Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2016, Article ID 4289176, 13 pages
http://dx.doi.org/10.1155/2016/4289176

Research Article

Detecting and Mitigating Smart Insider Jamming Attacks in MANETs Using Reputation-Based Coalition Game

Ashraf Al Sharah, Taiwo Oyedare, and Sachin Shetty

Department of Electrical and Computer Engineering, Tennessee State University, Nashville, TN 37209, USA

Correspondence should be addressed to Ashraf Al Sharah; aalshara@my.tnstate.edu

Received 15 January 2016; Accepted 22 March 2016

Academic Editor: Eduardo da Silva

Security in mobile ad hoc networks (MANETs) is challenging due to the ability of adversaries to gather necessary intelligence to launch insider jamming attacks. The solutions to prevent external attacks on MANET are not applicable for defense against insider jamming attacks. There is a need for a formal framework to characterize the information required by adversaries to launch insider jamming attacks. In this paper, we propose a novel reputation-based coalition game in MANETs to detect and mitigate insider jamming attacks. Since there is no centralized controller in MANETs, the nodes rely heavily on availability of transmission rates and a reputation for each individual node in the coalition to detect the presence of internal jamming node. The nodes will form a stable grand coalition in order to make a strategic security defense decision, maintain the grand coalition based on node reputation, and exclude any malicious node based on reputation value. Simulation results show that our approach provides a framework to quantify information needed by adversaries to launch insider attacks. The proposed approach will improve MANET's defense against insider attacks, while also reducing incorrect classification of legitimate nodes as jammers.

1. Introduction

Mobile ad hoc networks (MANETs) are self-organized networks which require distributed, reliable, and flexible networks which provide interdependency and rational decision-making. MANETs are vulnerable to jamming attacks due to the shared nature of the wireless medium. There are two main categories of jamming attacks: external jamming and internal/insider jamming. Several research efforts [1–4] have focused on external jamming attacks. This type of attack is launched by foreign adversary that is not privy to network secrets such as the network's cryptographic credentials and the transmission capabilities of individual nodes of the network. These types of attacks could be relatively easier to counter through some cryptography based techniques, some spread spectrum methodology such as Frequency-Hopping Spread Spectrum (FHSS) [5] and Direct Sequence Spread Spectrum (DSSS) [5, 6], Ultrawide Band Technology (UWB) [7], Antenna Polarization, and directional transmission methods [8].

Smart insider attacks on the other hand are much more sophisticated in nature because they are launched from a compromised node that belongs to the network. The attacker exploits the knowledge of network secrets it has gathered to adaptively target critical network functions. This makes it very hard for legitimate nodes to restore a new communication channel securely.

Owing to the manner of interaction between nodes in a network, game theory has been extensively used to solve interesting research problems facing MANETs. This game is broadly categorized as cooperative and noncooperative games. A cooperative game is played between nodes who have mutual relationship with each other while the noncooperative game is played between nodes that do not seem to coexist mutually. There have been several efforts on using noncooperative games to model security in wireless networks [9–12]. To the best of our knowledge, little work has been done in using cooperative or coalitional games to ensure security in MANETs. Coalition game is a form of cooperative game that is formed when more than two nodes agree to form an alliance in order to achieve a better probability of success. The cooperation of nodes in the network is dependent on individual node's experience and previous history records it

has gathered. Individual nodes in themselves tend to be weak against attacks but could achieve higher level of security when they form a coalition.

In this paper, we present a reputation-based coalition game-theoretic approach to detect and mitigate insider attacks on MANETs. In our approach, nodes implement reputation mechanism based on transmission rates. Reputation of a node is the collection of ratings maintained by other nodes about the given node [13]. The reputation mechanism can be first hand or second hand depending on whether the reputation values are collected directly or relayed. The choice of first hand versus second hand will impact the reliability of the reputation values. We adopt first-hand reputation because nodes within the transmission range are best equipped to provide reliable information [13, 14].

Different from existing works [15, 16] which made use of an alibi-based protocol and a self-healing protocol, respectively, to either detect or recover from a jamming attack, we make use of a reputation-based coalition game to ensure security in the network. These approaches are too generalized and might not be implementable for a mobile ad hoc network for which our system is modeled. Our model, instead, follows a game-theoretic approach by (1) implementing a coalition formation algorithm, (2) maintaining the coalition via a reputation mechanism, (3) identifying the insider attackers by setting up a reputation threshold, and (4) excluding the attackers from the coalition by rerouting their paths and randomly changing their channel of transmission. This method is fully distributed and does not rely on any trusted central entity to operate at optimal performance.

The rest of this paper is organized as follows: in Section 2, we presented relevant works that are closely related to our approach; in Section 3, we presented the network and jammer model; Section 4 describes the proposed defense model; in Section 5, we provide the simulation and result of the model; and, finally in Section 6, we conclude and present future work.

2. Related Work

Previous researches have devoted great efforts to security in mobile ad hoc networks. There is a plethora of works that have used other techniques besides game theory to prevent security attacks in MANETs. Li et al. [16] designed a protocol to protect self-healing wireless networks from insider jamming attacks. The protocol is not applicable to MANET as the pairwise key design in the protocol works best in a centralized system. Some other works have only focused on node selfishness and not on intentional malicious acts or jamming attacks.

Marti et al. [17] categorized nodes according to a dynamically measured behavior; a watchdog mechanism identifies the misbehaving nodes and a path-rater mechanism helps the routing protocols avoid these nodes. The research showed that the two mechanisms make it possible to maintain the total throughput of the network at an acceptable level, even in the presence of a high amount of misbehaving nodes. However, the operation of the watchdog is based on an assumption which is not always true, the promiscuous node of the wireless interface. Also, the selfishness of the node does not seem to be castigated by both the watchdog and path-rater mechanisms; in other words, the misbehaving nodes still enjoy the possibility of generating and receiving traffic.

Also, Michiardi and Molva [18] have used a reputation mechanism they termed CORE which is an acronym for collaborative reputation mechanism. They suggested a generic mechanism based on reputation to enforce cooperation among the nodes of a MANET to prevent selfish behavior. The only challenge with this mechanism is that it would only work for node selfishness whereas there is a greater risk of service denial in malicious nodes attacks. Furthermore, reputation mechanism was also used by Cheng and Friedman in P2P networks where the notion of Sybil proofness was formalized using static graph formulation of reputation [19]. According to the authors, this model cannot be generalized because reputation functions did not depend on the state of the network at previous time steps as well as the current state of the network. Buchegger and Le Boudec [20] described the use of a self-policing mechanism based on reputation to enable mobile ad hoc networks to keep functioning despite the presence of misbehaving nodes. They explained how second-hand information is used while mitigating contamination by spurious ratings. Their survey pointed out that a reputation system is effective as long as the number of misbehaving nodes is not too large.

Other works have used noncooperative games to model security scenarios as well as the corresponding defense strategies to such attacks [13, 21–25]. Most of these works focused on two-player games where all legitimate nodes are modeled as a single node and attacker nodes are also modeled as a single node too; this is only valid for centralized networks, whereas MANETs are self-organized networks. Thamilarasu and Sridhar formulated jamming as a two-player, noncooperative game to analyze the interaction between attackers and monitoring nodes in the network. The mixed strategy Nash Equilibrium was computed while the optimal attack and detection strategies were derived [22].

Researchers have also used cooperative game theory in the form of coalition game to ensure security in MANETs. Majority of their works have only focused on node selfishness and not on intentional malicious acts or jamming attacks. Yu and Liu presented a joint analysis of cooperation stimulation and security in autonomous mobile ad hoc networks under a game-theoretic framework [26]. Their results however show that the proposed strategies would only stimulate cooperation among selfish nodes in autonomous mobile ad hoc networks under noise and attacks which does not properly address intentional malicious attacks. Han and Poor [27] used coalition game in which boundary nodes used cooperative transmission to help backbone nodes in the middle of the network and in return the backbone nodes would be willing to forward the boundary nodes' packets.

Saghezchi et al. [28] proposed a credit scheme based on coalitional game model; the authors provided credit to the cooperative nodes proportional to the core solution of the game, and this distributes the common utility among the players in a way that all players are satisfied. Mathur et al. [29] studied the stability of the grand coalition when users in

a wireless network are allowed to cooperate while maximizing their own rates which serve as their utility function.

Our approach is unique in that (1) each node in the MANET is defined by a security characteristic function for the coalition formation, (2) each node uses a reputation mechanism to accurately detect insider jamming attack, (3) each node maintains a history of transmission rates for nodes in the coalition, and (4) the combination of transmission rates and reputation values for nodes in the coalition is used to detect insider attacker and exclude it from the coalition.

3. Network and Jammer Model

3.1. Network Model. We consider a model for the system as a reputation-based coalition game with imperfect information. The game will be repeated at each iteration until the nodes arrive at their destination. The model will consist of $N(1, 2, \ldots, N)$ numbers of nodes and $A(0, 1, \ldots, (N/2) - 1)$ numbers of attackers, where the number of attackers would not exceed the number of legitimate nodes. The attacker would be able to join the coalition because it acts like a regular node at the beginning, which permits it to become a member of the coalition. On joining the coalition, a new node has a reputation value of zero and would start cooperating by sharing its transmission rate to all the nodes in its range of transmission. Each node builds and maintains two tables. The tables contain an accumulative history of the entire transmission rate and reputation of all neighboring nodes based on their willingness to share their transmission rate with their neighbors. The transmission rate is broadcast periodically during time interval, t. This transmission rate is then stored according to our AFAT algorithm [30]. Nodes that share their transmission rates with neighboring nodes will receive a positive reputation from those neighbors and hence update their reputation table about the node. Nodes that refuse to share their transmission rate will receive a negative reputation. A node whose negative reputation value exceeds a preset threshold will be tagged as an attacker and excluded from the coalition.

3.1.1. Coalition Formation Model. A coalition game is an ordered pair $\langle N, v\rangle$, where $N = (1, 2, \ldots, n)$ is the set of players and v is the characteristic function. Any subset of N is called a coalition, and the set involving all players is called the grand coalition. The characteristic function $v : 2^N \to R$ assigns any coalition $C \subset N$ a real number $v(C)$, which is called the worth of coalition S. By convention, $v(\phi) = 0$, where ϕ denotes the empty set [31].

Let $n \geq 2$ denote the number of players in the game, numbered from 1 to n, and let N denote the set of players, $N = (1, 2, \ldots, n)$. A coalition, C, is defined to be a subset of N, $C \subset N$, and the set of all coalitions is denoted by 2^N. The set N is also a coalition, called the grand coalition. For example, if there are just two players, $n = 2$, then there are four coalitions, $(\phi, 1, 2, N)$. If there are 3 players, there are 8 coalitions, $(\phi, (1), (2), (3), (1, 2), (1, 3), (2, 3), N)$. For n players, the set of coalitions, $2N$, has 2^n elements. A game with transferrable utility (TU) is a game which involves a universal currency that can be freely exchanged among the players. A game which lacks this kind of currency is called a game with nontransferrable utility (NTU) [31]. In addition, $G = (N, v)$ is called a superadditive game if, $\forall C, T \subset N$ and $C \cap T \neq \phi$; then,

$$\begin{aligned} v(C \cup T) &\geq v(C) + v(T), \\ v(C \cup T) &\geq v(C) + v(T) - v(C \cap T). \end{aligned} \tag{1}$$

A payoff vector x is called feasible if it distributes the worth of grand coalition among the players completely [31]; that is,

$$\sum_{i \in N} x_i = v(N). \tag{2}$$

A payoff vector x is called individually rational if it offers players more payoff than what they can obtain individually [31]; that is,

$$x_i \geq v(i) \quad \forall i \in N. \tag{3}$$

The coalition formation process starts with nodes forming small disjoint coalition with neighboring nodes in their range of transmission and then gradually grows until the grand coalition is formed with the testimony of intersecting nodes. The final outcome of the coalition formation process is to form a stable grand coalition which comprises all nodes in the network. Forming a grand coalition implies that all the smaller coalitions formed would be merged by the presence of these intersecting nodes which would belong to more than one coalition at a time. Our coalition formation process depends on the transmission rate table that has been stored according to the previous work done by [30].

In [30], an accumulative feedback adaptation transmission (AFAT) rate was proposed; this design follows a decentralized approach which ensures the communication of transmission rates between neighboring nodes in a network. This crucial knowledge helps a node to adjust its own rate accordingly [30]. In other words, AFAT ensures maximum transmission rates for the nodes in order to meet the specific application bandwidth requirements [30]. According to AFAT, the transmission rates of the nodes are adjusted based on the history of neighbors' transmission rates. A list of the transmission rates has been built into the transmission rate table and is updated periodically [30].

The final outcome of the coalition formation process is to form a stable grand coalition which comprises all nodes in the network. The intersecting nodes would be very key to the formation of the grand coalition because they belong to the smaller coalitions that would be merged into a single coalition.

Our network model involves a characteristic function and a coalition formation model described in [31, 32]. Our security characteristic function consists of three parameters capturing the node mobility in the MANET. The support rate is the neighbors in the node's transmission range. The maximum transmission rate in the coalition is provided by AFAT. The maximal admitting probability or cooperation probability is unchanged.

Nodes can testify for each other so that the coalition has integrity compared to individuals. Any node that does not

(1) *Start* for all nodes, N
(2) Begin the 1st round of formation
(3) Pick a node with the highest $v_t(C)$
(4) Broadcast forming option to the neighboring nodes in the network
(5) **if** $v_t(C)$ is beyond threshold and ≥2 nodes match **then**
(6) Form a small coalition
(7) **else**
(8) Do not pick any node
(9) **end if**
(10) Update transmission rate table in AFAT [30] with the rate of newest members
(11) Begin the 2nd round
(12) Pick a node with the highest security value, $v_t(C)$
(13) **if** the first option has been matched successfully **then**
(14) Pick the next best option available
(15) **else**
(16) Broadcast the forming option to the neighbors again
(17) **end if**
(18) **if** there is an intersecting node- nodes that belongs to more than one small coalition **then**
(19) Merge the small coalitions
(20) **else**
(21) Re-broadcast forming option again to the network
(22) **end if**
(23) **if** $v(N) \geq$ payoff from any disjoint set of smaller coalition **then**
(24) Form a grand coalition
(25) **else**
(26) Repeat step (11)
(27) **end if**

Algorithm 1: Algorithm for coalition formation.

belong to the coalition would not be seen to be trustworthy. There are N nodes in the network; for any coalition, $C \in 2^N$. The number of nodes in it is $|C|$; any node in the coalition would have $|C| - 1$ nodes that can testify for it. Let $|G_i|$ be the set of nodes in a transmission range. Therefore, at time slot t, the support rate for a node, i, is

$$S_t(C) = |G_i| - 1. \tag{4}$$

The transmission rate, $T_t(C)$, of coalition C at time t would also be a part of the security function. The nodes' sharing of their transmission rate is very key to their admittance into the small coalition. In other words, to form a coalition with any node, there is a need to know the maximum available transmission rate. The maximum transmission rate ensures that the nodes match the best nodes in terms of transmission rate before settling for the next best option as seen in the coalition formation algorithm. The maximum transmission rate is given by

$$D_t(C) = \max\{T_t(C)\}. \tag{5}$$

The larger the transmission rate of a node is, the more probable it is for such a node to quickly find a match. These transmission rates are stored according to AFAT [30].

The third parameter for the characteristic function is the maximal admitting probability, because nodes in the network have different admitting probabilities and it would be necessary to pick the highest probability which would be used as a reference for the whole coalition. Every node in the coalition formed was admitted with a certain probability. The nodes having different admitting probability engender the need to assign a maximal admitting probability as the cooperation probability of the whole coalition. Hence, a larger coalition size ensures a higher cooperation probability.

The maximal admitting probability is given by

$$A_t(C) = \max_{j \in C} \left\{ \frac{\sum_{i \in C} P_{ij}}{|C|} \mid C = \{i \mid i \in C,\ i \neq j,\ P_{ij} \neq 0\} \right\}. \tag{6}$$

Algorithm 1 shows the coalition formation steps.

The coalition formation is a dynamic process; it is performed in an iterative manner until all nodes belong to the coalition. No matter the location of a node in the network, it still has neighbors that can testify about it. From the coalition formation algorithm, we can see that, at each round of formation, every coalition member tries to find a partner. The convergence time of formation is short, thereby increasing the speed of coalition formation. The grand coalition is eventually formed when two conditions are met: presence of an intersecting node to aid the merging and whether $v(N)$ is at least greater than the individual payoff of any disjoint smaller coalition.

A coalition approach is needed to detect insider attacks. As stated earlier, we are interested in a singular coalition, called the grand coalition as shown in Figure 1. In the grand

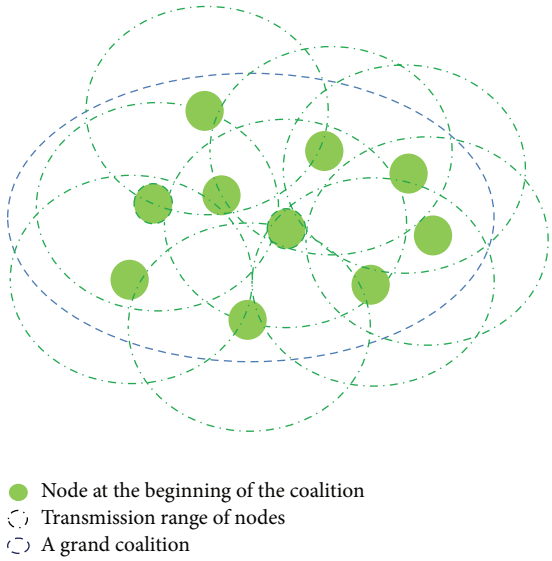

Figure 1: A coalition of ten (10) nodes with no malicious node.

coalition, all nodes in the network should belong to this single coalition.

From the coalition formation algorithm, we can see that, at each round of formation, every coalition member tries to find a partner. Therefore, the speed of coalition formation is fast, which means the convergence time of formation is short. And the size will keep growing until a grand coalition is reached or all misbehaving nodes are identified. It is important to explain how large the size of the coalition would be. The grand coalition is eventually formed from merging the smaller coalitions that have the same members. These intersecting nodes will be a condition to form a grand coalition between the smaller coalitions. The maximal admitting probability is the cooperation probability of the whole coalition, because the larger the coalition size is, the more tolerant and robust the coalition is, and the coalition can therefore have a higher cooperation probability. Each node has no limit on the number of neighbors in its range because they are all moving (as the name implies mobile ad hoc networks). In other words, there are no fixed numbers of neighbors to a particular node. From our proposed model, the size of the grand coalition could be any size of three nodes and above as would be seen in the simulation section which have three cases, where each case consists of different numbers of legitimate and malicious nodes. For any node $i \in C$, $|C| > 1$, its security payoff share is defined as

$$x_t(i) = \frac{1}{|C|}\left(\alpha S_t(C) + \beta A_t(C) + \gamma D_t(C)\right). \quad (7)$$

The coalition game definitely has a core; a core exists only if the sum of payoff shares of all the members for each coalition is larger than the value of that coalition. From (3) and (4), we can deduce that

$$\sum_{i \in C} x_t(i) \geq v_t(C). \quad (8)$$

The game has a core because it satisfies the concept of core of the coalition game [31].

3.1.2. Admitting a Node into the Grand Coalition. A new node would be accepted into the grand coalition based on its ranking in the smaller coalition. To be admitted to a grand coalition, the node should build up good reputation while it is a part of the small coalition. It is possible for a new node to be denied access to the grand coalition even when it was a part of the smaller coalition. This is possible when the new node is temporarily out of range from the intersecting node as at the time its smaller coalition is forming a grand coalition. So, in essence, the new node is not totally new to some nodes in the coalition. This process could continue while there are intersecting nodes to testify about the new node. This would make the grand coalition get bigger which would help provide more robust security in the network as we stated earlier.

Incorporating these three parameters, we can write the characteristic function by weighing each parameter. The characteristic function proposed is then

$$v_t(C) = \begin{cases} 0, & \text{if } |C| = 1 \\ \alpha S_t(C) + \beta A_t(C) + \gamma D_t(C), & \text{if } |C| \geq 1. \end{cases} \quad (9)$$

α, β, and γ are weight parameters and

$$\alpha + \beta + \gamma = 1. \quad (10)$$

These weight parameters can be used to help provide variability for the characteristic function of the nodes. Due to the mobility factor in our model, it is important to keep track of the neighbors of any node at a given time; α helps to weigh the support rate parameter which is responsible for the number of neighbors of a node. Our assumption is that the nodes are slow-moving and there cannot be a rapid change of neighbors. β provides a weight value for the maximal admitting probability. The value assigned to β depends on the size of the coalition; if the coalition size is very big (say about 100 nodes), then it could be important to make it bigger than the other parameters.

The transmission rate is affected by two major factors: propagation environment and the degree of congestion. Depending on these two factors, we could assign a weight value for the maximum transmission rate using γ. Therefore, the three main parameters that affect the payoff are the support rate, cooperative probability, and transmission rates of the nodes. That is according to the dynamism of those variables. If the coalition refuses to admit some nodes, that means that these nodes did not meet the requirements for joining the coalition regardless of whether it is a malicious node or not.

3.1.3. Network Assumptions. We assume N mobile nodes with A attackers, where A is less than $N/2$ (i.e., the number of attackers would not exceed the number of legitimate nodes). The following are the assumptions under which we present our work:

(i) Nodes cannot easily generate identities which can be exploited to launch a Sybil attack; hence, we do not consider the possibility of Sybil attacks in this paper.

(ii) All players (or nodes) are rational (i.e., they would always choose the strategy that benefits them the most).

(iii) Individual nodes have weak security and would jointly have higher security by joining a coalition.

(iv) There is no hierarchy, leader-follower, or centralized mechanism in this system.

(v) The goal of the game is to form a stable grand coalition where any node that is unable to join this grand coalition would be designated as a malicious node.

(vi) The nodes are moving slowly because fast movement brings about a frequent change in the node's neighbors which may affect the reputation of the nodes adversely.

(vii) A node's continuous membership of the grand coalition is dependent on its reputation value.

3.2. Jammer Model. Liao et al. have classified attacks on wireless ad hoc networks; they classified attacks as palpable and subtle, with palpable attacks being attacks resulting in conspicuous impact on network functions which results in intolerable impacts on the users. On the other hand, they defined subtle attacks as attacks that lead to invisible damage in a vaguer way. According to them, palpable attacks include jamming, traffic manipulating, blackhole, and flooding attacks, while subtle attacks include eavesdropping, traffic monitoring, grayhole, wormhole, and Sybil attacks [33].

The jammer starts out by being a member of a smaller coalition and as such has earned a good reputation from its neighboring nodes. We would recollect that the grand coalition is formed only when there is an intersecting node from the other smaller coalitions (i.e., the intersecting node or nodes belong to more than one coalition according to the coalition formation algorithm explained in the coalition formation process). The intersecting node would serve as a referee for the other nodes. The attacker who has met all the criteria to be a part of the coalition would be seen to start out as an eavesdropper by passively monitoring the network and even participating in sharing its transmission rate with all the neighbors in its range of transmission in the coalition. At this stage, the attacker would still partake of the crucial network assignments like routing and packet forwarding and in turn gain a good reputation for itself. After gathering information about what channel its neighbors are transmitting on, the attacker stops sharing its own transmission rate and at this point its reputation starts reducing at every time slot.

The jammer would then launch its palpable attack by intentionally sending a high-powered interference signal to the channel that has a lot of traffic on it, thereby attempting to disrupt communication. As can be seen from the jammer model above, the jammer is an intelligent jammer who has acted as an "undercover agent" in the coalition. The jammer would start to initiate its attack right after it has enough information in its history table. The most important requirement is that the jammer must gather information about the transmission rates that have been shared by the other nodes in its range of transmission. It is also monitoring the communication in the coalition as well as initially participating in the network functions before launching its attack. The aim of jamming a selected channel is to disable the functionality of the channel in question thereby causing a jamming attack to all the nodes in the coalition. The complexity of the jamming can be seen in the fact that the movement of the jammers may hinder the detection capability of the coalition. The jammers distinctive attack would be different from a normal interference or noise in that it would send a high-powered signal to disrupt communication in a selected channel it has enough information on.

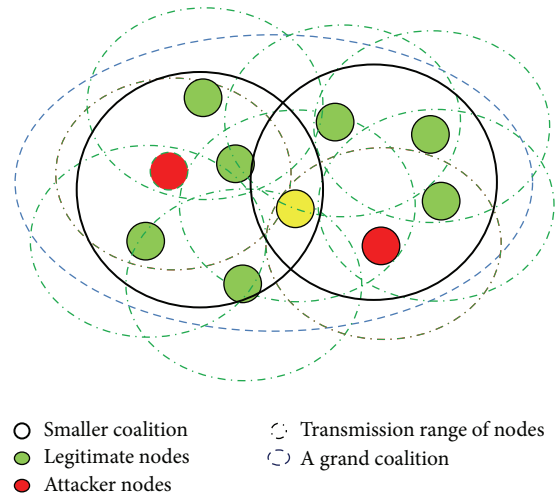

Figure 2: A coalition of ten (10) nodes with two (2) jammers.

Figure 2 shows the presence of two jammers in a coalition of ten nodes. The jammers first became a part of two smaller coalitions which in turn merged to become a grand coalition. The node marked by the yellow color will be the intersecting node for both coalitions. It can be seen that the first jammer has three other legitimate nodes in its range of transmission; it has the capability of jamming the channels at which they are broadcasting their transmission rate. The second jammer on the other hand has two legitimate nodes in its transmission range. The scenario painted below shows that there could be a case of more than one jammer and subsequently our simulation results would show how these malicious nodes are excluded from the coalition.

4. The Proposed Defense Model

4.1. Maintaining the Coalition through Reputation. Here, we present a maintenance method that employs the node reputation to track all the history of each node's cooperation as they broadcast their transmission rate. Reputation, in the context of cooperation, is defined as the goodness of a node as perceived by other nodes in a network. A higher value of reputation indicates that the node is cooperative while a smaller value indicates misbehavior. The reputation of a node is maintained by its neighbors who monitor the nodes behavior and

(1) Assign values for σ and λ
(2) *Start* for all nodes
(3) Node i checks its transmission rate table to assign reputation value for neighbor j.
(4) **if** j shares its transmission rate **then**
(5) compute reputation value according to:
(6) $$v_{i,j}(y) = \frac{y}{R_{i,j}}$$
(7) **else**
(8) Set $v_{i,j}(y) = 0$ if $y/R_{i,j} \leq b_f$ [34]
(9) **end if**
(10) **if** j refuses to share its transmission rate **then**
(11) compute reputation value according to
(12) $$k_{i,j}(m) = \frac{m}{R_{i,j}}$$
(13) **else**
(14) Set $k_{i,j}(m) = 0$ if $m/R_{i,j} \leq T_f$
(15) **end if**
(16) Node i updates node j's reputation value according to:
(17) $$R_{i,j} = R^*_{i,j} + \sigma * \left(v_{i,j}(y)\right) - \lambda * \left(k_{i,j}(m)\right)$$
(18) Store this reputation value in its reputation table
(19) Share reputation table with neighbors at every time-slot.
(20) **return** $R_{i,j}$
(21) All nodes continue to update their reputation table.

Algorithm 2: Coalition maintenance through reputation.

update its reputation accordingly. We define a good behavior as the timely broadcast of transmission rate and misbehavior as refusal to broadcast transmission rate at any time slot. Every node monitors and is in turn monitored by its neighbors. A new node that joins the network is neither trusted nor mistrusted but is assigned a neutral reputation q_N. All reputations are valid for a time period, T_v. There is an upper threshold, q_U, and a lower threshold, q_L, where $q_L < q_N < q_U$.

Reputation is increased at the rate of σ and decreased at the rate of λ, where $\sigma, \lambda < 1$ and are both real numbers. Both σ and λ need to be chosen carefully; this is because if σ is very large when compared to λ, a node may cooperate and build high reputation in a short time span and then consequently refuse to share its transmission rate for a long time; also, it may lack the motivation to continue cooperating after reaching the upper threshold, q_U, due to the high rate of increment. On the other hand, if λ is reduced at a low rate, a node can stay in the coalition long enough to exploit the network infrastructure; decreasing at a very high rate also causes an unjust punishment for a node that misbehaves because of network congestion. It is possible to set σ equal to λ, as this would make the reputation increase and decrease at the same rate to ensure fairness. Algorithm 2 shows the monitoring process and how the reputation is either increased or decreased depending on the node's behavior.

m is the number of observations made by node j about node i's refusal to share its transmission rate. T_f is the tolerance of the network, that is, m per reputation value before reducing reputation of a node.

y is the number of observations made by node j when node i shares its transmission range in the time period b_f. b_f is the broadcast factor of the network.

4.2. Jammer's Exclusion from the Coalition. The exclusion of jammer from the coalition should factor in false positive which results when a legitimate node is classified as a jammer when it is unable to share transmission rates due to impairing wireless environment. False positive could also happen when a node fails to broadcast its transmission range at a particular time slot due to being in an out-of-range location. This situation often arises in a mobile system where nodes are constantly in motion. We adopt reputation management to encourage trustworthy behavior from nodes in the coalition. In addition, reputation profiles are predictive of node's actions. The implementation of reputation systems is of particular importance in games where repeated interactions between multiple players are probable. Furthermore, because of the nature of the attack which includes carefully monitoring the network and then turning against the network when enough information has been gathered, it is necessary to drum up support from all nodes in the coalition to be able to properly exclude any malicious node.

As it has been explained in Section 4.1, each node starts out with the same reputation value and these values will increase as the nodes continue to cooperate and reduce as well when they refuse to cooperate. When a node joins a small coalition, it would start with a reputation value of zero. The reputation is updated according to (10). Nodes that belong to the coalition have a monitor for observations and reputation records for first-hand information about routing and forwarding behavior of other nodes, nodes publishing of their transmission rates, and a path manager to adapt their behavior according to reputation and to take action against any misbehavior. The coalition excludes the jammer by following Algorithm 3.

(1) Node i checks node j' reputation value after update.
(2) Node j is tolerated until its reputation falls below q_L
(3) Classify misbehaving nodes according to:
jammer, if $R_{i,j} < q_L$
regular, if $R_{i,j} \geq q_L$
(4) **if** $R_{i,j}$ is below q_L **then**
(5) Node i sends an alarm message
(6) All nodes change their channel of transmission
(7) Accused node's payoff reduces due to bad testimony
(8) Node j attempts to jam the communication channel that has the best transmission rate.
(9) Jammer records little or no success because of the proactive step taken by the coalition.
(10) Neighbors of node j, blacklist him and exclude him from their small coalition.
(11) Nodes with reputation greater than q_L regroup again.
(12) **else**
(13) No alarm is sent and nodes continue their transmission
(14) **end if**
(15) Nodes with $R_{i,j}$ greater than q_L are retained
(16) Continue transmission

Algorithm 3: Jammer exclusion from the coalition.

The jammer prevention algorithm aims to reduce the number of false positives. False positive occurs when a legitimate node is classified as a jammer when a node fails to broadcast its transmission rate at a particular time slot due to being out of range, which is typical of mobile networks. The implementation of reputation systems is of particular importance in games where repeated interactions between multiple players are probable. Nodes that belong to the coalition have a monitor for observations and reputation records for first-hand information about the degree of cooperation of their neighbors as regards sharing their transmission rates. The coalition excludes the jammer by Algorithm 3.

A malicious node that has been excluded from the coalition cannot be redeemed. Algorithm 3 provides the needed self-dependency and self-organization that are usually required in mobile ad hoc networks.

Table 1: Parameters for simulation.

Parameter	Level
Area	2300×1300
Speed	15 m/s
Radio range	250 m
MAC	802.11
Simulation time	130 s
Number of mobile nodes	5, 10, 20, 40, and 80
Network interface type	Wireless
Channel type	Wireless channel
Transmission rate	1–11 Mbps
Percentage of jammer	20%
Threshold, q_U	0.975
Threshold, q_L	0.70

5. Simulation and Results

5.1. Simulation Scenarios and Parameters. We implemented our approach using NS2 simulator. The results will show three different scenarios. The first scenario focuses on network throughput and delay; in this scenario, we show how the coalition size affects these two parameters. The second scenario shows how varying the reputation parameters can affect the performance of the jammer. The third scenario focuses on the varying of the weights (α, β, γ) of the security characteristic function. The parameters for the simulation are shown in Table 1.

5.2. Results

5.2.1. Scenario One: Network Throughput and Delay. For this scenario, we show the network throughput and the delay with respect to time for three cases of different coalition sizes $(5, 10, 20)$. This is done in order to show that delay would reduce significantly as the coalition size increases in a very short period of time.

The network throughput and delay for the first case are discussed here. The first case consists of five nodes $(N1, N2, N3, N4, N5)$: four of them are legitimate nodes and one is the jammer. Figure 3 shows the throughput for this case; from the results as shown in Figure 3, we see that, owing to the small ratio of jammer to legitimate node, the throughput of the jammer is still considerably high until after about 3 ms when it decreases sharply. After 3 ms, the jammer has been excluded from the coalition and hence its throughput takes a nosedive.

Figure 4 shows the network delay for the first case when the coalition is under attack. There is a spike at the beginning of the attack which indicates the sharp increase in the delay due to the jamming attack launched by the jammer. The delay is seen to improve as the coalition regroups again after excluding the jammer.

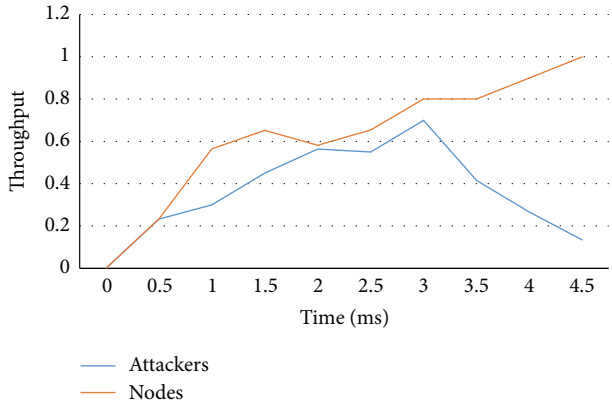

Figure 3: Throughput for 4 legitimate nodes versus 1 jammer.

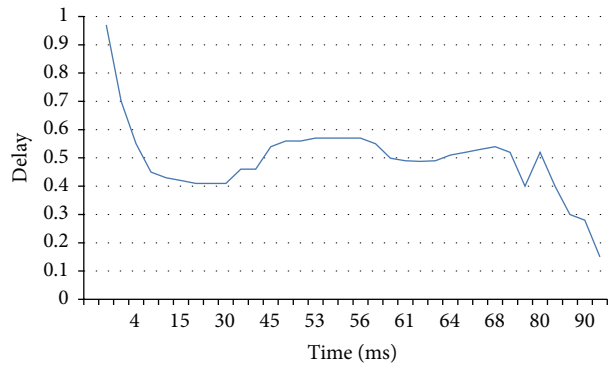

Figure 4: System delay for 4 legitimate nodes and 1 jammer.

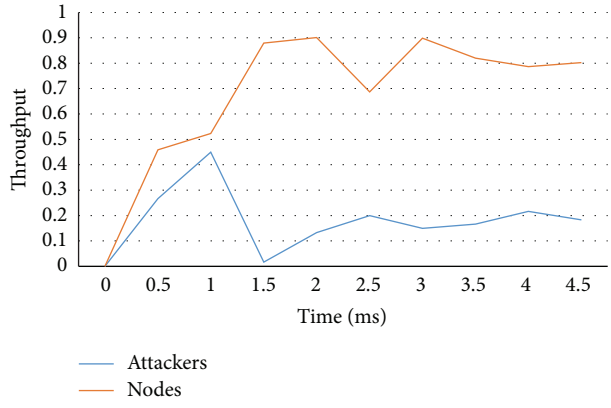

Figure 5: Throughput for 8 legitimate nodes versus 2 jammers.

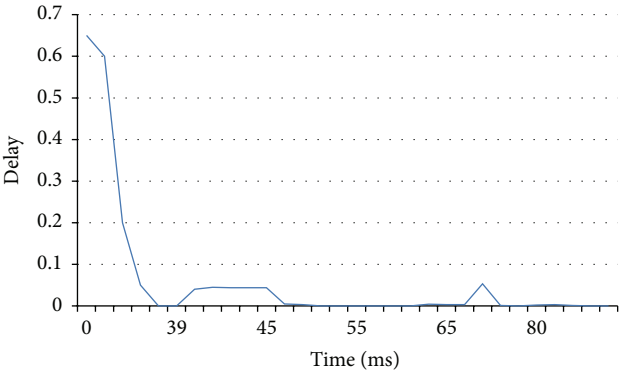

Figure 6: System delay for 8 legitimate nodes and 2 jammers.

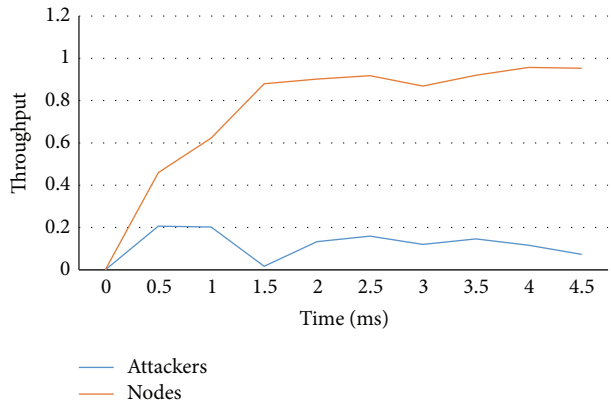

Figure 7: Throughput for 16 legitimate nodes versus 4 jammers.

For the second case, we also discuss the network throughput and delay with respect to time. In this case, there are ten nodes ($N1, N2, N3, \ldots, N10$): eight of them are legitimate nodes and two are jammers. Figure 5 displays the throughput of the jammer and the network during the attack. The throughput of the jammers reduced sharply right after 1 ms. This is because we have a larger number of neighboring nodes that could observe the activities of the jammer. After 1.5 ms, the jammer having been excluded from the coalition still seeks to continue jamming the network but its throughput is soon reduced to the barest minimum.

Figure 6 shows the network delay for the second case when the coalition is under attack. Even though we still notice a spike at the beginning of the attack, the network delay has been greatly reduced. The reason for this is that the coalition has more nodes than the previous scenario which help to provide a more robust defense to attacks. After some time, we see that the delay is reduced to zero, which is the ideal delay that is expected in any network.

In the third case, the network throughput and delay with respect to time are also shown. In this case, there are twenty nodes ($N1, N2, N3, \ldots, N20$): sixteen of them are legitimate nodes and four are attackers. From the results as shown in Figure 7, we see that the throughput of the attacker reduces after 0.5 ms. It can be seen that if we keep increasing the number of nodes in the coalition, the value of the network throughput improves tremendously. This occurs because our system relies on reputation value assigned by a node's neighbor and the more neighbors a node has, the better an alert would be raised when it crosses the threshold value for its reputation.

Figure 8 shows the network delay for the third case when the coalition, again, is under attack. As can be observed, the spike has been reduced by more than 200 percent of the second case. This proves that the more nodes we have in the coalition, the better results we get.

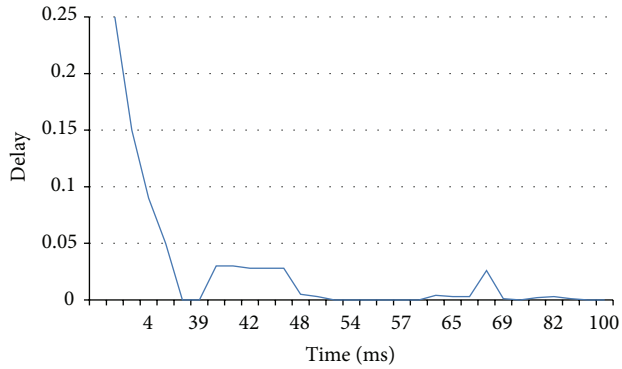

Figure 8: System delay for 16 legitimate nodes and 4 jammers.

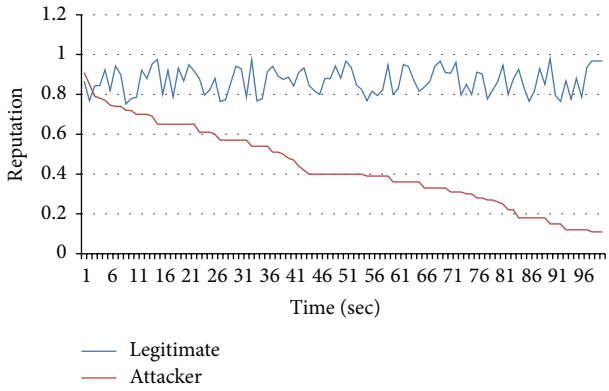

Figure 9: Reputation of both regular and jammer node over time.

5.2.2. Scenario Two: Reputation. For this scenario, we show how reputation can affect different aspects for both legitimate nodes and jammers and show how reputation can be a major issue for classifying nodes and detecting jammers.

In Figure 9, we show the comparison between the reputations of both regular and jammer nodes. A regular node retains its reputation value by sharing its transmission rate at every time slot while the reputation value for the insider jammer reduces when it stops cooperating. The nearest neighbor of the jammer node computes the reputation at every time slot. The computation follows (9) and (10) in Algorithm 2.

Figure 10 shows the number of observations made by the nodes for cooperative, suspicious, and malicious nodes. A node is observed as suspicious if its reputation value is close to the lower threshold for the reputation. As seen in the figure, the number of observations made increases with increase in coalition size. This figure particularly shows the importance of the support rate parameter, as only the neighbors of a node can make a genuine observation about its activities in the coalition.

Figure 11 shows the average payoff of the insider jammer after detection with different decreasing reputation values λ. From the figure, it can be seen that if we keep increasing λ, the punishment for a jammer is increased by a large decrease in its reputation score; this, in turn, reduces the average payoff of the jammer. A value of $\lambda = 0.7$ shows a great reduction in the payoff of the jammer.

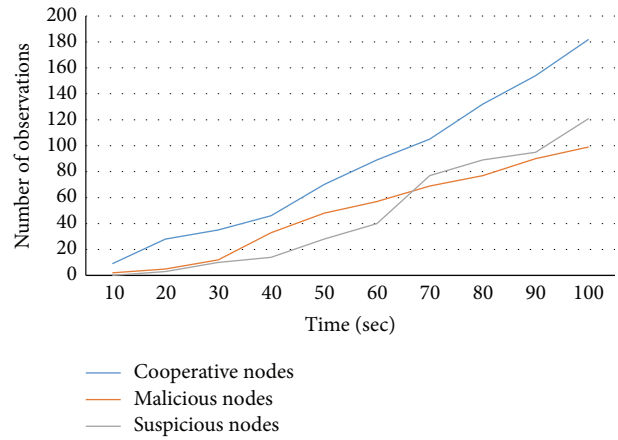

Figure 10: Number of observations made for all nodes.

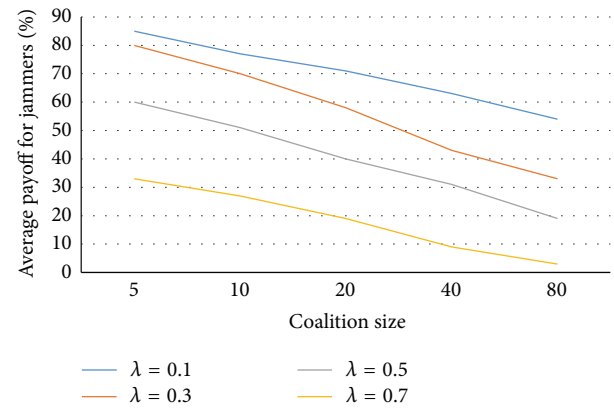

Figure 11: Average payoff of the insider jammer after detection.

5.2.3. Scenario Three: Security Characteristic Function. This scenario shows outputs for different value assigned for security characteristic function weight and shows how these weights affect their respective parameters.

Figure 12 illustrates network overhead when support rate parameter α is varied for different coalition size. Overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal. The goal for us here is to have as many neighbors as possible to testify for a node. Due to this goal, the network overhead needs to be reduced as much as possible. This is reduced by specifying a suitable value for α. Here, the network overhead slightly changes with an increase in the number of neighbors.

Figure 13 illustrates admitting probability for different coalition size and β values. When β is increased, the probability of admitting a node into a coalition is also increased which has a tendency of allowing more malicious nodes to gain access to the coalition. It is important to state that this parameter needs to be carefully chosen as well. For optimum results, it is better to set this value to 0.3. The value can however be chosen based on the peculiarity of the network.

Figure 14 illustrates the degree of congestion when transmission rate is varied for different coalition size and

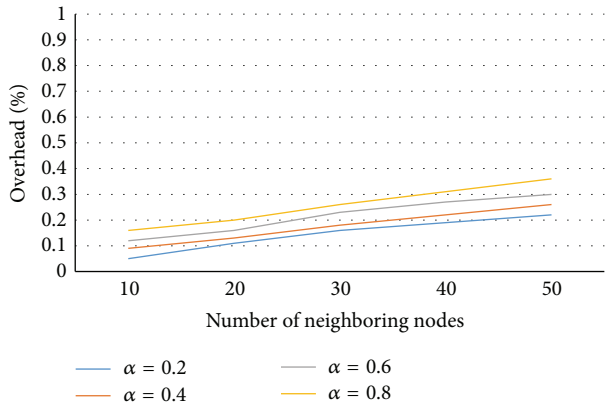

Figure 12: System overhead percentage with different numbers of neighboring nodes.

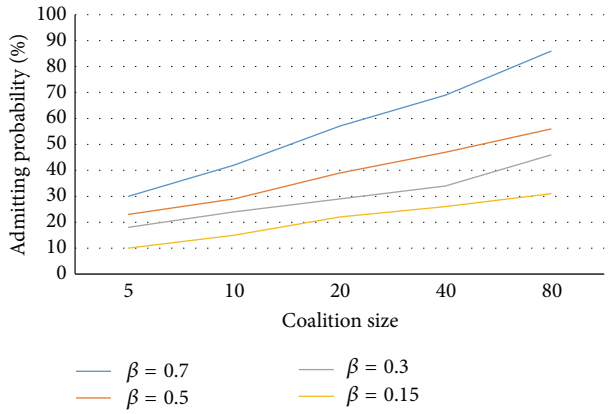

Figure 13: Admitting probability for different coalition size and beta values.

γ values where γ is the value maximum transmission rate factor. When there are more nodes in the network, there is a tendency that the network would get congested when they start communicating. With an increase in γ, the degree of congestion for the network slowly increases as seen in Figure 14. The highest degree of congestion is seen when γ is set to 0.8 for a coalition size of 80 nodes.

6. Conclusion and Future Work

We have been able to show through simulation that a reputation-based coalitional game can help prevent insider attacks in a mobile ad hoc network. We discussed a coalition formation algorithm and showed how nodes can be admitted into a coalition using a modified security characteristic function. We came up with a unique mechanism that keeps track of the transmission rates and reputation of individual nodes in the network. Also, we showed how the jammers action can be prevented and how it is excluded from the coalition. In the future, we would like to show through simulations and experiments that this model can be scaled up to include thousands of nodes and this would further show that the algorithm would work best when there are so many nodes in the coalition. We would also like to investigate a case of cooperative attacks that could occur when the excluded nodes form a coalition with the aim of jamming communication in their previous coalition.

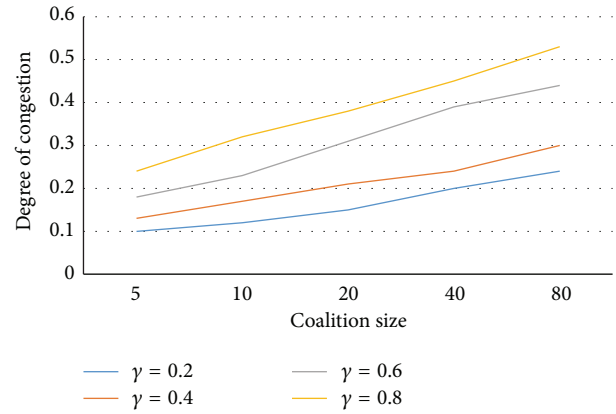

Figure 14: Degree of congestion when transmission rate is varied.

Notations

N: Number of nodes in the network
C: Coalition of nodes
G_i: Nodes in the transmission range of node i
$v_t(C)$: Security characteristic function for coalition C
$v(N)$: Payoff of the grand coalition
$S_t(C)$: Support rate for coalition C
$T_t(C)$: Transmission rate of coalition C
$P_{i,j}$: Probability of cooperation of node i with node j
$A_t(C)$: Maximal admitting probability for coalition C
$x_t(i)$: Payoff share of node i
$R_{i,j}$: Reputation value of node i by node j
$R^*_{i,j}$: Previous reputation value of node i by node j
$R_{i,k}$: Reputation value of node i by node k
$v_{i,j}(y)$: Factor responsible for increasing reputation value
$k_{i,j}(m)$: Factor responsible for reducing reputation value
q_L, q_N, q_U: Lower, neutral, and upper threshold value, respectively
T_f, b_f: Tolerance factor of the network and broadcast factor
σ, λ: Rate of increase and decrease of reputation value.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work is supported by Office of the Assistant Secretary of Defense for Research and Engineering Agreements FAB750-15-2-0120, NSF CNS-1405681, and DHS 2014-ST-062-000059.

References

[1] M. Albanese, A. De Benedictis, S. Jajodia, and D. Torrieri, "A probabilistic framework for jammer identification in MANETs," *Ad Hoc Networks*, vol. 14, pp. 84–94, 2014.

[2] P. Sharma and A. Suryawanshi, "Enhanced security scheme against Jamming attack in mobile Ad hoc network," in *Proceedings of the International Conference on Advances in Engineering and Technology Research (ICAETR '14)*, pp. 1–5, IEEE, Unnao, India, August 2014.

[3] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 2, pp. 245–257, 2011.

[4] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[5] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread-spectrum communications–a tutorial," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 855–884, 1982.

[6] DSSS-wikipedia, http://en.wikipedia.org/wiki/Direct-sequencespreadspectrum.

[7] UWB-wikipedia, http://en.wikipedia.org/wiki/Ultrawideband.

[8] W. Stutzman and G. Thiele, *Antenna Theory and Design*, John Wiley & Sons, New York, NY, USA, 2nd edition, 1997.

[9] P. Goudarzi, "A non-cooperative quality optimization game for scalable video delivery over MANETs," *Wireless Networks*, vol. 19, no. 5, pp. 755–770, 2013.

[10] X. Guan, M. Chen, and T. Ohtsuki, "Non-cooperative game-based packet ferry forwarding for sparse mobile wireless networks," *Wireless Communications and Mobile Computing*, vol. 15, no. 12, pp. 1633–1648, 2015.

[11] P. R. Baggidi, D. Giri Prasad, and T. Srinivas, "Security enhancement in mobile ad hoc networks using non-zero non-cooperative game theory," *International Journal of Research in Computer and Communication Technology*, vol. 2, no. 8, pp. 614–621, 2013.

[12] B. Paramasiva and K. M. Pitchai, "Modeling intrusion detection in mobile ad hoc networks as a non cooperative game," in *Proceedings of the International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME '13)*, pp. 300–306, IEEE, Salem, India, February 2013.

[13] B. Zong, F. Xu, J. Jiao, and J. Lv, "A broker-assisting trust and reputation system based on artificial neural network," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC '09)*, pp. 4710–4715, San Antonio, Tex, USA, October 2009.

[14] M. T. Refaei, L. A. DaSilva, M. Eltoweissy, and T. Nadeem, "Adaptation of reputation management systems to dynamic network conditions in ad hoc networks," *IEEE Transactions on Computers*, vol. 59, no. 5, pp. 707–719, 2010.

[15] H. Nguyen, T. Pongthawornkamol, and K. Nahrstedt, "A novel approach to identify insider-based jamming attacks in multi-channel wireless networks," in *Proceedings of the IEEE Military Communications Conference (MILCOM '09)*, pp. 1–7, IEEE, Boston, Mass, USA, October 2009.

[16] L. Li, S. Zhu, D. Torrieri, and S. Jajodia, "Self-healing wireless networks under insider jamming attacks," in *Proceedings of the IEEE Conference on Communications and Network Security (CNS '14)*, pp. 220–228, San Francisco, Calif, USA, October 2014.

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 255–265, August 2000.

[18] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security*, Portorož, Slovenia, September 2002.

[19] A. Cheng and E. Friedman, "Sybilproof reputation mechanisms," in *Proceedings of the ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems*, Philadelphia, Pa, USA, 2005.

[20] S. Buchegger and J.-Y. Le Boudec, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Communications Magazine*, vol. 43, no. 7, pp. 101–107, 2005.

[21] P. Michiardi and R. Molva, "A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile ad hoc networks," in *Proceedings of the Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt '03)*, pp. 3–5, Sophia Antipolis, France, March 2003.

[22] G. Thamilarasu and R. Sridhar, "Game theoretic modeling of jamming attacks in ad hoc networks," in *Proceedings of the 18th International Conference on Computer Communications and Networks (ICCCN '09)*, pp. 1–6, San Francisco, Calif, USA, August 2009.

[23] D. Slater, P. Tague, R. Poovendran, and M. Li, "A game-theoretic framework for jamming attacks and mitigation in commercial aircraft wireless networks," in *Proceedings of the AIAA Infotech at Aerospace Conference and Exhibit and AIAA Unmanned, Unlimited Conference*, Seattle, Wash, USA, April 2009.

[24] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Jamming games in wireless networks with incomplete information," *IEEE Communications Magazine*, vol. 49, no. 8, pp. 112–118, 2011.

[25] S. Bhattacharya and T. Başar, "Game-theoretic analysis of an aerial jamming attack on a UAV communication network," in *Proceedings of the American Control Conference (ACC '10)*, pp. 818–823, Baltimore, Md, USA, July 2010.

[26] W. Yu and K. J. R. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 507–521, 2007.

[27] Z. Han and H. V. Poor, "Coalition games with cooperative transmission: a cure for the curse of boundary nodes in selfish packet-forwarding wireless networks," *IEEE Transactions on Communications*, vol. 57, no. 1, pp. 203–213, 2009.

[28] F. B. Saghezchi, A. Radwan, and J. Rodriguez, "A coalitional gametheoretic approach to isolate selfish nodes in multihop cellular network," in *Proceedings of the 9th IEEE Symposium on Computers and Communications (ISCC '14)*, Madeira, Portugal, June 2014.

[29] S. Mathur, L. Sankar, and N. B. Mandayam, "Coalitions in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 7, pp. 1104–1115, 2008.

[30] A. Al-Sharah and S. Shetty, "Accumulative feedback adaptation transmission rate in mobile ad-hoc networks," in *Proceedings of*

the International Conference and Workshop on Computing and Communication (IEMCON '15), pp. 1–5, Vancouver, Canada, October 2015.

[31] T. S. Ferguson, *Game Theory*, Mathematics Department, University of California, Los Angeles, Calif, USA, 2nd edition, 2014.

[32] X. Li, *Achieving secure and cooperative wireless networks with trust modelling and game theory [Ph.D. thesis]*, 2009.

[33] X. Liao, D. Hao, and K. Sakurai, "Classification on attacks in wireless ad hoc networks: a game theoretic view," in *Proceedings of the 7th International Conference on Networked Computing and Advanced Information Management (NCM '11)*, pp. 144–149, Gyeongju, The Republic of Korea, June 2011.

[34] A. Balasubratuanian and J. Ghosh, "A reputation based scheme for stimulating cooperation in MANETs," in *Proceedings of the 19th International Teletraffic Congress (ITC '19)*, Beijing, China, September 2005.