the network.

Although all nodes can become selfish, in most cases selfish behavior is observed in only some of the nodes comprising the network. If all nodes are selfish, then there can be no multi-hop operation of the network and only direct communication is possible. However, even when a small number of

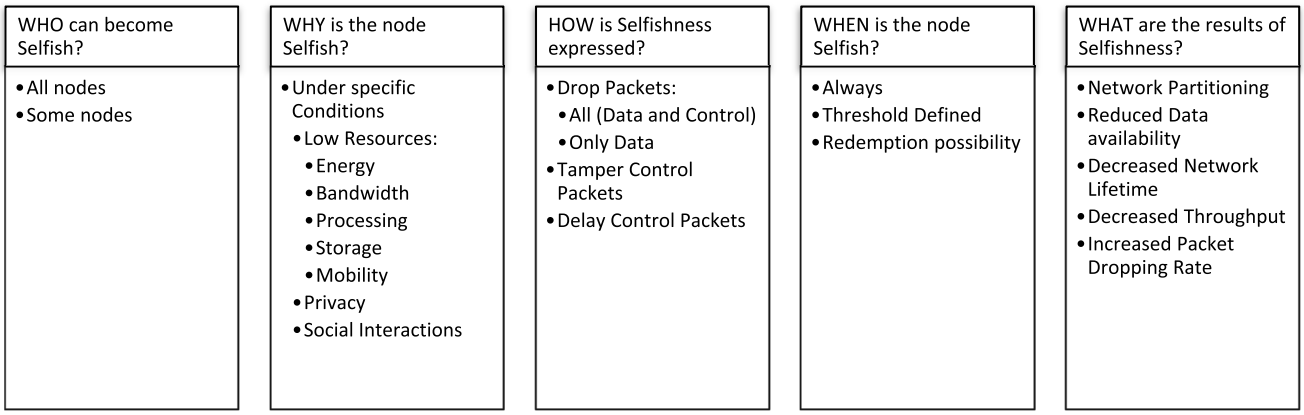

FIGURE 2. Aspects of selfishness definition.

the nodes is selfish, the network can become partitioned, and its performance can be greatly affected.

Depending on the routing protocol employed, selfish nodes can be characterized as such according to the routing protocol operations they participate in. For example, when DSR is employed, a type of selfish nodes participates in the route discovery and route maintenance processes but abstain from the data forwarding process when they are selected into a routing path. This could happen always, or under some conditions. In [30] the behavior where a node replies to route requests but then drops the packets routed through it, is referred to as *misleading*.

There is also the case where a node modifies its behavior depending on the source or the destination node of the received packet. For example, a node that receives a packet from a node that has a specific role in the network, e.g., cluster head or administration node will always forward it, or when it receives a packet for a node that is flagged as selfish or malicious, it will always drop it.

The results of selfishness can vary from slight degradation in network performance and reduced data availability and throughput, to decreased network lifetime and eventually to the total collapse of the network. The proposed approaches try to alleviate these results, and some approaches manage to accomplish their purpose quite successfully, keeping selfish behavior of the nodes under control or even in some cases use it to benefit the network operation. In the next section, we examine the different methods that have been proposed for this purpose.

The impact of selfishness on network performance has been investigated in various works, either independently, or as a means of comparison after employing a new detection and prevention or punishment scheme. In [31], the impact of selfishness is investigated, setting different behaviors to nodes according to their residual energy that vary from altruistic to entirely selfish behavior. In [32], the impact of selfishness is investigated considering both static and dynamic scenarios. Authors observe four parameters that can impact the network performance and examine them with respect to packet delivery ratio, end-to-end delay, throughput, and energy consumption. In [33], the impact of the spatial concentration of selfish nodes in MANETs is investigated.

V. METHODS TO DEAL WITH SELFISHNESS

In this section, we attempt to answer RQ2, by outlining the various techniques and solutions proposed to address the selfishness problem in MANETs focusing on the network layer. We attempt to categorize the various approaches and present some of the prominent ones from each category. While our attempt might not be exhaustive, we believe it contains the most representative contributions to the field and can be used to understand the main features and challenges of each group of approaches and set the starting point for future research.

The most common taxonomy of articles that consider selfishness in any of its aspects categorizes the methods or approaches as reputation-based, credit-based, trust-based, game-theoretic, etc. We propose a new taxonomy to depict the field. We focus on the operation objectives of each research approach, and we use reputation, credits, trust, or tokens as a metric to measure the behavior of each node or to give incentives, and not to define the approach. We define three categories of approaches, depending on the operation objective of each research approach. All the described methods leverage reputation, credits, trust, or tokens, in conjunction with other available parameters (which will be discussed later), to facilitate their operations and decision-making processes. These methods also consider node-specific parameters such as residual battery and network-related parameters such as network density, which define the node's behavior and the overall network characteristics.

The first category considers the prevention methods. These are mechanisms that are employed and integrated into the routing protocol before any selfishness has even appeared in the network. They provide incentives to the nodes entering the network to prevent them from behaving selfishly, but in most cases luck punitive processes for the non-cooperative ones. In this same category belong the cooperation enforcement methods, that not only provide incentives,

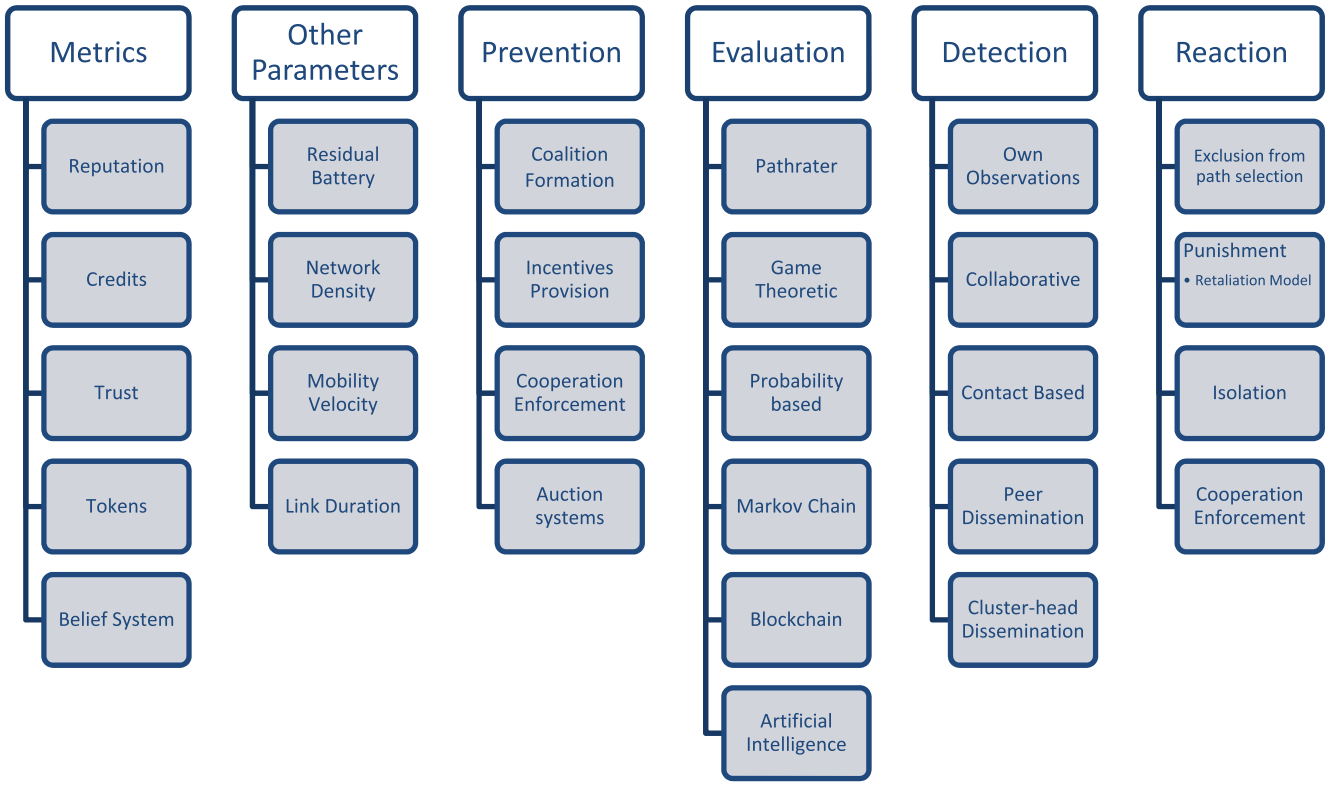

FIGURE 3. Modular taxonomy of main approaches to the selfishness problem in MANETs.

but also enforce nodes to cooperate by forcing rules that make non-cooperative behavior damaging to the selfish node. In the same category there are auction systems and coalition formation systems. These usually use game theoretic approaches to maximize utility and to form beneficial groups to optimize network performance respectively.

The second category, which is the most complex one, contains the modules for the detection and evaluation of selfishness in a MANET. The evaluation module is the method of calculation of the selfishness of each node, considering the metrics and the network parameters and the detection module is the way that metrics are collected, stored, disseminated, and utilized to define whether a node is selfish or not. These two modules act together and that is the reason that we examine them in the same category.

Finally, there is the reaction category, where there are modules that decide the actions against selfish nodes and perform them. It is decided whether the node should be punished for selfish behavior, for example whether it should be isolated from the network permanently or for a specific amount of time. In this category, cooperation enforcement preventive approaches can also be used. However, as most approaches have been developed after security-oriented approaches in the field, in most cases the selfish nodes are permanently isolated from all network operations.

In Fig. 3, a graphical representation of the above taxonomy is presented with some of the most cruci9al elements for each category. In Table 2, the collected articles are listed. For each article we have extracted the approach used in each category. The articles are in chronological order to depict the evolution of the research field.

A. METRICS

The performance of a MANET can be measured using QoS metrics, such as Packet Delivery Ratio (PDR), End-to-End Delay (EED), and Throughput. These metrics provide information about the network operation in total, and not information about the interaction between nodes in terms of data transmission through the network in a multi-hop manner.

To retrieve information about each node and the interaction between them, the methods that deal with selfishness define special metrics. Moreover, other metrics can be embedded into the routing protocols to allow the nodes to modify their behavior. Each node has specific characteristics, such as residual battery, transmission range, speed of movement, mobility model, number of neighbors etc., whereas the network can be sparse or dense, use a specific routing protocol, channel of communication, transfer specific data such as video or aggregated sensor data etc. Some approaches consider metrics from other layers, such as MAC layer queue length, forming cross-layer solutions.

To deal with selfishness, the routing protocols are modified accordingly and can consider various metrics for routing

TABLE 2. Methods to deal with selfishness and features.

Study	Metric	Detection	Evaluation	Reaction	Comments on the method	Year
Marti *et al.* [28]	Reputation	Watchdog	Pathrater	Exclusion from routing paths.	Cooperation is rewarded. Selfish nodes face no consequences for their misbehavior. Instead, by being excluded from the routing paths they have less traffic to handle.	2000
Buttyan *et al.* [42] (Nuglets)	Credits (Nuglets)	Nugget Count	Nugget count	Packets with no nuglets are dropped.	A secure tamper-proof module must be installed in each node. It is a preventive mechanism. Two different models are proposed. In the first one the nuglets are carried on the packets. In the second one packets are traded by nodes.	2000
Michiardi *et al.* [29] (CORE)	Reputation	Direct and Indirect Observation	Reputation Table	Nodes with bad reputation are not served by other nodes.	Modular approach. Three different reputation values are computed and combined.	2002
Buchegger *et al*. [41] (CONFIDANT)	Reputation	Direct and Indirect Observation	Reputation and Trust records Path manager	Exclusion from routing paths	Modular approach where selfish nodes are excluded from the routing paths. There is a substantial number of falsely accusing nodes as selfish.	2002
Buttyan *et al.* [51]	Nuglets	Nuglet Counter	Nuglet Counter	Nodes with no nuglets do not get served by other nodes	A secure tamper-proof module must be installed in each node. It is a preventive mechanism. It does not directly detect or punish selfish nodes.	2003
Miranda *et al.* [45] (Friends and Foes)	Belief system	Each node declares its status	Presence of node in selfish list	Selfish nodes are penalized	Large overhead.	2003
Anderegg *et al.* [52] (Ad hoc-VCG)	Credits	No	VCG Mechanism	VCG Mechanism	Is a preventive method that uses an auction mechanism which can be used with other payment delivery schemes, as it considers only the payment computation and not delivery	2003
Bansal *et al.* [30] (OCEAN)	Reputation	Direct Observation (NeighborWatch)	Pathrater (RouteRanker)	Drops packets from selfish nodes / Redemption allowed	Less complex and less vulnerable to false accusations	2003
Zhong *et al.* [53] (SPRITE)	Credits	No	Game Theory	No	Is a preventive method, which provides incentives for cooperation. A central authority keeps track of the transactions between nodes	2003
Chen *et al.* [40] (iPass)	Credits	No	Vickrey auction	No	Vickrey auction based preventive mechanism. Data packets are extended with special headers.	2004
Balakrishnan *et al.* [54] (TWOACK and S-TWOACK)	Reputation	A two-hop away acknowledgement is transmitted. If not received the path is considered to contain a selfish node.	Receipt or not of ACK	Misbehaving routes are excluded from future routing paths.	Designed for source routing protocols	2005
Conti *et al.* [50] (REEF)	Reliability	Own observations End-to-end ACK	Receipt or not of ACK	Slows down selfish nodes' traffic	It includes security features for robustness and trustworthiness	2006
Hu *et al.* [34] (LARS)	Reputation	Direct Observation	Reputation value compared to a threshold	Routes with selfish nodes are deleted. Selfish nodes' packets are dropped.	Secondhand reputation information is not exchanged between nodes.	2006
Demir *et al.* [55] (Auction-based)	Credits	No	Energy levels and credits are considered into a Vickrey auction	No	Vickrey auction based preventive mechanism. The auction takes place for routes not nodes.	2007
Rizvi *et al.* [56] (Repu-Trust)	Trust Reputation	Watchdog	Pathrater using a table with	Confirmed selfish behavior	Uses only local reputation. Discrete levels of trust	2008

TABLE 2. ***(Continued.)*** **Methods to deal with selfishness and features.**

		Local Reputation only	reputation and trust values.	is penalized with exclusion from network for specific time	Reputation between 0 and 1	
Eldenbenz *et al.* [57]	Credits	VCG Game Theory	Pricing scheme	Selfish nodes remain out of credits so cannot use the network	They introduce the *cost of cooperation*.	2008
Abd El-Haleem *et al.* [46] (TRIDNT)	Trust	Data Link Layer ACK and TCP ACK	Path searching tool identifies selfish nodes	Selfish nodes are isolated	Two disjoint routes are formed. No continuous promiscuous overhearing.	2011
Akhtar *et al.* [49]	Reputation Credits	Promiscuous listing	Retaliation Model	Retaliation Model	Modular approach based on the punishment of misbehaving nodes	2013
Estahbanati *et al.* [58] (Markov chain)	Trust Energy	Trust is computed using a Hidden Markov Model	Trust and energy levels determine the optimal route.	Selfish nodes have low trust values and are not selected in routes.	The method is not applied onto an actual routing protocol. It would be interesting to do so.	2014
Subramaniyan *et al.* [59] (Record and Trust-Based Detection – RTBD)	Trust	Trust table	Trust value depends on the request packets processed by the node	Selfish nodes receive less traffic and get blocked for misreporting	Quick detection of selfish nodes with low overhead.	2014
Das *et al.* [60] (Least Total Cost Factor – LTCF)	Credits	Game theoretic	Paths are selected using LTCF	Paths with selfish nodes are deleted.	Each node has a unique ID and its own Cost Factor.	2015
Kumar *et al.* [35] (Improved Token-Based Umpiring Technique -TBUT)	Token	Promiscuous overhearing	Check token status	Nodes with selfish status are not allowed to participate to network operation	The normal nodes exchange information about suspicious nodes for selfishness, which might increase overhead significantly.	2015
Hernandez-Orallo *et al.* [43] (Collaborative Watchdog - CoCoWa)	Reputation	Collaborative Contact-based Watchdog	Reputation value is computed by data acquired by Local Watchdog and dissemination module	No	Increases detection precision and speed.	2015
Sengathir *et al.* [48]	Trust	Semi-Markov	Futuristic trust coefficient	Isolates selfish nodes	The method can forecast the probability of a mobile node to become selfish based on stochastic properties as an outcome of its present behavior	2015
Zhang *et al.* [61] (Audit-based Misbehavior Detection - AMD)	Reputation	Behavioral Audits Local overhearing	Uses trustworthy route discovery	Isolates selfish nodes	Modular approach that employs a reputation module, a route discovery module and an audit module that interact mutually.	2016
Lupia *et al.* [37] (TEEM)	Trust Link duration	Distributed Monitoring among friendly nodes Periodic HELLO messages	Companion Score that is computed using trust and link duration	Punishing scheme	Divides monitoring time between friendly nodes.	2017
Narayanan *et al.* [62] (Game Theoretical with Audit-based Misbehavior Detection - GAMD)	Reputation	Game Theoretic Behavioral Audits	Uses trustworthy route discovery	Isolates selfish nodes and rewards normal nodes	Similar to [61] with the addition of a game theoretical module that implements a supervisory game	2018
Bounouni *et al.* [63] (New Adaptive Credit-based Stimulation Scheme – NADS)	Credits	Price and reward functions	Normal nodes can send their packets with low price	Exclusion of selfish nodes	Incentive provision and fairness guarantee scheme without central authority	2018
Abiarami *et al.* [64] (Neighbor Credit Value – NCV)	Credits	Direct Observation	Neighbor Credit Value table is maintained at each node.	Exclusion from routing paths.	The authors present an extension of the AODV routing protocol. When a node is suspected to be selfish a test packet is transmitted to that node to confirm its behavior.	2018

TABLE 2. *(Continued.)* **Methods to deal with selfishness and features.**

Sahnoun *et al.* [39]	Residual Energy Number of Neighbors	Cooperative game theoretic	Nodes select coalitions with more benefit	Coalitions that contain selfish nodes are not selected	It is a modified OLSR cross layer approach also considering MAC queue size.	2018
Hasani *et al.* [65]	Hop count Residual Energy Cooperation history	Cooperation rate is calculated using the metrics	Fuzzy Logic	Routes with higher cooperation rate are selected that usually do not contain selfish nodes, as they have low cooperation rates.	The authors use an emulator (MobEmu) to simulate their approach and evaluate its performance.	2019
Jim *et al.* [66]–[68] (Artificial Immune System – AIS)	Trust Reputation [66]	Bio-inspired	Decision Tree [67] Danger Theory [68]	No	Artificial Immune System is used under various assumptions to detect selfish nodes.	2019 2022
Ling *et al.* [38] (Data Broker)	Credits	Blockchain	Credits acquired through ledger list	Reward Policy	Based on B-RAN (blockchain radio access network)	2021
Priya *et al.* [47] (Skellam Distribution Inspired Trust Factor-based – SDITF)	Trust	Intermittent monitoring	Statistics Calculation to determine SDITF value	Selfish nodes are isolated	Nodes with SDITF value less than a threshold are considered selfish and isolated from the network.	2021
Sarumathi *et al.* [36]	Residual Energy	Residual Energy is checked and if it is lower than a threshold the node is considered selfish.	Table of neighbors' behavior	Selfish nodes are isolated	Each node has a table of all its neighbor information, including the residual battery and also the number of RREQ and total packets it has been detected to have forwarded for other nodes.	2022
Fayaz *et al.* [69]	Reputation	Promiscuous overhearing	Consumption to Contribution rate (C2C)	Selfish nodes are isolated	Modular approach that contains reputation module, path manager and selfish node isolation unit.	2022

decisions. Reputation, credits, trust, and tokens can be defined in the routing protocol as measures of nodes behavior.

1) REPUTATION

Reputation can be defined qualitatively as a Boolean value that declares whether a node is normal or selfish, or quantitatively as an integer or real value to indicate how selfish or altruistic a node is on a predefined scale. The reputation value is assigned to each of the nodes and then it is available to the detection and evaluation modules to decide whether to forward or not packets to and from each node. The approaches differ on the way this reputation value is computed, updated, and disseminated through the network and most importantly the way this reputation value affects the routing decisions.

The reputation information can be first-hand (the nodes acquire information for other nodes by directly watching them) or second-hand (the reputation information is disseminated between the nodes of the network). Of course, a combination of these two methods of information retrieval is also possible. In [29], three types of reputation are defined, namely, subjective reputation, indirect reputation, and functional reputation. These three different types of reputation are then combined to calculate the reputation of each node.

There is also the distinction between local and global reputation. As explained in [34], global reputation has the advantage of making reputation information available to all the nodes of the network and therefore the detection time of selfish nodes is decreased. However, more overhead is created in the network and the individual nodes need to maintain and disseminate indirect reputation. In addition, trust issues arise as some nodes might praise or accuse other nodes and different nodes might have different reputation information about the same node. Hence, in [34], a locally aware reputation system is proposed.

2) TRUST

Trust can be used either together with reputation or independently. Trust can be defined in both qualitative and quantitative terms, or it can be achieved by integrating specialized software or hardware modules into the node, enhancing its overall trustworthiness or it can be achieved by integrating specialized software or hardware modules into the node, enhancing its overall trustworthines. Trust-based solutions are associated with security-oriented solutions; therefore, they usually isolate the selfish nodes permanently.

Trust-based approaches develop belief systems about the credibility of relay nodes. When a relay node is trustworthy that means not only that it will forward the packet to the appropriate destination but also that it will report about it

honestly to its peers. Also trusted nodes can be used to report other nodes misbehavior.

Trust-based solutions are mostly utilized in security-oriented approaches aiming to identify malicious nodes, but the same concepts have also been used to identify selfish nodes. However, trust-based solutions tend to be security-oriented, incorporating authentication schemes and more punitive than cooperation enforcement schemes. They are used together with reputation methods in many approaches.

3) CREDITS

Credits are a virtual currency that is exchanged between the nodes when sending, forwarding, or receiving packets, creating a digital economy. In the approaches that use credits, there is a set of economic rules that apply to the network and define the ability of a node to use the network resources and the profit or the cost of receiving and transmitting packets, respectively.

In [27], nuglets are used by the Packet Purse Model (PPM) and the Packet Trade Model (PTM) forming two different implementations of a similar approach proposed by the same authors. The *nuglet* is a virtual currency that is exchanged between the nodes to perform network operations among them. The immediate consequence is that non-cooperative nodes do not have any nuglets, so they are not permitted to participate in the network operation. In the PPM implementation, a virtual Purse is used that contains the nuglets for each node. The main issue with this approach is the need for special hardware to keep nuglets balance reliably.

4) TOKENS

Tokens are special data exchanged between nodes to notify each other about specific incidents. In most cases, a token is transmitted towards a specific node to notify it of an incident, for example upon receival of a packet from an intermediate node that was a suspect of selfishness. Although mentioned mostly in acknowledgement-based (ACK) approaches, they can be used also for other operations in the network. In [35], tokens are used as permission to use the network.

5) BELIEF SYSTEM

Belief systems can contain any kind of information about other nodes. A data structure is maintained into each node that might contain information about other nodes behavior, including reputation values, credits, tokens, trust, friendly nodes, hostile nodes, battery level, etc. They are usually formed through arbitrary data exchange between nodes that is integrated into the protocol and their values are updated accordingly during network operation. Then, various combinations of these data are used to calculate complex metrics or make complex decisions about network operation.

B. OTHER PARAMETERS

The metrics analyzed in the previous section can be combined with node or network characteristics for evaluation of node willingness to cooperate. For example, a node with good reputation is expected not to behave selfishly. However, if the same node has low residual battery, the probability it will start to behave selfishly is inversely proportional to its residual battery. In a sparse network selfish nodes can have a bigger impact than in a denser network.

Metrics are usually kept into a table or other data structure embedded into each node – whereas there are also solutions where the distributed nature of MANETs is overridden and metrics are kept into the cluster head node, when clusters are formed, or into a central authority that ensures trust. Then, depending on the routing protocol employed, these tables help form routing tables in proactive routing protocols, or decide routes or next-hop nodes in reactive routing protocols.

For example, in [36] each node has a table of all its neighbor information, including the residual battery and also the number of RREQ and total packets it has been detected to have forwarded for other nodes. This information is later utilized to make routing decisions. In [37], link duration is considered together with trust to make routing decisions.

C. PREVENTION

Prevention methods are employed and integrated into the routing protocols to provide incentives to the nodes when they enter the network to motivate them to abstain from behaving selfishly.

Many of the preventive mechanisms are based on game theoretic approaches. As game theory examines the interactions between self-centered individuals, it is an appropriate mathematical tool to model the interactions between nodes in MANETs, especially when they behave selfishly. Therefore, it has been widely used for this purpose combined with various concepts, as will be discussed onwards. Most of the game theoretic approaches aim to derive strategies to achieve Nash Equilibrium, under which, the nodes cannot benefit from violating the proposed strategy.

1) COOPERATION ENFORCEMENT

In cooperation enforcement methods, the nodes are not able to use the network resources unless they first provide network services to other nodes. They are initialized having some type of credit to use the network, but if they spend it and, in the meanwhile, they do not help other nodes by forwarding their packets, they soon run out of credits and cannot use the network services, unless they cooperate.

2) INCENTIVES PROVISION

In incentive provision methods, the nodes are not explicitly enforced to cooperate but they are given incentives to choose to cooperate instead of being selfish. This can be achieved by providing rewards when the nodes are not selfish by appropriate reward mechanisms, like in [38].

3) COALITION FORMATION

Some game-theoretic approaches involve coalition formation games, for example in [39] selfishness is prevented by using a

Hedonic Coalition Formation Game model. They can also be triggered by selfishness and applied on the network protocol when selfishness is detected and not before. In this case, the risk for selfishness emerging in the network is outweighed by the energy conservation achieved by not employing the extra preventive mechanism.

4) AUCTION SYSTEMS

Auction based mechanisms have been used in conjunction with credit-based schemes or with reputation-based schemes to elect cluster heads or identify the best route. They cannot be directly used to detect selfish nodes, but they can identify them indirectly by observing their bidding history. The source node must pay an amount of the virtual currency to forward its packets to the destination. Intermediate nodes bid and declare the amount of the virtual currency they want to forward the packets. All the bids are sent to the source node, the path costs are calculated, and the path with the lowest cost is selected. The bid of each node is proportional to its residual energy and its available virtual currency.

These methods are clearly related to the credit-based approaches as they depend also on virtual currencies and economic transactions between the nodes. In [40] a generalized Vickrey auction scheme is utilized to facilitate packet forwarding.

D. DETECTION AND EVALUATION

The metrics described earlier, and the node and network parameters can be used to detect selfishness. In each approach these metrics define the way a node is characterized as selfish. In some cases, reputation and trust are combined, as for example in [41], whereas in others they are independent metrics. Credits have been given various names, for example in [42] they are called *nuglets*and they are used in two different currency exchange models to motivate nodes to cooperate.

Other network parameters considered when detecting and evaluating selfishness in a network include the residual battery or other resource, the network density or prediction of position or velocity. These parameters can be used by the prevention, detection, and evaluation modules to predict whether a node is about to become selfish.

The nodes employ various methods to detect and disseminate knowledge about selfishness in the network. There are cases where the nodes depend only on their own experience or observations [34], whereas in other cases they communicate with other nodes to exchange information about nodes that might be selfish or trustworthy [43]. Therefore, the detection techniques can employ simple Watchdogs that use promiscuous overhearing to notice when a node forwards or not packets. Promiscuous overhearing means that when two nodes are within each other's transmission range they can overhear communications to and from the other node, even if those communications do not involve the overhearing node. There have been proposed more complex solutions and implementations as collaborative watchdogs [43] that communicate and disseminate reputation information.

Watchdog methods can be enhanced using suspect nodes testing. In [44], when a node is suspected to be selfish a test packet is forwarded to it, and depending on its response, or the absence of one, the node is flagged as selfish and isolated from the network.

In addition to detection methods, in some proposed protocols there is the option for the node to declare to its neighbors its status, for example its residual battery level or even its willingness to cooperate or its level or degree of selfishness. In [45], a special packet is broadcasted periodically by each node that contains the nodes it is willing to cooperate with, the nodes that the node is not willing to cooperate with, and the nodes that are known not to cooperate with it. In [46], some degree of selfishness is encouraged, so that selfish nodes declare their status to their neighbors.

One of the current trends in research is the application of Blockchain technology in various disciplines. In [38], Blockchain is used to model to suppress selfish behavior in ad hoc networks.

Statistical and computational methods have been employed successfully to detect selfish nodes. In [47], Skellam distribution is used to compute trust and detect selfish nodes, whereas in [48] a semi-Markov process is used to calculate a futuristic trust coefficient that defines the probability of a node to become selfish, based on its present behavior.

E. REACTION

The reaction to selfishness highly depends on the routing protocol that is used by the network. In source routing protocols, such as DSR, the most common reaction when a node is found to be selfish is to *exclude* it from routing paths. That does not necessarily mean that the node cannot use the network resources. When access to the network resources is also forbidden for the selfish node, we refer to this as *isolation* from the network.

Reaction methods include giving *incentive* to the nodes so as not to become selfish or punish the nodes that have already behaved selfishly. So, we can categorize these methods as preventive or punitive. Prevention mechanisms might also be employed before any selfish nodes are detected in the network.

In [49], the authors use a retaliation model to punish the misbehaving nodes. Their approach uses a combination of reputation and credits system, which they name 'Grade' and 'Bonus Points', to isolate selfish nodes and to define the number of packets dropped. They use a clustering method to divide the network into Friendly Groups and minimize the control traffic overhead generated.

In [29], nodes that are detected as selfish are not served at all from other nodes in the network, whereas in [50] the traffic that originates from selfish nodes is slowed down.

VI. DISCUSSION

In this section, we discuss our findings, and we attempt to answer RQ3. We were able to collect almost all the representative relevant literature dealing with selfishness in MANETs and extract the various methods proposed in them.

We identified the modular nature of the methods and categorized them with respect to their operation. The best performing solutions require some kind of central authority, either to form clusters or to keep some central database of the nodes credits or reputation. These approaches, however, contradict the principle MANETs are built on, that is the distributed nature of routing decision making and the independency of the nodes.

The most common reaction to selfishness is to isolate the node that behaves selfishly. That is a reaction inherited from security-oriented approaches where malicious nodes are blocked and permanently removed from the network. However, when the nodes are selfish, isolating them permanently is not the best approach in terms of network fragmentation and lifetime. Studying the available research, we can conclude that the best way to deal with selfishness is to provide incentives to selfish-prone nodes to cooperate.

The basic idea is that the nodes should be given incentives to cooperate, but if they deviate then the routing protocol should be able to detect that deviation from the cooperative behavior promptly. This can be done using appropriate metrics and then the network should either provide better incentives or punish the selfish node, temporarily or permanently. All the approaches so far employ this basic idea applying different metrics, algorithms, and methods.

Due to the diversity of metrics, scenarios, simulation software and methods employed to evaluate the performance of each method, directly comparing the various methods is not feasible.

Concerning RQ3, we observe that at the early stages of the research field most of the research focused on two separate directions: i) using Watchdogs and Pathraters, either simple or collaborative, and ii) using some kind of trust authority that would keep track of the reputation or credits of the nodes. The common reaction was exclusion from routing paths or starvation due to lack of credits.

As the field evolved, more complex solutions appeared. Modular approaches that involve more than one metric for defining the behavior of each node, audit systems that checked the behavior when the node was suspected of selfishness, and game theoretic cooperation enforcement solutions became the next stage of evolution of the field.

Recently, bio-inspired modeling of MANETs solutions appeared that seem to have a different approach to traditional solutions proposed. Accompanied with blockchain solutions and some artificial intelligence solutions, they are the next big thing in the field.

VII. CONCLUSION AND FUTURE DIRECTIONS

The field of MANETs is a dynamic and constantly evolving field of wireless networking. New techniques, algorithms and approaches continue to emerge as researchers work towards more robust solutions to tackle the selfishness problem and enhance the efficiency and reliability of MANETs. This literature review article serves as a valuable resource for researchers, providing support and direction in advancing the current state-of-the-art in this field and offering a solid starting point for their endeavors.

The recent advances in artificial intelligence and machine learning algorithms in conjunction with the increasing availability of processing power has altered the research directions and perspectives in almost every research field. It is of no surprise that a paradigm shift is observed on the research field of wireless networking, and we expect to observe it soon on the routing for MANETs and the resulting networks. Vehicular and Flying networks and Internet of Everything are about to become the normal way of communication and Artificial Intelligence is the obvious option to facilitate the transition to the future.

Using these innovative technologies should allow researchers to implement lightweight, yet powerful solutions, which will be able to adapt to any network conditions. Applying principles from previous research, selfishness prevention and detection mechanisms will be able to predict network operation and nodes' behavior efficiently and provide users with the best network performance and lifetime.

REFERENCES

[1] C. S. R. Murthy and B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*. London, U.K.: Pearson, 2004.

[2] *Optimized Link State Routing Protocol (OLSR)*, document IETF RFC 3626, Oct. 2003. [Online]. Available: https://www.rfc-editor.org/info/rfc3626, doi: 10.17487/RFC3626.

[3] D. B. Johnson, D. A. Maltz, and J. Broach, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad Hoc Netw.*, vol. 5, pp. 139–172, Jan. 2001. [Online]. Available: http://www.monarch.cs.cmu.edu/

[4] *The Zone Routing Protocol (ZRP) for Ad Hoc Networks*, Internet-Draft, IETF, 2002. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-manet-zone-zrp-04

[5] D. Ramphull, A. Mungur, S. Armoogum, and S. Pudaruth, "A review of mobile ad hoc network (MANET) protocols and their applications," in *Proc. 5th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, May 2021, pp. 204–211, doi: 10.1109/ICICCS51141.2021.9432258.

[6] L. Femila and M. M. Beno, "Optimizing transmission power and energy efficient routing protocol in MANETs," *Wireless Pers. Commun.*, vol. 106, no. 3, pp. 1041–1056, Jun. 2019, doi: 10.1007/s11277-019-06202-7.

[7] A. M. Abdullah, E. Ozen, and H. Bayramoglu, "Investigating the impact of mobility models on MANET routing protocols," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 2, pp. 1–11, 2019. [Online]. Available: www.ijacsa.thesai.org

[8] R. R. Roy, *Handbook of Mobile Ad Hoc Networks for Mobility Models*. Berlin, Germany: Springer, 2011, doi: 10.1007/978-1-4419-6050-4.

[9] A. K. Biswas and M. Dasgupta, "A secure hybrid routing protocol for mobile ad-hoc networks (MANETs)," in *Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2020, pp. 1–7, doi: 10.1109/ICCCNT49239.2020.9225474.

[10] M. H. Hassan, S. A. Mostafa, A. Budiyono, A. Mustapha, and S. S. Gunasekaran, "A hybrid algorithm for improving the quality of service in MANET," *Int. J. Adv. Sci., Eng. Inf. Technol.*, vol. 8, no. 4, pp. 1218–1225, 2018, doi: 10.18517/ijaseit.8.4.5004.

[11] K. Chawda and D. Gorana, "A survey of energy efficient routing protocol in MANET," in *Proc. 2nd Int. Conf. Electron. Commun. Syst. (ICECS)*, Feb. 2015, pp. 953–957, doi: 10.1109/ECS.2015.7125055.

[12] D. Kampitaki and A. A. Economides, "Simulation study of MANET routing protocols under FTP traffic," *Proc. Technol.*, vol. 17, pp. 231–238, Jan. 2014, doi: 10.1016/J.PROTCY.2014.10.233.

[13] N. F. Rozy, R. Ramadhiansya, P. A. Sunarya, and U. Rahardja, "Performance comparison routing protocol AODV, DSDV, and AOMDV with video streaming in MANET," in *Proc. 7th Int. Conf. Cyber IT Service Manag. (CITSM)*, vol. 7, Nov. 2019, pp. 1–6, doi: 10.1109/CITSM47753.2019.8965386.

[14] Y. Yoo and D. Agrawal, "Why does it pay to be selfish in a MANET?" *IEEE Wireless Commun.*, vol. 13, no. 6, pp. 87–97, Dec. 2006, doi: 10.1109/MWC.2006.275203.
[15] H. Yadav and H. K. Pati, "A survey on selfish node detection in MANET," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Oct. 2018, pp. 217–221, doi: 10.1109/ICACCCN.2018.8748420.
[16] S. Aifa and T. Thomas, "Review on different techniques used in selfish node detection," in *Proc. Int. Conf. Circuits Syst. Digit. Enterprise Technol. (ICCSDET)*, Dec. 2018, pp. 1–4, doi: 10.1109/ICCSDET.2018.8821063.
[17] S. Kumar, K. Dutta, and G. Sharma, "A detailed survey on selfish node detection techniques for mobile ad hoc networks," in *Proc. 4th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC)*, Dec. 2016, pp. 122–127, doi: 10.1109/PDGC.2016.7913128.
[18] S. J. H. Al-Shakarchi and R. Alubady, "A survey of selfish nodes detection in MANET: Solutions and opportunities of research," in *Proc. 1st Babylon Int. Conf. Inf. Technol. Sci. (BICITS)*, Apr. 2021, pp. 178–184, doi: 10.1109/BICITS51482.2021.9509889.
[19] J. Webster and R. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quart.*, vol. 26, no. 2, pp. 13–23, Jun. 2002.
[20] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, and R. Chou, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *Int. J. Surg.*, vol. 88, Apr. 2021, Art. no. 105906, doi: 10.1136/BMJ.N71.
[21] B. Kitchenham. (2007). *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. [Online]. Available: https://www.researchgate.net/publication/302924724
[22] I. Wahid, A. A. Ikram, M. Ahmad, S. Ali, and A. Ali, "State of the art routing protocols in VANETs: A review," *Proc. Comput. Sci.*, vol. 130, pp. 689–694, Jan. 2018, doi: 10.1016/J.PROCS.2018.04.121.
[23] G. A. Kakamoukas, P. G. Sarigiannidis, and A. A. Economides, "FANETs in agriculture—A routing protocol survey," *Internet Things*, vol. 18, May 2022, Art. no. 100183, doi: 10.1016/J.IOT.2020.100183.
[24] S. M. Tornell, C. T. Calafate, J.-C. Cano, and P. Manzoni, "DTN protocols for vehicular networks: An application oriented overview," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 868–887, 2nd Quart., 2015, doi: 10.1109/COMST.2014.2375340.
[25] T. Gautam and A. Dev, "Opportunistic network routing protocols: Challenges, implementation and evaluation," in *Proc. 9th Int. Conf. Cloud Comput., Data Sci. Eng.*, Jan. 2019, pp. 100–106, doi: 10.1109/CONFLUENCE.2019.8776947.
[26] C. Xu, Z. Xiong, G. Zhao, and S. Yu, "An energy-efficient region source routing protocol for lifetime maximization in WSN," *IEEE Access*, vol. 7, pp. 135277–135289, 2019, doi: 10.1109/ACCESS.2019.2942321.
[27] J. Marietta and B. C. Mohan, "A review on routing in Internet of Things," *Wireless Pers. Commun.*, vol. 111, no. 1, pp. 209–233, Mar. 2020, doi: 10.1007/s11277-019-06853-6.
[28] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, New York, NY, USA, Aug. 2000, pp. 255–265, doi: 10.1145/345910.345955.
[29] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced Communications and Multimedia Security* (IFIP—The International Federation for Information Processing), vol. 100. Boston, MA, USA: Springer, 2002, pp. 107–121, doi: 10.1007/978-0-387-35612-9_9.
[30] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," 2003, *arXiv:preprintcs/0307012*.
[31] D. G. Kampitaki, E. D. Karapistoli, and A. A. Economides, "Evaluating selfishness impact on MANETs," in *Proc. Int. Conf. Telecommun. Multimedia (TEMU)*, Jul. 2014, pp. 64–68, doi: 10.1109/TEMU.2014.6917737.
[32] A. Shan, X. Fan, C. Wu, X. Zhang, and S. Fan, "Quantitative study on the impact of energy consumption based dynamic selfishness in MANETs," *Sensors*, vol. 21, no. 3, pp. 1–19, 2021, doi: 10.3390/s21030716.
[33] S. Gupta, C. K. Nagpal, and C. Singla, "Impact of selfish node concentration in MANETs," *Int. J. Wireless Mobile Netw.*, vol. 3, no. 2, pp. 29–37, Apr. 2011, doi: 10.5121/ijwmn.2011.3203.
[34] J. Hu and M. Burmester, "LARS—A locally aware reputation system for mobile ad hoc networks," *Proc. Annu. Southeast Conf.*, 2006, pp. 119–123, doi: 10.1145/1185448.1185475.
[35] J. M. S. P. J. Kumar, A. Kathirvel, N. Kirubakaran, P. Sivaraman, and M. Subramaniam, "A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, pp. 1–11, Dec. 2015, doi: 10.1186/s13638-015-0370-x.
[36] R. Sarumathi and V. Jayalakshmi, "Detection of selfish nodes based on node energy in mobile adhoc networks—MANETs," in *Proc. Int. Conf. Autom., Comput. Renew. Syst. (ICACRS)*, Dec. 2022, pp. 346–350, doi: 10.1109/ICACRS55517.2022.10029094.
[37] A. Lupia, C. A. Kerrache, F. D. Rango, C. T. Calafate, J.-C. Cano, and P. Manzoni, "TEEM: Trust-based energy-efficient distributed monitoring for mobile ad-hoc networks," in *Proc. Wireless Days*, Mar. 2017, pp. 133–135, doi: 10.1109/WD.2017.7918128.
[38] X. Ling, P. Chen, J. Wang, and Z. Ding, "Data broker: Dynamic multi-hop routing protocol in blockchain radio access network," *IEEE Commun. Lett.*, vol. 25, no. 12, pp. 4000–4004, Dec. 2021, doi: 10.1109/LCOMM.2021.3114218.
[39] 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. (IJECE)*, vol. 8, no. 1, p. 26, Feb. 2018, doi: 10.11591/ijece.v8i1.pp26-33.
[40] K. Chen and K. Nahrstedt, "IPass: An incentive compatible auction scheme to enable packet forwarding service in MANET," in *Proc. 24th Int. Conf. Distrib. Comput. Syst.*, 2004, pp. 534–542, doi: 10.1109/ICDCS.2004.1281620.
[41] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in *Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2002, pp. 226–236.
[42] L. Buttyan and J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in *Proc. 1st Annu. Workshop Mobile Ad Hoc Netw. Comput.*, 2000, pp. 87–96, doi: 10.1109/MOBHOC.2000.869216.
[43] E. Hernández-Orallo, M. D. S. Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, "CoCoWa: A collaborative contact-based watchdog for detecting selfish nodes," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1162–1175, Jun. 2015, doi: 10.1109/TMC.2014.2343627.
[44] 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, doi: 10.1109/ICACCCN.2018.8748632.
[45] H. Miranda and L. Rodrigues, "Friends and foes: Preventing selfishness in open mobile ad hoc networks," in *Proc. 23rd Int. Conf. Distrib. Comput. Syst. Workshops*, 2003, pp. 440–445, doi: 10.1109/ICDCSW.2003.1203592.
[46] A. M. A. El-Haleem, I. A. Ali, I. I. Ibrahim, and A. R. H. El-Sawy, "TRIDNT: Isolating dropper nodes with some degree of selfishness in MANET," in *Communications in Computer and Information Science*, vol. 131. Berlin, Germany: Springer, 2011, pp. 236–247, doi: 10.1007/978-3-642-17857-3_24.
[47] M. D. Priya, A. C. J. Malar, J. Sengathir, and T. Akash, "A Skellam distribution inspired trust factor-based selfish node detection technique in MANETs," in *Proc. 6th Int. Conf. Recent Trends Comput.*, vol. 177, 2021, pp. 357–368, doi: 10.1007/978-981-33-4501-0_34.
[48] J. Sengathir and R. Manoharan, "A futuristic trust coefficient-based semi-Markov prediction model for mitigating selfish nodes in MANETs," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, pp. 1–13, Dec. 2015, doi: 10.1186/s13638-015-0384-4.
[49] M. A. K. Akhtar and G. Sahoo, "A novel methodology to overcome routing misbehavior in MANET using retaliation model," *Int. J. Wireless Mobile Netw.*, vol. 5, no. 4, pp. 187–202, Aug. 2013, doi: 10.5121/ijwmn.2013.5414.
[50] M. Conti, E. Gregori, and G. Maselli, "Reliable and efficient forwarding in ad hoc networks," *Ad Hoc Netw.*, vol. 4, no. 3, pp. 398–415, May 2006, doi: 10.1016/J.ADHOC.2004.10.006.
[51] L. Buttyán and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *Mobile Netw. Appl.*, vol. 8, no. 5, pp. 579–592, 2003, doi: 10.1023/A:1025146013151.
[52] L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *Proc. 9th Annu. Int. Conf. Mobile Comput. Netw.*, New York, NY, USA, Sep. 2003, pp. 245–259, doi: 10.1145/938985.939011.
[53] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proc. 22nd Annu. Joint Conf. IEEE Comput. Commun. Societies*, Mar. 2003, pp. 1987–1997, doi: 10.1109/INFCOM.2003.1209220.
[54] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, vol. 4, Mar. 2005, pp. 2137–2142, doi: 10.1109/WCNC.2005.1424848.

[55] C. Demir and C. Comaniciu, "An auction based AODV protocol for mobile ad hoc networks with selfish nodes," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2007, pp. 3351–3356, doi: 10.1109/ICC.2007.555.

[56] S. S. Rizvi, V. Edla, S. Poudyal, and R. Nepal, "Reducing malicious behavior of mobile nodes in ad hoc networks," in *Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics*. Dordrecht, The Netherlands: Springer, 2008, pp. 526–531, doi: 10.1007/978-1-4020-8737-0_95.

[57] S. Eidenbenz, G. Resta, and P. Santi, "The COMMIT protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes," *IEEE Trans. Mobile Comput.*, vol. 7, no. 1, pp. 19–33, Jan. 2008, doi: 10.1109/TMC.2007.1069.

[58] M. M. Estahbanati, M. Rasti, and S. M. S. Hamami, "A mobile ad hoc network routing based on energy and Markov chain trust," in *Proc. 7th Int. Symp. Telecommun. (IST)*, Sep. 2014, pp. 596–601, doi: 10.1109/ISTEL.2014.7000775.

[59] S. Subramaniyan, W. Johnson, and K. Subramaniyan, "A distributed framework for detecting selfish nodes in MANET using record- and trust-based detection (RTBD) technique," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, p. 205, Dec. 2014, doi: 10.1186/1687-1499-2014-205.

[60] D. Das, K. Majumder, and A. Dasgupta, "Selfish node detection and low cost data transmission in MANET using game theory," *Proc. Comput. Sci.*, vol. 54, pp. 92–101, Jan. 2015, doi: 10.1016/j.procs.2015.06.011.

[61] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 8, pp. 1893–1907, Aug. 2016, doi: 10.1109/TMC.2012.257.

[62] 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, doi: 10.1109/ICICCT.2018.8473197.

[63] M. Bounouni and L. Bouallouche-Medjkoune, "Adaptive credit-based stimulation scheme for dealing with smart selfish nodes in mobile ad hoc network," in *Proc. Int. Symp. Program. Syst. (ISPS)*, Apr. 2018, pp. 1–5, doi: 10.1109/ISPS.2018.8379006.

[64] K. R. Abirami and M. G. Sumithra, "Evaluation of neighbor credit value based AODV routing algorithms for selfish node behavior detection," *Cluster Comput.*, vol. 22, no. S6, pp. 13307–13316, Nov. 2019, doi: 10.1007/s10586-018-1851-6.

[65] H. Hasani and S. Babaie, "Selfish node detection in ad hoc networks based on fuzzy logic," *Neural. Comput. Appl.*, vol. 31, no. 10, pp. 6079–6090, Oct. 2019, doi: 10.1007/s00521-018-3431-3.

[66] L. E. Jim and M. A. Gregory, "An artificial immune system-based strategy to enhance reputation in MANETs," *J. Telecommun. Digit. Economy*, vol. 7, no. 1, pp. 68–82, Mar. 2019, doi: 10.18080/jtde.v7n1.176.

[67] L. E. Jim and M. A. Gregory, "Improvised MANET selfish node detection using artificial immune system based decision tree," in *Proc. 29th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2019, pp. 1–6, doi: 10.1109/ITNAC46935.2019.9077968.

[68] L. E. Jim, N. Islam, and M. A. Gregory, "Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes," *Comput. Secur.*, vol. 113, Feb. 2022, Art. no. 102538, doi: 10.1016/j.cose.2021.102538.

[69] M. Fayaz, G. Mehmood, A. Khan, S. Abbas, M. Fayaz, and J. Gwak, "Counteracting selfish nodes using reputation based system in mobile ad hoc networks," *Electronics*, vol. 11, no. 2, p. 185, Jan. 2022, doi: 10.3390/electronics11020185.

DIMITRA G. KAMPITAKI (Member, IEEE) received the bachelor's degree in electronics engineering from the Alexander Technological Educational Institute of Thessaloniki, Greece, in 2004, and the master's degree in information systems from the University of Macedonia, Greece, in 2008, where she is currently pursuing the Ph.D. degree.

She was a Lab Instructor with the Department of Electronics, Alexander Technological Educational Institute of Thessaloniki, and an Electronics Engineer with the Meteorological Applications Centre-Hellenic Agricultural Insurance Organization. She is currently an Electronics Engineer with the Aristotle University of Thessaloniki. She has contributed to many National and European funded research programs. She has several publications in peer-reviewed journals and conferences. Her research interests include the optimization of telecommunication systems, routing for mobile networks, and machine learning for communications.

ANASTASIOS A. ECONOMIDES (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer engineering from the University of Southern California, Los Angeles, CA, USA, in 1987 and 1990, respectively.

He is currently with the University of Macedonia (UoM), Thessaloniki, Greece. He is the Director of the Smart and Mobile Interactive Learning Environments (SMILE) Laboratory and the Computer Networks and Telematics Applications (CONTA) Group. He is listed among the top 2% of scientists all over the world. He has published two books and more than 400 peer-reviewed papers in international journals, conference proceedings, and books. He has received more than 9000 citations. His research interests include online and mobile teaching and learning, routing and competition in telecommunication networks, and digital marketing. He was the keynote speaker in several international conferences, in the program committees of dozens of conferences and in the editorial committee boards of many journals.