Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 5653010, 17 pages
http://dx.doi.org/10.1155/2016/5653010

Research Article

Security-Based Mechanism for Proactive Routing Schema Using Game Theory Model

Hicham Amraoui,[1] Ahmed Habbani,[1,2] Abdelmajid Hajami,[3] and Essaid Bilal[4]

[1]*SIME Lab, MIS Team, ENSIAS, Mohammed V University, Rabat, Morocco*
[2]*LEC Lab, EMI, Mohammed V University, Rabat, Morocco*
[3]*LAVETE Lab, FST, Hassan I University, Settat, Morocco*
[4]*Research and Development, OCP, Casablanca, Morocco*

Correspondence should be addressed to Hicham Amraoui; amraoui.hicham1@gmail.com

Received 25 August 2016; Accepted 12 October 2016

Academic Editor: Jose M. Barcelo-Ordinas

Game theory may offer a useful mechanism to address many problems in mobile ad hoc networks (MANETs). One of the key concepts in the research field of such networks with Optimized Link State Routing Protocol (OLSR) is the security problem. Relying on applying game theory to study this problem, we consider two strategies during this suggested model: cooperate and not-cooperate. However, in such networks, it is not easy to identify different actions of players. In this paper, we have essentially been inspired from recent advances provided in game theory to propose a new model for security in MANETs. Our proposal presents a powerful tool with a large number of players where interactions are played multiple times. Moreover, each node keeps a cooperation rate (CR) record of other nodes to cope with the behaviors and mitigate aggregate effect of other malicious devices. Additionally, our suggested security mechanism does not only take into consideration security requirements, but also take into account system resources and network performances. The simulation results using Network Simulator 3 are presented to illustrate the effectiveness of the proposal.

1. Introduction

In our everyday life, we are very interested in and dependent on wireless connection technology. In addition, the use of mobile devices and applications based on wireless networks is continuously increasing day after day. However, this may generate several kinds of problems in terms of communication between mobile devices in some difficult situations. These problems can be observed, especially where a network infrastructure is missing. Therefore, we need a powerful and efficient mobile ad hoc network (MANET) to ensure and improve communication between devices in different situations such as military fields, conferencing, and sensor networks.

MANETs are a collection of wireless mobile devices that form a temporary network without an existing infrastructure or a centralized administration. Furthermore, and due to limited transmission range of wireless interfaces, it may be necessary for one node to identify other nodes to forward their packets to its destinations. In such networks, each node does not merely work as a host for transmitting and receiving data but acts as a router or gateway for routing packets from other nodes as well. Moreover, each node participates in routing process that allows it to establish paths to reach any possible destination inside the network. In addition, all nodes dynamically establish paths between themselves to create network infrastructure that depends on individual behavior of nodes. Along these lines, and in a spontaneous nature of MANET, all nodes move randomly across the network because of the nodes mobility and bandwidth-constrained wireless connection for communicating with each other. This nature permits infiltrating and disrupting network performances by malicious and selfish nodes. Thereby, malicious behavior represents one of the most famous challenges and destructive routing problems that can influence network performances. Additionally, the concept of selfish node attack

is based on the absorbing of significant amount of traffic, dropping received packets, and not cooperating during the packet routing process. However, this problem arises when examining network topology where malicious nodes cannot be easily detected.

MANETs are infrastructureless and self-organized; all nodes have to cooperate between themselves in order to provide the best performances and offer necessary network functionalities. The cooperation mechanism must comply with the rules imposed by the routing protocol for transmitting and receiving data. On the other hand, the noncooperation behavior can be produced by nodes that do not follow these rules. However, all nodes act as routers or gateways and contribute to discovering and maintaining the routing process. Moreover, each node is constrained in terms of limited resources (energy, etc.), and it may not always be interesting to accept relay requests that require consumption of most resources. Therefore, a cooperative system should be integrated and incorporated with any network operations such as packet forwarding and route discovery. The goal of this system is to prevent malicious behavior and encourage nodes to cooperate with each other. However, the application of cooperation mechanism is particularly difficult because of MANET features that impose certain requirements.

In this context, many researchers have investigated selfish nodes and security problems in MANETs. In this way, the authors in [1] proposed a solution to improve network performances when attacks are launched and mitigate aggregate effect, especially that all nodes in such networks are vulnerable to being isolated by malicious nodes. Furthermore, the authors in [2] presented a powerful intrusion detection system called Enhanced Adaptive ACKnowledgment (EAACK). Compared to other intrusion detection mechanisms, EAACK shows an efficient attack detection without affecting network performances. Likewise, the authors in [3] surveyed the impact of packet dropping attacks in MANET. In their work, the authors try to demonstrate the importance of attacks, elaborate a new detection system, and avoid malicious nodes during communication with each other. Additionally, MANET nature makes it more attractive to many types of attacks. In this way, the authors in [4] proposed a survey in two parts: the first one addresses important security mechanisms and types of attacks that can affect network performances, especially in the network layer. The second one addresses the classification of detection mechanisms that deal with a single or series of attacks. Furthermore, in the work presented in [5], the authors suggested a powerful solution called I-Watchdog protocol to detect malicious nodes in MANETs. In addition, the authors proved through simulations the effectiveness of this solution with Destination-Sequenced Distance-Vector (DSDV) routing protocol in terms of packet drop ratio (PDR), throughput, and end-to-end delay.

Recently, game theory provides a useful solution for modeling and addressing different problems in MANETs. In such networks, players (nodes) have conflicting objectives and different profiles with each other. Additionally, in the game theory, a utility function represents a payoff (reward) that allows each player to evaluate a particular outcome that reflects its objectives. The utility of each player depends not only on its actions (strategies), but also on others' actions. In addition, a security scheme must take into account past and current strategies of different players to be successful in MANETs.

In the same context, our research is focused on mobile ad hoc networks using Optimized Link State Routing Protocol (OLSR) which is a proactive protocol. In such networks, OLSR is one of the most used routing protocols. Moreover, the cooperation concept is an essential element that can result in the evolution of network performances in MANET. In this way, and in this paper the cooperation rate (CR) represents the value which indicates how many times a node cooperates or not during the game (or during network lifetime). Through this value, each node can evaluate the behavior of another node before sending a packet. Moreover, in this paper, a threshold is considered as the minimum value of the CR accepted by all rational nodes. We consider that each node which has a $CR > 0$ is considered as a legitimate node, whereas a node with $CR < 0$ is considered as a noncooperative node. Therefore, our contribution is briefly summarized below:

(i) Firstly, our conduct is to put forward an enhanced algorithm based on game theory and establishing confident relationships between nodes. In this proposed model, each node keeps a cooperation rate (CR) record of other nodes to evaluate their behaviors and avoid malicious nodes.

(ii) Secondly, the calculation of CR is based on OLSR messages (HELLO and topology control (TC)) exchanged between nodes and forwarding processes.

(iii) Thirdly, the cooperation rate will be shared between nodes in addition to other network information using HELLO and TC messages.

(iv) Fourthly, the key novelty of this paper is that the value of CR will be used as a metric to construct routing tables instead of hop count metric used by OLSR standard.

The remainder of this paper is organized as follows: The OLSR routing protocol as a proactive scheme is presented in Section 2. Some previous studies that aim at addressing cooperation and selfish behavior in MANETs are presented in Section 3. A game model formulation is described in Section 4. Our suggested system model based on cooperation between nodes is discussed in Section 5. A malicious detection algorithm and enhanced routing table computation are introduced in Section 6. A simulation environment used to address our approach is discussed in Section 7. The results that concern the validation of our solution are presented in Section 8. Finally, the paper is concluded in Section 9 with future work.

2. Proactive Schema: Case of OLSR

OLSR is a proactive routing protocol [6] based on MPR (multipoint relay) mechanism that is considered as the key concept used in this protocol. The MPRs are used to maintain

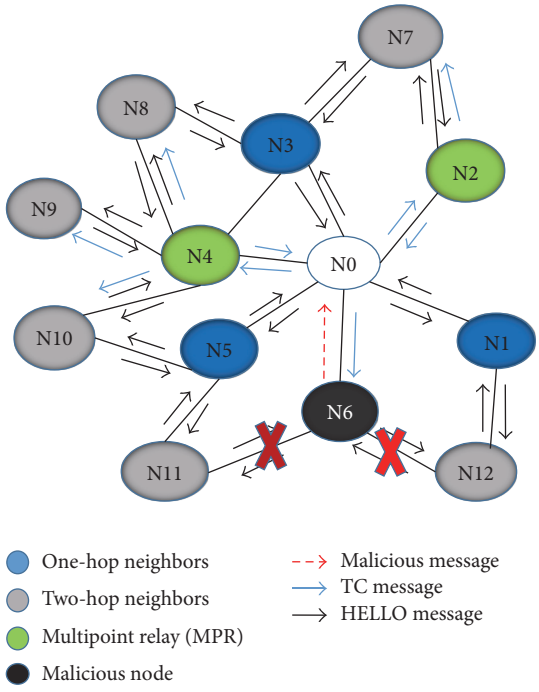

Figure 1: Attack example in MANETs.

routing tables and topology control. In addition, and owing to the proactive nature of OLSR, the control of the state links and paths is done proactively and periodically. In the same way, the optimization in this protocol can be done in two steps: the first one uses control messages with reduction in size. The second one uses a reduced number of links to forward the link state packets. In addition, this reduction is made by declaring only a subset of links in link state updates. Moreover, each node in OLSR uses HELLO messages to find its one-hop and two-hop neighbors through their replies. The transmitter node can select its MPR based on its one-hop neighbors set that offers the best reachability to nodes belonging to the two-hop neighbors. Furthermore, the transmitter uses TC (topology control) messages to declare a set of links (advertised link set) that must include at least the links to all nodes of its MPR selector set [6].

The routing in MANETs using OLSR is a method through which each node sends information to a quite precise recipient. The problem of routing is limited not only to how to find a path between two nodes inside the network, but also to how to find an optimal and secure routing path. However, in such networks, one of the major problems of routing processes is the noncooperative and selfish behaviors as denoted in Figure 1. In these cases, the noncooperative and selfish nodes take advantage of legitimate nodes and do not cooperate with others in order to save resources for their own communication. Thereby, network resources become unavailable for legitimate nodes.

3. State of the Art

MANETs are used in a wide range of applications in various fields. For successful execution of different operations in such networks, routing processes are the most important operations that improve network performances. Therefore, many researches have been reported in the literature to address routing processes. In this way, the authors in [7] presented an incentive solution for probabilistic routing in order to stimulate selfish nodes to cooperate with others. In addition, the authors proved properties of this solution and extensively evaluated it using GloMoSim. Furthermore, the result presents more than 75.8% of the gain concerning delivery ratio compared to other probabilistic routing protocols without incentive.

On the other hand, and in order to address joint routing, network coding, and scheduling problems, matrix game theoretic models, which are based on a nonlinear cubic game, have been proposed in several works such as [8]. The authors in this work, due to necessity of the inherent multicast gain of network, proposed a new approach based on a compressed topology matrix to model routing and network coding problems. Additionally, the authors proposed a new approach called Network Graph Soft Coloring (NGSC) to optimize scheduling problems. Furthermore, the authors in [9] presented a solution based on a two-hop relay with limited packet redundancy f, to propose a forwarding game and address the optimal forwarding problem in MANETs. In this game, each node (i) chooses a strategy with probability T_i ($T_i \in [0, 1]$) to send and forward its own traffic. Additionally, each node (i) helps to forward other traffic with probability p, where $p = 1 - T_i$, while its payoff is the attainable throughput capacity of its own traffic.

In wireless ad hoc networks, the routing is the most important process that needs cooperation between nodes. Thus, some cooperation schemes and trusted models have been proposed in several works such as [10–15]. The main objectives of these works are the following: (i) to enforce cooperation between nodes and (ii) to evaluate and address aggregate effect of malicious nodes. Moreover, and in order to reach these objectives, the authors presented many solutions such as collaborative reputation model, a game theoretic trust model, collaborative caching priority, coalition formation, and cooperation strategies for processing requests. In addition, the authors in [16] presented, in noncooperative wireless ad hoc networks, a study of collusion-resistant routing. This work is based on two solutions: Group Strategy Proofness and Strong Nash Equilibrium for collusion resistance in game theory. Also, the authors proposed a cryptographic mechanism to avoid profit transfer among colluding players (nodes). In the same context, the authors in [17] used the game theory to address cooperation incentive of nodes based on reputation mechanisms, price-based systems, and a system without cooperation incentive strategy. Through this work, a strategy based on a threshold to determine node reliability and reward cooperative nodes may be manipulated by selfish nodes. In addition, the authors in [18] proposed a powerful solution built on Mean Field Game (MFG) approach with multiple players for security enhancements in MANET. Based on recent advances in MFG theory, this approach permits enabling each node to elaborate strategic security defense decisions. Additionally, this approach takes into account system resources, permits each node to know its

own state information and evaluate aggregate effect of other nodes. However, the authors studied the interactions between nodes and only one attacker.

In MANETs, nodes must cooperate between them to send and forward packets from sources to destinations. In this way, the work presented in [19] showed that node misbehavior problems can influence MANETs and sensor networks performances. In addition, and in order to avoid this problem, the authors proposed a solution adapted to wireless multihop network in order to deal with collusive networking behavior based on game theory. Additionally, this solution is derived from recent works that are based on the theory of imperfect private monitoring for the dynamic Bertrand Oligopoly. Also, the authors showed the effectiveness of this solution under a wireless environment. Along these lines, and due to the importance of the cooperation concept, the authors in [20] proposed a solution called Finite-Time Reputation System (FITS) that uses a new technique named Threat To Interfere (TTI) to enforce cooperation between nodes. In addition, this mechanism is based on two solutions: the first one called FITS-D needs a Perceived Probability Assumption (PPA). The second one called FITS-I uses more techniques to avoid the necessity of PPA. Moreover, this work showed that both of schemes have a Subgame Perfect Nash Equilibrium (SPNE) in which the probability of forwarding packet of nodes is close to one.

In the same context, the authors in [21, 22] proposed a secure routing protocol to protect nodes from anonymous behaviors. These works are based on game theory which provides a powerful tool to analyze, formulate, and address selfish behaviors. In addition, these authors used the Dynamic Bayesian Signaling Game (DBSG) to analyze strategy profiles for rational and malicious nodes to find the best strategies for each player (node). Furthermore, the authors studied the equilibrium by combining strategies and utility functions (payoff) of nodes to solve this incomplete information problem. Moreover, and to reach this goal, the authors used Perfect Bayesian Equilibrium (PBE) that offers an important solution for signaling games. Likewise, the authors presented in [23] a solution to deal with selfishness and moral hazard in noncooperative wireless networks. In addition, they proposed a solution based on several methods that discourage hidden actions under secret information. Furthermore, some mechanisms for routing scenarios have been proposed; for instance, each malicious node tries to maximize its utility function when it sincerely declares its cost and actions. Also, the authors proved through simulations that payments are larger compared to current cost incurred by all intermediate devices.

Along these lines, and in order to detect and isolate packet dropping attacks efficiently, the work in [24] proposed a protocol named SADEC (Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure). This protocol is based on two techniques: the first one is based on how to keep additional information about routing paths by neighbors. The second one is based on how to add some checking mechanisms to each neighbor. This protocol can offer a powerful solution to use local monitoring. In addition, the authors showed by simulations the effectiveness of the protocol in how to reduce the impact of packet dropping attack. In the same way, the authors in [25] proposed a solution based on Social Network Analysis (SNA) to develop an intrusion detection mechanism (SN-IDS) in MANETs using MAC and network layers data. After that, these authors selected relevant social functionalities and constructed a set of sociomatrices. Moreover, these authors showed that these methods based on social analysis can be applied to these matrices to detect malicious activities of mobile nodes using multiple rules.

Similarly, in the work proposed in [26], the authors presented an intrusion detection system to detect attack sequences in MANET using MAC layer applications. This system can be applicable to MANET environment based on stable and efficient attack observations. In such a way, the solution presented in [27] suggested an intrusion detection and adaptive response mechanism to provide an effective reply in case of a range of attacks in MANETs. This solution, in order to offer a better security requirement, proposed a flexible response scheme based on effectiveness level of network performances, measured confidence, and the impact of attacks. In addition, the authors in [28] proposed a solution called Sentinel Protocol (SP) to detect and deal with replica attacks that can influence network performances. The main objective of this attack is that malicious nodes deploy a large number of replicas of compromised or captured devices across the network. Furthermore, the authors proved through simulations the effectiveness of this protocol.

Due to the importance of the routing efficiency in delay tolerant networks, the authors in [29] suggested an enhanced routing protocol which is based on the social link awareness. The main objective of this algorithm is to avoid the selfish nodes and solve the problems of intermittent connection and high latency in order to improve the routing process. In addition, the proposed algorithm used the social links to construct the friendship communities of the nodes. Moreover, different mechanisms such as the intracommunity and intercommunity forwarding are implemented to improve network performances in terms of the successful delivery ratio with low overhead and decrease the transmission delay. In the work presented in [30] the authors proposed a solution based on game theory and load feedback control (LFC) with price elasticity to maximize profit benefits for distributed generations (DGs) for their participation in energy loss reduction. In addition, the proposed model can be used to reward DGs and improve their profit by using the game theory approach. Moreover, and where a distributed locational marginal pricing (DLMP) feedback signal is calculated by customer demand, the proposed mechanism can be used to regulate peak-load value of multiple customers by using an LFC submodel with price elasticity. In addition, the authors in [31] proposed a global punishment-based repeated game model to enforce the cooperation between nodes across the network. Additionally, when the whole network is in a cooperative state, the authors investigated the equilibrium conditions of packet forwarding strategies by taking into account rational nodes. Moreover, a metamodel is used to design forwarding strategies in order to reduce the impact

Table 1: A duality between a game approach and a MANET.

Elements of a game	Elements of a mobile ad hoc network
Players	Nodes
Strategy	Action linked to each player to evaluate its utility. In our game, we consider two strategies: cooperate and not-cooperate
Utility function	(i) Performance metrics (throughput, packet forwarded, packet received, and end-to-end delay). (ii) The cooperation rate (CR) of each node (player)

of selfish nodes on network performances and encourage the cooperation between mobile nodes.

Recently, the effective cooperation incentive of nodes has become a hot issue in cooperative communication such as mobile ad hoc networks. In such a way, the authors in [32] proposed a topology transform-based recommendation trust model to stimulate the cooperation between nodes and mitigate effect of selfish behaviors. Furthermore, the model is used to mitigate the aggregate of malicious effects on the accuracy of recommendation trust, which result from fake recommendation. In addition, the authors used some mathematical models and simulation to ensure the effectiveness of their proposed model.

To address these problems and imperfections, and through this paper, our concern is to design a new algorithm of cooperation based on relationships between nodes. Then, we will compare the proposal with the original OLSR and a selfish OLSR protocol; after that, we integrate it with original OLSR. Additionally, we address the proposal based on a mathematical model and set of simulations. Furthermore, the main objective is to be fully extended to universal ad hoc networks and practical MANET applications, especially routing processes and malicious node detection.

4. Game Model Formulation

4.1. Modeling Ad Hoc Network as a Game. In this section, we propose a description of a mobile ad hoc network G, which is formed by a set of mobile nodes, using the game theory approach. This formulation contains a set of nodes (players) denoted by (N), a strategy space denoted by (S), and a utility function denoted by (F). Thus, the network can be expressed by $G = \{N, S, F\}$. Table 1 presents briefly a duality between a game approach and the mobile ad hoc network in our situation.

In the abovementioned network G, each node has a utility function F that represents the payoff of each player (node) across the network. In addition, a utility function represents a payoff (reward) that allows each player to evaluate a particular outcome which reflects its objectives. The main objective of all nodes (players) is how to maximize or minimize the utility function depending on a context. In the same way, each player acts as a relay or gateway for routing packets from other players based on available routing and topology tables. In addition, each player (i) chooses its strategy S_i from the strategy space S defined by $S = \{\text{C: cooperate, NC: not-cooperate}\}$ (cooperate means to participate in packet forwarding and not-cooperate means packet dropping).

4.2. Static and Repeated Game Approach. To analyze the outcome of the static game, our two-player game is similar to the prisoners dilemma game [33]. Each player can choose different strategies: cooperate (C) or not-cooperate (NC). If one of the two players chooses to cooperate, it will act as a router or gateway for the other player. However, if the player chooses the not-cooperate strategy, it will forward its own packets and will not participate in routing packets for the other player.

In this paper, we consider that if a player chooses to cooperate, it will be rewarded by a lot of information (ACKs, topology control, links update, routing of packets, etc.); this reward is denoted by V, but at the same time it will lose a cost denoted by (e). However, if the two players choose not-cooperate strategy, both of them will lose the information already mentioned above.

Let us denote by $(V - e)$ the reward of each player that chooses to cooperate and by (V) the reward of the player that chooses not-cooperate in case the first player chooses to cooperate and by $(-r)$ the punishment that each player receives if both choose not-cooperate strategy. Therefore, in the rest of this paper, we assume that $V > (V - e) > -r$.

The only optima equilibrium if the two players are rational is the strategy profile $(V - e, V - e)$, where the first strategy denoted in the pair is that of player (1) and the second is that of player (2). This strategy profile will be available only if the two players choose the cooperate strategy. Moreover, this situation cannot be realized in all static games due to a selfish behavior of some players. However, the profile $(-r, -r)$ where the two players choose the not-cooperate strategy is undesirable from the network perspective.

In our situation, we consider that the past strategies influence the payoff (utility) function in current period (stage). Thus, the game can be analyzed using the repeated game approach [34, 35], where all players face the same static game many times and in every period t. Therefore, we choose to apply the repeated game approach in our situation for the following reasons:

(1) The game or nodes interactions are played several times. In addition, when a node (player) takes into consideration the impact of its current strategy on future actions of other nodes, the game is called repeated game.

(2) During this kind of games, all nodes (players) can observe different actions of other players, and this characteristic helps to adapt their actions (strategies) to respond to other players, especially that each node keeps track of the cooperation rate (CR) record of other nodes.

Table 2: Payoff matrix of two-player game in strategic form.

Player (1)	Player (2)	
	C	NC
C	$(V-e, V-e)$	$(V-e, V)$
NC	$(V, V-e)$	$(-r, -r)$

Table 3: Payoff matrix in mixed strategy of two-player game in strategic form.

Player (1)	Player (2)	
	C (p)	NC ($1-p$)
C (q)	$(V-e, V-e)$	$(V-e, V)$
NC ($1-q$)	$(V, V-e)$	$(-r, -r)$

(3) Furthermore, selfish players act as routers or gateways only to their interest without taking into consideration network performances. So we can define and impose some rules to enforce cooperation between nodes. In addition, these rules can be modeled using the repeated game.

(4) These rules can be implemented to reach a desirable result of developed games. Moreover, repeated games support different equilibrium solutions which are adapted for many requirements of ad hoc networks.

In this paper, and in order to enforce cooperation between nodes, each player keeps track of the cooperation rate (CR) record of other players as a rule in this game model. The main objective of this rule is to show the importance of cooperation potential benefits through interactions between nodes. Also, this rule can be modeled in a repeated game.

4.3. Problem Formulation and Nash Equilibrium

4.3.1. Pure Strategy. In this section, we consider a problem that may exist in different types of networks, where optimization of communication is very important. In our study, we consider a flow of network traffic generated by a finite number of nodes (players). In addition, each node knows a list of paths that fits its strategy, and its objective is to maximize its utility function. The situation where all players maximize their utility functions is known as Nash Equilibrium (NE) [31, 36]. In the repeated and noncooperative game models, the NE is used to predict the stable situation where no player (node) has nothing to gain by changing its strategy unilaterally.

In the same context, and in this pure strategy, a Nash Equilibrium is a strategic profile $S^* = \{S_1^*, S_2^*, \ldots, S_n^*\}$ such that each player (i) has its utility U_i, and for each strategy $S_i' \in S_i$,

$$U_i\left(S_i^*, S_{-i}^*\right) \geq U_i\left(S_i', S_{-i}^*\right), \tag{1}$$

where S_i^* is the best response of player (i), S_{-i}^* are the best responses of other players, and S_i is the set of strategies of player (i). In addition, we are dealing with a dynamic game with N players (nodes) playing a repeated game. The payoff of different profiles in strategic form is presented in (bimatrix) Table 2, with cooperate strategy denoted by C and not-cooperate strategy denoted by NC.

We use the strategic form because our game is considered as a simultaneous game, where both players can choose their strategies simultaneously.

Based on the matrix payoff (Table 2), if one of the two players chooses to cooperate and if the other player chooses not-cooperate strategy, thus, the payoff of the second player is improved from $(V-e)$ to (V). In addition, if one of the two players chooses not-cooperate strategy and the other player also chooses the same strategy, then, the payoff of the second player is decreased from $(V-e)$ to $(-r)$. Furthermore, we note that any strategy (cooperate or not-cooperate) cannot always offer a better utility to each player in different situations. Thus, a dominant or dominated strategy does not exist. However, in terms of stability, this game supports two Nash Equilibria (NE): $(V-e, V)$ and $(V, V-e)$. In both situations of NE, no player can profitably change its strategy. Furthermore, $(V-e, V-e)$ and $(-r, -r)$ cannot be NE because the two players would have an incentive to change their strategies. In this game, the two NE are considered as situations of stability but are not equitable, because only one of the two players can be rewarded. Additionally, the $(-r, -r)$ strategy profile is undesirable from the network context.

4.3.2. Mixed Strategy. A mixed strategy of a player (i) is a probability distribution σ_i defined upon all its pure strategies. Let us denote by $\sum_i$ all mixed strategies of player (i) and by σ_i a mixed strategy of this player.

A mixed strategy Nash Equilibrium is a mixed profile of strategies $\sigma^* \in \sum_i$, such that for each player (i) and for all $\sigma_i \in \sum_i$,

$$U_i\left(\sigma_i^*, \sigma_{-i}^*\right) \geq U_i\left(\sigma_i, \sigma_{-i}^*\right), \tag{2}$$

where σ_i^* is the best response of player (i) and σ_{-i}^* are the best responses of other players.

In the mixed strategy, and to analyze the outcome of the static game, each player chooses a strategy cooperate (C) with probability p (or q) and the other strategy, not-cooperate, with probability $(1-p)$ or $(1-q)$. Table 3 presents the payoff matrix of the two players in the mixed strategy.

Let us denote by $U_1(\mathrm{C})$ the average utility of player (1) when it chooses cooperate strategy. Thus, the average utility $U_1(\mathrm{C})$ can be written as

$$U_1(\mathrm{C}) = \left((V-e)\times p\right) + \left((V-e)\times\left(1-p\right)\right) = V-e. \tag{3}$$

Let us denote by $U_1(\mathrm{NC})$ the average utility of player (1) when it chooses not-cooperate strategy. Thus, the average utility $U_1(\mathrm{NC})$ can be written as

$$U_1(\mathrm{NC}) = \left(V\times p\right) + \left((-r)\times\left(1-p\right)\right). \tag{4}$$

At the mixed strategy Nash Equilibrium: $U_1(\mathrm{C}) = U_1(\mathrm{NC})$ (i.e., (3) = (4)). Then,

$$(V - e) = (V \times p) + ((-r) \times (1 - p)). \quad (5)$$

Equation (5) can be written as

$$(V - e) + r = p \times (V + r). \quad (6)$$

Therefore,

$$p = \frac{((V - e) + r)}{(V + r)}. \quad (7)$$

Thus, (7) can be written as

$$p^* = 1 - \left(\frac{e}{(V + r)}\right), \quad (8)$$

where p^* represents the probability at the mixed strategy Nash Equilibrium.

In this game, r represents a punishment that needs to penalize the players and encourage them to cooperate. In addition, if the value of r is very high (see infinity) the players will tend to cooperate in order to avoid this punishment. Therefore, we can calculate the limit of p^* when r approaches infinity ($r \to \infty$):

$$\lim_{r \to \infty} p^* = 1. \quad (9)$$

We can follow the same operations concerning player (2) because the game is symmetrical; therefore,

$$p^* = q^*. \quad (10)$$

Thus the mixed strategy (p^*, q^*) is a Nash Equilibrium.

However, in case of (N) players the situation can be considered as the volunteer's dilemma game [37, 38]. In addition, we can demonstrate that in such a situation the cooperation between nodes decreases.

Therefore, in this case and from Table 3, we can calculate the average utility of each player (i) depending on actions of other players. Thus, we will study two cases.

Case 1. Let us denote by $U_i(\mathrm{C})$ the average utility of player (i) if it chooses to cooperate. Then, we have to study two subcases.

Case 1.1. If at least one of the other players chooses to cooperate,

$$U_i(\mathrm{C}) = (V - e) \times \left(1 - (1 - p)^{(n-1)}\right), \quad (11)$$

where $(1 - (1 - p)^{(n-1)})$ is the probability that at least one of the other players chooses to cooperate.

Case 1.2. If no player chooses to cooperate,

$$U_i(\mathrm{C}) = (V - e) \times (1 - p)^{(n-1)}, \quad (12)$$

where $((1 - p)^{(n-1)})$ is the probability that no player chooses to cooperate.

Then, the average utility $U_i(\mathrm{C})$ of player (i) can be written as

$$U_i(\mathrm{C}) = (11) + (12). \quad (13)$$

So

$$U_i(\mathrm{C}) = \left((V - e) \times \left(1 - (1 - p)^{(n-1)}\right)\right) + \left((V - e) \times (1 - p)^{(n-1)}\right). \quad (14)$$

Equation (14) can be written as

$$U_i(\mathrm{C}) = (V - e). \quad (15)$$

Case 2. Let us denote by $U_i(\mathrm{NC})$ the average utility of player (i) if it chooses not-cooperate strategy. In this case we have to study two subcases as well.

Case 2.1. If at least one of the other players chooses to cooperate,

$$U_i(\mathrm{NC}) = \left(V \times \left(1 - (1 - p)^{(n-1)}\right)\right), \quad (16)$$

where $(1 - (1 - p)^{(n-1)})$ is the probability that at least one of the other players chooses to cooperate.

Case 2.2. If no player chooses to cooperate,

$$U_i(\mathrm{NC}) = (-r) \times (1 - p)^{(n-1)}, \quad (17)$$

where $((1 - p)^{(n-1)})$ is the probability that no player chooses to cooperate.

Then, the average utility $U_i(\mathrm{NC})$ of player (i) can be written as

$$U_i(\mathrm{NC}) = (16) + (17). \quad (18)$$

So

$$U_i(\mathrm{NC}) = \left(V \times \left(1 - (1 - p)^{(n-1)}\right)\right) + \left((-r) \times (1 - p)^{(n-1)}\right). \quad (19)$$

Equation (19) can be written as

$$U_i(\mathrm{NC}) = V - \left((V + r) \times (1 - p)^{(n-1)}\right). \quad (20)$$

At the mixed strategy Nash Equilibrium: $U_i(\mathrm{C}) = U_i(\mathrm{NC})$ (i.e., (15) = (20)). Thus,

$$(V - e) = V - \left((V + r) \times (1 - p)^{(n-1)}\right). \quad (21)$$

Equation (21) can be written as

$$(1 - p)^{n-1} = \frac{e}{(V + r)}. \quad (22)$$

So

$$(1 - p) = \left(\frac{e}{(V + r)}\right)^{(1/(n-1))}. \quad (23)$$

Therefore,

$$p = 1 - \left(\frac{e}{V+r}\right)^{1/(n-1)}. \quad (24)$$

So

$$p^* = 1 - \sqrt[(n-1)]{\left(\frac{e}{V+r}\right)}, \quad (25)$$

where p^* represents the probability at the mixed strategy Nash Equilibrium. In addition, we can follow the same operations concerning player (2) because the game is symmetrical; therefore,

$$p^* = q^*. \quad (26)$$

Thus, when the number of players is increased (i.e., when n approaches infinity) the limit of p^* when $n \to \infty$ is

$$\lim_{n\to\infty} p^* = 0. \quad (27)$$

Therefore, we notice that, in such a situation, where the number of players increases, the cooperation between nodes decreases as well and becomes more interesting to encourage nodes (players) to cooperate. In addition, we notice that the noncooperative strategy can offer a selfish player to take advantage of a cooperating player. Therefore, we must take into account a cooperative system to deal with this behavior and enforce cooperation between nodes. In addition, this cooperative system must offer each node (player) a reward for cooperating and impose a punishment on each node for not cooperating.

Thus, let us denote by $h(t)$ the cooperation utility (the cooperation history) of the ith player in the entire reputation game and in each stage or period t. The utility is the sum of its utilities in all stages. Additionally, let us denote by $\beta(t)$ the value added or subtracted periodically according to player behavior (cooperate or not-cooperate) during the game in order to update its $h(t)$. The cooperation rate (CR) of each player (i) is calculated using the following equation:

$$\mathrm{CR} = \sum \left(h(t) + \beta(t)\right). \quad (28)$$

In the next section, we propose a mathematical model where we formulate the calculation of the cooperation rate (CR).

5. System Model

5.1. Cooperation-Based Mechanism. In other similar game theory models which have been cited above in related work section, a reputation entity, such as the watchdog, is used to detect misbehaving nodes. In addition, and in every time a monitoring entity needs to monitor and verify the correct execution of a function. However, this mechanism is based on an assumption which is not always true and required more energy consumption. Moreover, many other game models are not adequate to OLSR routing protocol.

Concerning our proposed model, we have selected, for performance evaluation, the OLSR protocol that considers the stability of links. The key novelty of this model is to stimulate the cooperation between nodes in a MANET using the cooperation rate (CR) in order to prevent selfish behavior. Additionally, the CR value is calculated based on various types of specific OLSR messages (HELLO and topology control (TC)) and different network operations (forwarding and routing). In our proposal, the correct execution of a function is according to the player behavior: cooperate or not-cooperate (cooperate means to participate in packet forwarding and the exchange of OLSR messages (HELLO and TC) with reception of ACKs and not-cooperate means packet dropping). Thus, this process ensures the correct execution of an OLSR function.

In this paper, we propose a new strategy based on the game theory to enforce the cooperation between nodes by calculating a cooperation rate (CR) for each node. Additionally, this strategy has evaluated using OLSR messages (HELLO and TC) and different network processing (forwarding and routing). In the rest of this section, we propose a mathematical model where we formulate the calculation of the cooperation rate (CR).

In the rest of this section, we propose a mathematical model where we formulate the calculation of cooperation rate (CR). In this model, each node (j) can know the cooperation rate of a node (i) inside the network.

5.1.1. Cooperation Rate: CR. The cooperation rate (CR) of a node (i) in relation to its neighbors set is directly calculated from an observation of each node (j) which belongs to the neighbors set H_i of the node (i). The CR, at time interval t, is calculated using a weighted average of the observations' rating factors provided by nodes belonging to the neighbors set H_i of the node (i). Moreover, and in order to (i) reach a better evaluation of node behaviors, (ii) avoid incorrect detections due to connection breaks, (iii) and ensure that the nodes which are involuntary noncooperative due to their limited resources (energy levels, etc.) are not excluded from the network, we should take into consideration a minimal impact on the evaluation of the final cooperation value. In addition, the CR value is calculated periodically over a given time interval (t) that depends on the default time of OLSR messages exchanged between nodes. Therefore, in case of HELLO message the time interval is 2 seconds, in case of TC message the time interval is 5 seconds, and in case of a forwarding process it is directly calculated after the end of this process. Moreover, in this paper, the threshold is considered as the minimum value of the CR accepted by all rational nodes. We consider that each node which has a ($\mathrm{CR} > 0$) is considered as a legitimate node, whereas a node with ($\mathrm{CR} \leq 0$) is considered as a noncooperative node. Moreover, at the beginning of this algorithm, the cooperation rate of each node is initialized by zero. In addition, all newly joined nodes will have a CR which is initialized to zero as well.

The equation that permits calculating the CR of node (i) at time interval t and based on a network operation F is

$$\mathrm{CR}(i,t,F) = \sum \left(h(t) + \beta(t)\right), \quad (29)$$

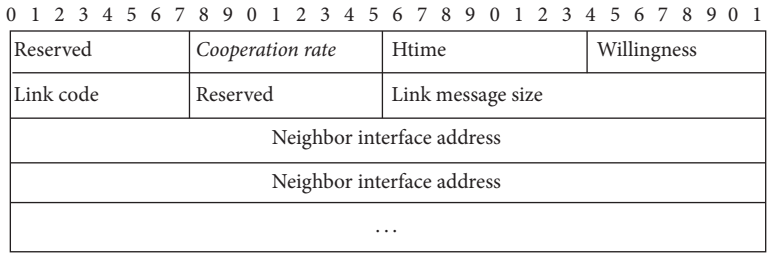

Figure 2: Enhanced HELLO message format.

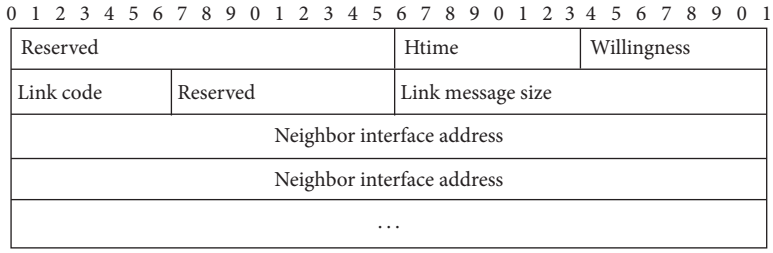

Figure 3: Standard HELLO message format.

where $\beta(t)$ is the value added or subtracted periodically according to node behavior (cooperate or not-cooperate) during the game.

$$\beta(t) = \begin{cases} \{+1, +2, +3, \ldots, +m\}: & \text{if the node cooperates} \\ -\text{last value added:} & \text{if the node does not cooperate} \end{cases} \quad (30)$$

(i) F is the network operation (TC and HELLO messages processing and forwarding processes).

(ii) $h(t)$ represents the cooperation rate (CR) record saved by a given node (i) in relation to another node (j). Also, it is a time dependent function that gives higher relevance to past values of CR. Additionally, (t) is used to update the CR according to node behavior (cooperate or not-cooperate) during the game in order to update its $h(t)$. Also, this value is influenced and depends on the observations' rating factors (other cooperation rates) provided, at time interval t, by other nodes belonging to neighbors set H_i of node (i).

5.1.2. Weighting Calculation. The cooperation rate depends on different network function F (HELLO and TC messages processing and forwarding processes). Therefore, during the calculation of the cooperation rate, we must take into account the impact of each function F according to its importance. In this way, and in order to calculate the weight W related to each function F, we use AHP (analytic hierarchy process) method [39, 40]. In AHP method, the decision process requires the execution of the following stages:

(1) Establish the main objective:

(i) Choose a processing function

(2) Define the criteria:

(i) Security, routing, and reliability

(3) Select options:

(i) HELLO message processing

(ii) TC messages processing

(iii) Forwarding processing

In our case, we consider that the security is the most important criterion, followed by routing process and reliability. The rest of the AHP process is very long, so we are going to present the results directly, and the CR of the node (i), which is presented in (29), can be written as follows:

$$\mathrm{CR}(i, t, F) = W \times \left\{ \sum \left(h(t) + \beta(t) \right) \right\}, \quad (31)$$

where (i) $W = 1.328$, if the function F is a TC processing. (ii) $W = 1.3060$, if the function F is a forwarding processing. (iii) $W = 1.2720$, if the function F is a HELLO message processing.

Moreover, each node must share its correct cooperation rate (CR) with other nodes using OLSR messages. We present in Figure 2 the enhanced format of HELLO message that contains the CR of the transmitter node, and the standard format is presented in Figure 3.

We present in Figure 4 the enhanced format of TC message that contains the CR of the transmitter node, and the standard format is presented in Figure 5.

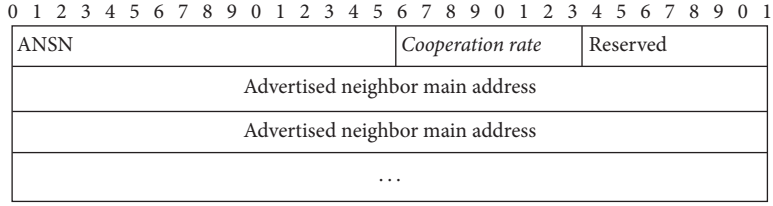

Figure 4: Enhanced TC message format.

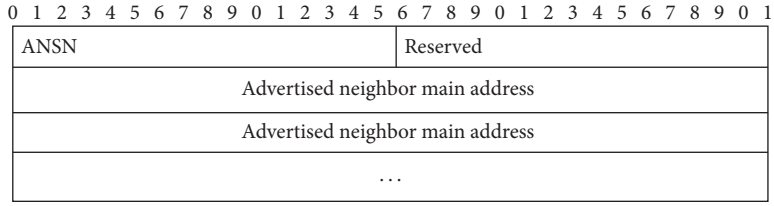

Figure 5: Standard TC message format.

6. Malicious Node Detection Algorithm

In this section, we propose an algorithm to detect and avoid malicious behavior based on CR value of all nodes across the network using the routing game approach during the routing tables computation.

6.1. Routing Game. The routing process requires cooperation between nodes for routing packets from other nodes. Therefore, the key novelty of this paper is to develop an algorithm based on game theory to enforce cooperation between nodes in order to avoid selfish and malicious nodes during the routing process. However, the existence of malicious nodes in this area threatens cooperation and influences network performances (routing control, lifetime, etc.) as denoted in Figure 6. Additionally, each node (player) tries to reach the following objectives: it tries to maximize its utility function, minimize a path cost function, or find an optimal and secure routing path. In the game theory, these objectives have been addressed in what is known as the routing game. Moreover, in each routing process, every node chooses its path and updates its strategy in terms of its utility function and the action it has chosen.

We represent our routing game model using an undirected graph $G(V, E)$, where

(i) V is the set of nodes or vertices,

(ii) E is the set of arcs (link) between nodes,

(iii) N denotes all players (nodes), where $N = \{1, 2, \ldots, n\}$,

(iv) any player $(n) \in N$ is characterized by the following information:

(1) $\mathrm{CR}(n)$ is utility or cooperation rate.

(2) A pair of vertices $(S_i, T_i) \in (V \times V)$ which represents its source and destination, respectively.

(3) $P_n \subset E$ is set of the shortest paths ranging from source S_i to destination T_i with cardinality m_i.

Table 4: Enhanced routing table format.

Destination address	Next address	Next interface	Cooperation rate

(4) A strategy space S = {C: cooperate; NC: not-cooperate} indexed on the set P_n.

(5) For each path $(i, j) \in P_n$,

$$F_n(i, j) = \sum_{l=1}^{M} \mathrm{CR}_{(l)}, \tag{32}$$

where (32) represents the utility function F of the player (n) in relation to the path (i, j) which belongs to P_n and is based on CR values of M nodes belonging to this path. In addition, and in case of multiple choice, each node chooses the path with greater value of this utility function F.

The routing table computation is an essential process in OLSR protocol. Therefore, and in order to avoid communication with malicious nodes which may act as routers or gateways, the calculated cooperation rate (CR) must be integrated in the routing table as a new metric in parallel with other information (destination address, next address, and next interface) to establish secure routes between nodes. In this way, we propose a new routing table shape as mentioned in Table 4.

6.2. Enhanced Routing Table Algorithm. In this section, we present a brief description of our enhanced routing table algorithm that provides the solution to avoid selfish nodes.

BEGIN

(1) Based on modified HELLO message with the cooperation rate of nodes, control all one-hop nodes.

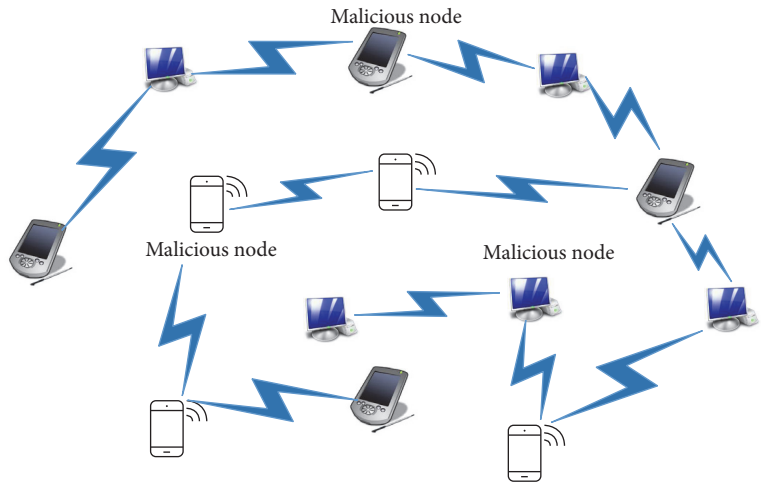

Figure 6: Network routing as a game in MANET.

(2) Add appropriate entries for each node to its routing table using its one-hop table.

(3) Update entries of routing table with the topology set.

(4) Keep recursively, for each node, its last address until attaining the destination.

(5) Based on modified TC message with the cooperation rate of nodes, save all path information in the routing table.

(6) Delete the loop entries, if any.

(7) For each node across the network select all paths of a given source-destination.

(8) Evaluate the behavior of each node based on CR to avoid selfish nodes on each path.

(9) Get the CR of each node on each path.

(10) For each node (n), calculate the utility function $F_n(i, j)$ on each selected path (i, j) using (32).

(11) Find out the maximum utility function F on each selected path.

(12) Use this selected path.

END

In the next subsection, we present an example to give a walk through example to explain our malicious node detection algorithm.

6.3. Proposed Example. In this example which is presented in Figure 7, we propose a MANET with six nodes, where the source node (1) tries to send packets to its destination node (6). After (i) calculating the cooperation rate of each node as mentioned in Tables 5, 6, 7, 8, and 9, (ii) sharing this value between all nodes using HELLO and TC messages, and (iii) introducing this value on routing tables, the source node (1) must choose one short path among the two possibilities to avoid malicious nodes. Therefore, the source node (1) must

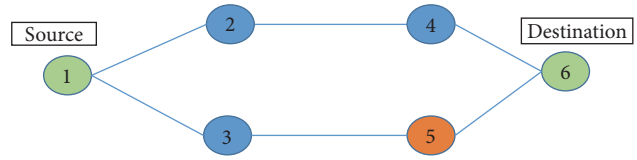

Figure 7: A sample MANET network with six nodes as routing game.

calculate its utility function in relation to the path (1, 2 4, 6) and path (1, 3, 5, 6) based on CR values of the nodes belonging to these paths. In addition, the source node will choose the path with greater value of this utility function F. In this example, we propose that the calculating of cooperation rate is made after five iterations needed to exchange OLSR messages (HELLO and TC). Additionally, we suppose that node (5) is considered as a malicious node and does not cooperate with other nodes.

In this example, we suppose that iteration 1 means that node (2) and node (1) exchange the HELLO message and both of them received a reply (the ACK); it means also that the link between them is symmetric. Therefore, the CR of node (2) in relation to node (1), which is initialized by zero, will be updated by adding 1. In addition, these nodes will exchange the HELLO message in the second iteration, and both of them received the ACK and the CR will be updated by adding 2. Furthermore, the nodes will exchange the TC message in iteration 3 and the CR will be updated again by adding 3 and so on.

$$\begin{aligned} \mathrm{CR}\left(\frac{2}{1}\right) &= 15, \\ \mathrm{CR}\left(\frac{2}{4}\right) &= 15, \\ \text{then } \mathrm{CR}(2) &= \mathrm{CR}\left(\frac{2}{1}\right) + \mathrm{CR}\left(\frac{2}{4}\right) = 30. \end{aligned} \tag{33}$$

Table 5: Cooperation rate of node (2) in relation to nodes (1) and (4).

	Node (1)	Node (4)
Node (2): iteration 1	+1 (ACK is received)	+1 (ACK is received)
Node (2): iteration 2	+2 (ACK is received)	+2 (ACK is received)
Node (2): iteration 3	+3 (ACK is received)	+3 (ACK is received)
Node (2): iteration 4	+4 (ACK is received)	+4 (ACK is received)
Node (2): iteration 5	+5 (ACK is received)	+5 (ACK is received)

Table 6: Cooperation rate of node (4) in relation to nodes (2) and (6).

	Node (2)	Node (6)
Node (4): iteration 1	+1 (ACK is received)	+1 (ACK is received)
Node (4): iteration 2	+2 (ACK is received)	+2 (ACK is received)
Node (4): iteration 3	+3 (ACK is received)	+3 (ACK is received)
Node (4): iteration 4	+4 (ACK is received)	+4 (ACK is received)
Node (4): iteration 5	+5 (ACK is received)	+5 (ACK is received)

Table 7: Cooperation rate of node (3) in relation to nodes (1) and (5).

	Node (1)	Node (5)
Node (3): iteration 1	+1 (ACK is received)	+1 (ACK is received)
Node (3): iteration 2	+2 (ACK is received)	+2 (ACK is received)
Node (3): iteration 3	+3 (ACK is received)	−2 (ACK is not received)
Node (3): iteration 4	+4 (ACK is received)	−1 (ACK is not received)
Node (3): iteration 5	+5 (ACK is received)	−1 (ACK is not received)

Table 8: Cooperation rate of node (5) in relation to nodes (3) and (6).

	Node (3)	Node (6)
Node (5): iteration 1	+1 (ACK is received)	+1 (ACK is received)
Node (5): iteration 2	+2 (ACK is received)	+2 (ACK is received)
Node (5): iteration 3	−2 (ACK is not received)	−2 (ACK is not received)
Node (5): iteration 4	−1 (ACK is not received)	−1 (ACK is not received)
Node (5): iteration 5	−1 (ACK is not received)	−1 (ACK is not received)

Thus, the same situation can be considered for other nodes and we can follow the same operations as mentioned in Tables 6, 7, 8, and 9.

Calculating the cooperation rate of node (4) in relation to nodes (2) and (6):

$$\begin{aligned} &\mathrm{CR}\left(\frac{4}{2}\right) = 15, \\ &\mathrm{CR}\left(\frac{4}{6}\right) = 15, \\ &\text{then } \mathrm{CR}(4) = \mathrm{CR}\left(\frac{4}{2}\right) + \mathrm{CR}\left(\frac{4}{6}\right) = 30. \end{aligned} \tag{34}$$

Concerning the cooperation rate of node (5), which is considered in this example as malicious node, we suppose that this node and other nodes will exchange the HELLO and TC messages during iterations (1) and (2). Additionally, the CR of node (5), which is initialized by zero, will be updated by adding 1 in the first iteration and by 2 in the second. However, we suppose that node (5) chooses not-cooperate with other nodes from iteration 3 (to save its energy); it means that this node will not send HELLO and TC messages. Therefore, when the other nodes do not receive these messages (it means that the ACK is not received) from node (5), then they will start by subtracting the last value added, which is 2, in iteration 3 and by subtracting 1 in iteration 4. Additionally, when the CR is equal to zero, it will be updated by subtracting 1 and so on.

Calculating of the cooperation rate of node (3) in relation to nodes (1) and (5):

$$\begin{aligned} &\mathrm{CR}\left(\frac{3}{1}\right) = 15, \\ &\mathrm{CR}\left(\frac{3}{5}\right) = -1, \\ &\text{then } \mathrm{CR}(3) = \mathrm{CR}\left(\frac{3}{1}\right) + \mathrm{CR}\left(\frac{3}{5}\right) = 14. \end{aligned} \tag{35}$$

Table 9: Cooperation rate of node (6) in relation to nodes (4) and (5).

	Node (4)	Node (5)
Node (6): iteration 1	+1 (ACK is received)	+1 (ACK is received)
Node (6): iteration 2	+2 (ACK is received)	+2 (ACK is received)
Node (6): iteration 3	+3 (ACK is received)	−2 (ACK is not received)
Node (6): iteration 4	+4 (ACK is received)	−1 (ACK is not received)
Node (6): iteration 5	+5 (ACK is received)	−1 (ACK is not received)

Calculating of the cooperation rate of node (5) in relation to nodes (3) and (6):

$$\begin{aligned} &\mathrm{CR}\left(\frac{5}{3}\right) = -1, \\ &\mathrm{CR}\left(\frac{5}{6}\right) = -1, \\ &\text{then } \mathrm{CR}(5) = \mathrm{CR}\left(\frac{5}{3}\right) + \mathrm{CR}\left(\frac{5}{6}\right) = -2. \end{aligned} \tag{36}$$

Calculating of the cooperation rate of node (6) in relation to nodes (4) and (5):

$$\begin{aligned} &\mathrm{CR}\left(\frac{6}{4}\right) = 15, \\ &\mathrm{CR}\left(\frac{6}{5}\right) = -1, \\ &\text{then } \mathrm{CR}(6) = \mathrm{CR}\left(\frac{6}{4}\right) + \mathrm{CR}\left(\frac{6}{5}\right) = 14. \end{aligned} \tag{37}$$

Thus, when the cooperation rate of node (5) will be shared, all nodes must detect that (CR(5) < 0) according to threshold, proposed in this paper, the nodes will handle this node as a noncooperative node. Therefore, the utility function F of node (1) in relation to the path (1, 2, 4, and 6) is

$$\begin{aligned} F_1(1,6) &= \sum_{l=1}^{M} \mathrm{CR}_{(2)} = \mathrm{CR}(2) + \mathrm{CR}(4) = 30 + 30 \\ &= 60. \end{aligned} \tag{38}$$

The utility function F of the node (1) in relation to the path (1, 3, 5, and 6) is

$$\begin{aligned} F_1(1,6) &= \sum_{l=1}^{M} \mathrm{CR}_{(2)} = \mathrm{CR}(3) + \mathrm{CR}(5) = 14 + (-2) \\ &= 12. \end{aligned} \tag{39}$$

Therefore, the source node (1) will choose the first path with the greater value of its utility function F in order to send packets to its destination which is node (6).

7. Simulation Environment

Our proposal is evaluated using Network Simulator 3 (NS-3.17) [41] that contains the OLSR module. In this work, we implement our algorithm and compare it with the original routing table algorithm described in the standard OLSR. In addition, we compare our proposal with a selfish OLSR where nodes choose to drop packets rather than forwarding them to their destinations. During all simulations, the network contains a variable number of mobile nodes and moving in a fixed area. We used the Random WayPoint (RWP) mobility model with pause time fixed to 0 seconds, various random seeds, and max speed of 20 meters/second. The choice of the simulation parameters can be justified by many scenarios of MANET applications such as military fields and conferencing. Additionally, and concerning the mobility, RWP seems to be an arduous environment to evaluate the effectiveness of our proposal. Moreover, our proposed model, original OLSR, and selfish OLSR protocols are evaluated based on the same mobility scenarios that define the nodes movement. Furthermore, in this experimental study, we conducted exhaustive simulations and Table 10 recapitulates all the simulation parameters.

Table 10: Simulation parameters.

Parameter	Value
Routing protocol	OLSR
Simulation time	300 seconds
Number of nodes	20, 40, 60, 80, and 100
Number of selfish nodes	50% of the number of nodes in selfish OLSR
Environment area	1000 meters × 1000 meters
The transmit power	7.5 dBm.
MAC protocol	IEEE 802.11
Transport layer	User Datagram Protocol (UDP)
Pause time	0 seconds
Maximum speeds	20 meters/second
Network Simulator	NS3.17
Mobility model	Random WayPoint

7.1. Performance Metrics. The main objective of the experiments using Network Simulator 3 (3.17) is to evaluate and validate our proposal by analyzing and addressing the following performance metrics.

(i) Energy is the metric used to quantify and evaluate the lifetime of nodes and network.

(ii) Throughput is the number of messages successfully delivered per time unit.

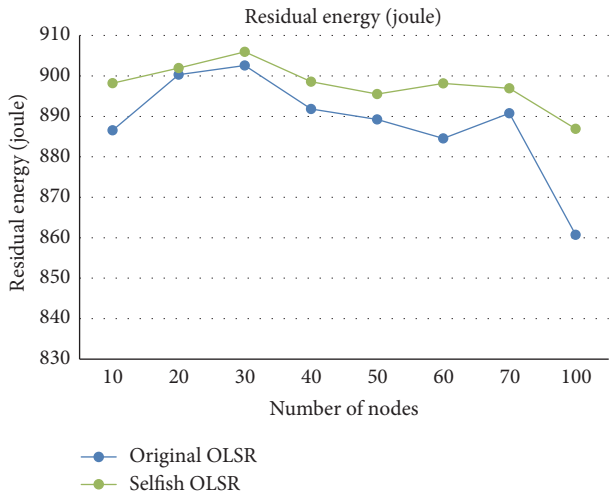

Figure 8: The residual energy in original OLSR and selfish OLSR.

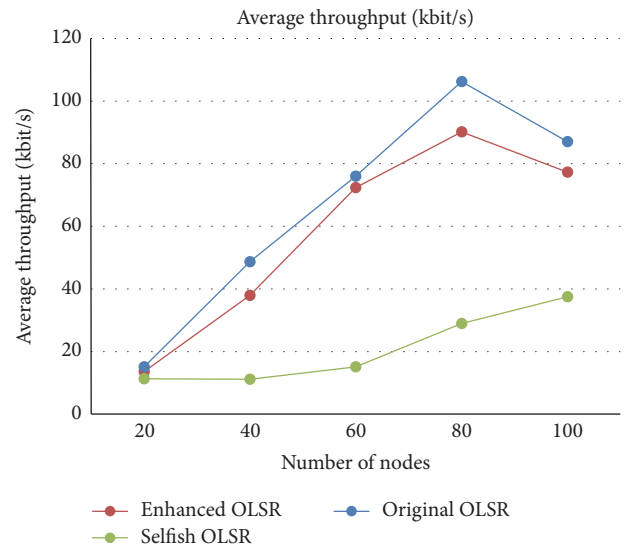

Figure 9: The average of throughput in enhanced OLSR, original OLSR, and selfish OLSR.

(iii) End-to-end delay is the time interval between the transmission of a packet and its reception.

(iv) Total packets forwarded are the total traffic and packets received and forwarded by nodes across the network

(v) Packets received are the successful packets transmitted to their destination.

8. Analytical Results

In this section we are going to compare between three variants of protocol: original OLSR, enhanced OLSR, and selfish OLSR.

Figure 8 shows the evolution of the residual energy in relation to the number of nodes. We can observe the impact of selfish behavior on energy consumption and the difference between original OLSR and selfish OLSR protocols. Furthermore, we notice that malicious nodes are able to save energy when they refuse to cooperate for routing packets from other nodes because these operations require most energy consumption. Therefore, the rational nodes need to do more work to compensate the job of selfish nodes and then spend more energy to complete this task.

In Figure 9, we observe the evolution of throughput as function of the number of nodes in different variants of OLSR. It is evident that the throughput in case of original OLSR is high compared to the selfish OLSR. We interpret the results by the existence of malicious nodes that choose to drop packets rather than forwarding them to their destinations. Therefore, this behavior can affect the throughput by the retransmission of the lost packets by rational nodes. In another observation, we notice that the throughput in case of enhanced OLSR is high compared to the selfish OLSR. This improvement can be justified because the packets discarded by the malicious nodes are decreased in enhanced OLSR using malicious detection algorithm. Furthermore, through our proposal, we can get almost the same performances and mitigate the aggregate effect in case of existence of malicious nodes compared to the original protocol.

In Figure 10, we observe the evolution of end-to-end delay (ETED) in relation to the number of nodes in the three variants of OLSR. In addition, we notice the impact of selfish nodes on ETED compared to the original and enhanced OLSR. The results concerning ETED in original and enhanced OLSR can be justified because the number of nodes that participate in the routing process is increased. Moreover, in OLSR routing protocol, the ETED depends on the routing process and the number of nodes involved. On the contrary, in the selfish OLSR and in our situation we are interested only in ETED of packets which are successfully transmitted. Additionally, most of the packets cannot reach their destinations due to the selfish nodes that choose to drop any packets that pass on instead of forwarding them to their destinations. Therefore, and owing to the large number of selfish nodes, the ETED must be less than the original and enhanced OLSR. On the other hand, our proposal can offer nearly the same performance compared to the original OLSR. Furthermore, and due to the impact of some packet collision, noise transmission, and the processing time that is needed to calculate CR, our solution provides an ETED which is less effective than the original OLSR.

In Figure 11, we observe the evolution of the total packets forwarded (TPF) as function of the number of nodes in original OLSR, selfish OLSR, and enhanced OLSR. We notice that the TPF is high in original and enhanced OLSR compared to selfish OLSR. Moreover, we interpret this result by the existence of malicious nodes that attempt to reduce network connectivity and undermine the network security. In addition, the impact of selfish behavior is due to the malicious nodes that choose to drop packets received instead of forwarding them to their destinations. Therefore, the TPF must be high in original and enhanced OLSR using malicious node detection mechanism. Furthermore, we interpret the

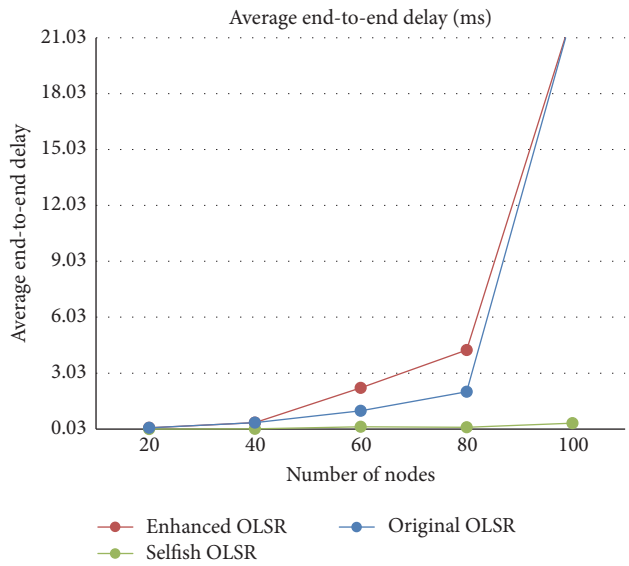

Figure 10: The average of end-to-end delay in enhanced OLSR, original OLSR, and selfish OLSR.

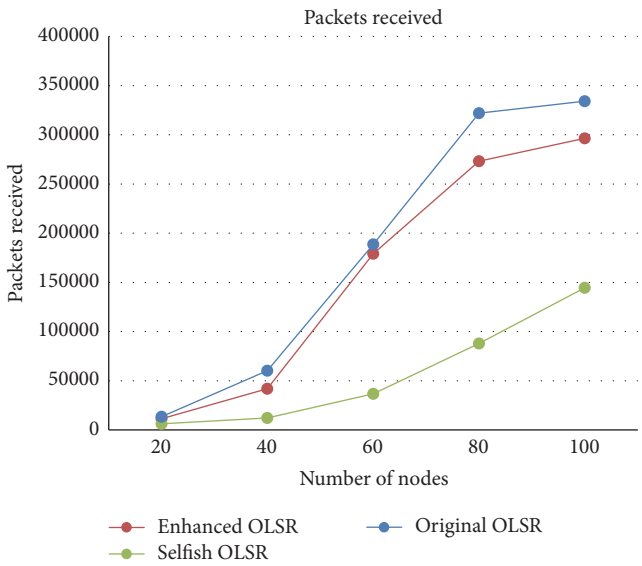

Figure 12: The average of packets received in enhanced OLSR, original OLSR, and selfish OLSR.

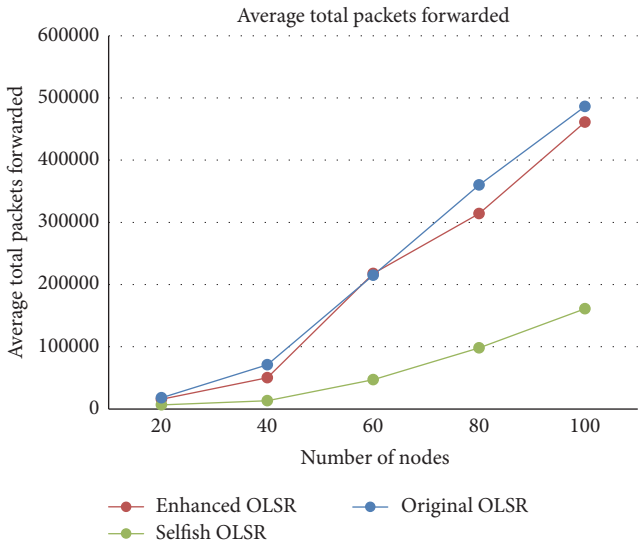

Figure 11: The average of packets forwarded in enhanced OLSR, original OLSR, and selfish OLSR.

difference between original OLSR and enhanced OLSR due to the impact of some packet collision and noise transmission during the calculation of CR.

In Figure 12, we observe the evolution of packets received in relation to the number of nodes concerning the three variants of OLSR. From this figure, we notice that the number of packets received is high in original OLSR and enhanced OLSR compared to selfish OLSR. This result is due to the malicious nodes that choose to drop packets received rather than forwarding them to their destinations. Therefore, this behavior should influence the number of received packets. In addition, the result in this figure shows the effectiveness of our proposal using malicious node detection mechanism and reinforces the result mentioned above concerning the total packets forwarded in Figure 11.

9. Conclusion and Future Work

In this paper, we have proposed a new idea based on a game theoretic approach to enhance OLSR security mechanism in MANETs. This proposal can be used to model interactions between selfish nodes and a large number of legitimate nodes inside the network. Contrary to some existing research on security in MANETs that rely on the game theory, the proposed solution can enable each node to evaluate behaviors of other nodes. Furthermore, the rational nodes can intelligently choose their strategies to deal with selfish behavior when each node keeps track of the cooperation rate (CR) record of other nodes. Moreover, many parameters (throughput, end-to-end delay, total packets forwarded, and packets received) can be improved significantly and the aggregate effect of selfish nodes can be reduced as well. In addition, the simulation results have shown that our proposed solution scheme takes into account, in addition to the security requirements, the system resources. Furthermore, in this paper we have proved that our proposal can be used as a security mechanism in order to enforce the cooperation between nodes, improve network performances, and prevent malicious nodes. However, the comparison with other game theory models can enhance the efficiency of this proposed solution. Therefore, and as future works,

(i) we plan to study and address other game models especially those treating OLSR routing protocol in order to compare our proposed solution with these models,

(ii) additionally, the cooperation rate is not the unique parameter to evaluate node behavior. For this, and as future work, we plan to improve this model to support

other parameters like the overload of the path and the energy consumption of the nodes constituting the path. Moreover, and in order to optimize the energy consumption, we will change the interval t needs to calculate the cooperation rate. Therefore, instead of using HELLO interval which is 2 seconds we will use 6 seconds, that is, after receiving three HELLO messages, and instead of using TC interval which is 5 seconds we will use 10 seconds, that is, after receiving two TC messages.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "A study of a routing attack in OLSR-based mobile ad hoc networks," *International Journal of Communication Systems*, vol. 20, no. 11, pp. 1245–1261, 2007.

[2] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "EAACKA secure intrusion-detection system for MANETs," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1089–1098, 2013.

[3] S. Djahel, F. Nait-Abdesselam, and Z. H. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 658–672, 2011.

[4] A. Nadeem and M. P. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2027–2045, 2013.

[5] N. Lal, K. Shishupal, S. Aditya, and V. K. Chaurasiya, "Detection of malicious node behaviour via I-watchdog protocol in mobile Ad Hoc network with DSDV routing scheme," *Procedia Computer Science*, vol. 49, pp. 264–273, 2015.

[6] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," IETF, RFC 3626, 2003.

[7] F. Wu, T. Chen, S. Zhong, C. Qiao, and G. Chen, "A game-theoretic approach to stimulate cooperation for probabilistic routing in opportunistic networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 4, pp. 1573–1583, 2013.

[8] E. Karami and S. Glisic, "Joint optimization of scheduling and routing in multicast wireless ad hoc networks using soft graph coloring and nonlinear cubic games," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 7, pp. 3350–3360, 2011.

[9] J. Liu, X. Jiang, H. Nishiyama, R. Miura, N. Kato, and N. Kadowaki, "Optimal forwarding games in mobile Ad Hoc networks with two-hop f-cast relay," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 11, pp. 2169–2179, 2012.

[10] 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*, J. B. Blazic and T. Klobucar, Eds., pp. 107–121, Springer, New York, NY, USA, 2002.

[11] M. Mejia, N. Peña, J. L. Muñoz, O. Esparza, and M. A. Alzate, "A game theoretic trust model for on-line distributed evolution of cooperation inMANETs," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 39–51, 2011.

[12] M. A. Elfaki, H. Ibrahim, A. Mamat, M. Othman, and H. Safa, "Collaborative caching priority for processing requests in MANETs," *Journal of Network and Computer Applications*, vol. 40, no. 1, pp. 85–96, 2014.

[13] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "A survey of collaborative services and security-related issues in modern wireless Ad-Hoc communications," *Journal of Network and Computer Applications*, vol. 45, pp. 215–227, 2014.

[14] H. Amraoui, A. Habbani, and A. Hajami, "CCS: a correct cooperation strategy based on game theory for MANETS," in *Proceedings of the IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA '14)*, pp. 326–332, 2014.

[15] P. Michiardi and R. Molva, "Analysis of coalition formation and cooperation strategies in mobile ad hoc networks," *Ad Hoc Networks*, vol. 3, no. 2, pp. 193–219, 2005.

[16] S. Zhong and F. Wu, "A collusion-resistant routing scheme for noncooperative wireless Ad Hoc networks," *IEEE/ACM Transactions on Networking*, vol. 18, no. 2, pp. 582–595, 2010.

[17] Z. Li and H. Shen, "Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 8, pp. 1287–1303, 2012.

[18] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1616–1627, 2014.

[19] S.-K. Ng and W. K. G. Seah, "Game-theoretic approach for improving cooperation in wireless multihop networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 40, no. 3, pp. 559–574, 2010.

[20] T. Chen, F. Wu, and S. Zhong, "FITS: a finite-time reputation system for cooperation in wireless ad hoc networks," *IEEE Transactions on Computers*, vol. 60, no. 7, pp. 1045–1056, 2011.

[21] M. Kaliappan and B. Paramasivan, "Enhancing secure routing in mobile ad hoc networks using a dynamic bayesian signalling game model," *Computers and Electrical Engineering*, vol. 41, pp. 301–313, 2015.

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

[23] Y. Wu, S. Tang, P. Xu, and X.-Y. Li, "Dealing with selfishness and moral hazard in noncooperative wireless networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 420–434, 2010.

[24] I. Khalil and S. Bagchi, "Stealthy attacks in wireless ad hoc networks: detection and countermeasure," *IEEE Transactions on Mobile Computing*, vol. 10, no. 8, pp. 1096–1112, 2011.

[25] W. Wang, H. Man, and Y. Liu, "A framework for intrusion detection systems by social network analysis methods in ad hoc networks," *Security and Communication Networks*, vol. 2, no. 6, pp. 669–685, 2009.

[26] T. P. Gondaliya and M. Singh, "Intrusion detection system on MAC layer for attack prevention in MANET," in *Proceedings of the 4th International Conference on Computing, Communications and Networking Technologies (ICCCNT '13)*, pp. 1–5, Tiruchengode, India, July 2013.

[27] A. Nadeem and M. P. Howarth, "An intrusion detection & adaptive response mechanism for MANETs," *Ad Hoc Networks*, vol. 13, pp. 368–380, 2014.

[28] K. R. Abirami, M. G. Sumithra, and J. Rajasekaran, "An enhanced intrusion detection system for routing attacks in MANET," in *Proceedings of the International Conference on Advanced Computing and Communication Systems (ICACCS '13)*, pp. 1–6, Coimbatore, India, December 2013.

[29] K. Wang and H. Guo, "An improved routing algorithm based on social link awareness in delay tolerant networks," *Wireless Personal Communications*, vol. 75, no. 1, pp. 397–414, 2014.

[30] K. Wang, Z. Ouyang, R. Krishnan, L. Shu, and L. He, "A game theory-based energy management system using price elasticity for smart grids," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1607–1616, 2015.

[31] K. Wang and M. Wu, "Nash equilibrium of node cooperation based on metamodel for MANETs," *Journal of Information Science and Engineering*, vol. 28, no. 2, pp. 317–333, 2012.

[32] K. Wang and M. Wu, "Cooperative communications based on trust model for mobile ad hoc networks," *IET Information Security*, vol. 4, no. 2, pp. 68–79, 2010.

[33] P. K. Dutta, *Strategies and Games Theory and Practice*, MIT Press, 2001.

[34] M. Le Treust and S. Lasaulce, "A repeated game formulation of energy-efficient decentralized power control," *IEEE Transactions on Wireless Communications*, vol. 9, no. 9, pp. 2860–2869, 2010.

[35] Y. Xiao, J. Park, and M. Van Der Schaar, "Repeated games with intervention: theory and applications in communications," *IEEE Transactions on Communications*, vol. 60, no. 10, pp. 3123–3132, 2012.

[36] S. lasaulce and H. Tembine, *Game Theory and Learning for Wireless Networks: Fundamentals and Applications*, Academic Press, New York, NY, USA, 2011.

[37] A. Diekmann, "Volunteer's dilemma," *Journal of Conflict Resolution*, vol. 29, no. 4, pp. 605–610, 1985.

[38] A. Diekmann, "Cooperation in an asymmetric volunteer's dilemma game theory and experimental evidence," *International Journal of Game Theory*, vol. 22, no. 1, pp. 75–85, 1993.

[39] W. L. Eddie and H. L. Cheng, "Analytic hierarchy process: an approach to determine measures for business performance," *Measuring Business Excellence*, vol. 5, no. 3, pp. 30–37, 2001.

[40] T. L. Saaty, *The Analytic Hierarchy Process*, McGraw-Hill, New York, NY, USA, 1980.

[41] "The network simulator NS-3," https://www.nsnam.org/.