A Reputation-Based Coalition Game to Prevent Smart Insider Jamming Attacks in MANETs

Taiwo Oyedare, Ashraf Sharah, Sachin Shetty

A Reputation-Based Coalition Game to Prevent Smart Insider Jamming Attacks in MANETs

Taiwo Oyedare, Ashraf Al Sharah, and Sachin Shetty

Department of Electrical and Computer Engineering
Tennessee State University
Nashville, TN 37209, United States.
{toyedare,aalshara,sshetty}@tnstate.edu

Abstract. Mobile Adhoc Networks (MANET) are susceptible to jamming attacks which can inhibit data transmissions. There has been considerable work done in the detection of external jamming attacks. However, detection of insider jamming attack in MANET has not received enough attention. The presence of an insider node that has constantly monitored the network and is privy to the network secrets can acquire sufficient information to cause irreparable damage. In this paper we propose a framework for a novel reputation-based coalition game between multiple players in a MANET to prevent internal attacks caused by an erstwhile legitimate node. A grand coalition is formed which will make a strategic security defense decision by depending on the stored transmission rate and reputation for each individual node in the coalition. Our results show that the simulation of the reputation-based coalition game would help improve the network's defense strategy while also reducing false positives that results from the incorrect classification of unfortunate legitimate nodes as insider jammers.

Keywords: Coalition, Reputation, Insider Jamming, Transmission Rate

1 Introduction

Mobile Ad-hoc Network (MANET) is a group of self-organized, infrastructureless mobile nodes that relies on interdependence and cooperation of all nodes to carry out critical network functions. 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 insider jamming[1]. External jamming attacks are launched by foreign devices that are not privy to network secrets such as the network's cryptographic credentials and the transmission capabilities of individual nodes the network [1]. These types of attacks are relatively easier to counter through some cryptography based techniques, some spread spectrum methodology [2], Antenna Polarization and directional transmission methods [3].

Smart insider jamming attacks on the other hand are much more sophisticated in nature because they are launched from a compromised node.[3] The

[1] Insider jamming is also known as internal jamming.

[2] Spread spectrum techniques include Frequency-Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) [2]

[3] Smart insider jammers are capable of passively scanning the network and then launching an attack based on the information gotten.

attacker exploits the knowledge of network secrets to deceptively target critical network functions. In order to effectively prevent the smart insider jamming attack, we adopt a reputation mechanism to detect the presence of smart jammer nodes when they are passively eavesdropping and collecting information about the network prior to launching the jamming attack. A lower reputation threshold is set such that the jammer would not be able to successfully jam the network without being detected by its neighbors. In this paper, we propose a reputation-based coalition game to prevent an attack that could be posed by an erstwhile legitimate node. Game theoretic based approaches for mitigating attack can be seen in the works of [4] where a coalition game with cooperative transmission was implemented as a cure for the curse of boundary nodes in selfish packet-forwarding. Alibi-based protocol [5] and self-healing protocol [6] have been used to either detect or recover from a jamming attack. Our reputation-based coalition game differs from the aforementioned approaches by (1) Designing a coalition formation algorithm, (2) Maintaining the coalition via a reputation mechanism, (3) Identifying the insider jammer based on reputation score , and (4) Excluding the attacker from the coalition by rerouting transmission path and randomly modifying communication channel. The game is fully distributed and does not rely on any trusted central entity to operate at optimal performance.

The remainder of this paper is organized as follows. Section II we present relevant works that are closely related to our model; in Section III we present the network and jammer model; Section IV contains the proposed defense model and in Section V we show our simulation results and finally in Section VI we conclude the work and highlight prospective future work.

2 Related Work

Researchers have devoted great efforts on security in MANET. In [7] and [8], the authors used watchdog/pathrater and collaborative reputation (CORE) mechanisms respectively to prevent to mitigate node misbehavior in MANETs. Other works have used non-cooperative games to model security scenarios as well as the corresponding defense strategies to such attacks [9]. Most of these works focused on two player games where all legitimate nodes are modelled as a single node and attacker nodes are also modeled as a single node as well; this is only valid for centralized networks, whereas MANETs are self-organized networks.

Some researchers have also used coalition game to ensure security in MANETs. Li et al [6] designed a self-healing wireless networks under insider jamming attacks. The concept of a pairwise key mentioned in their design shows that the design works best in a centralized system and not a self-organized system like MANETs. Some other works have only focused on node selfishness and not on intentional malicious acts or jamming attacks. Zhu et al [4] 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.

Our approach is unique in that (1) we refrain from treating the nodes in a collective manner, instead we consider them as individual node by defining a

security characteristic function for the coalition formation (2) we use reputation mechanism to prevent false positives (3) we kept a history of the nodes' transmission rates (4) we successfully identify the insider jammer and excluded it from the coalition.

3 Network and Jammer Model

3.1 Network Model

Our network model involves a characteristic function and a coalition formation model. This model is similar to related efforts [10] [11] [12] [13], [12]. It departs from the related efforts in the usage of accumulative feedback adaptation transmission rate (AFAT) [14] in the coalition formation; use of maximum transmission rate in security characteristic function; and the necessary conditions needed for the grand coalition formation.

Coation Formation Model According to [11], a coalition game is an ordered pair $\langle N, v\rangle$ where $N = (1, .., n)$ is the set of players [4] and v is the characteristic function.[5] By convention, $v(\phi) = 0$, where ϕ denotes the empty set [11].

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. Such an intersecting node will serve as the referee for a new node that seeks to join the coalition. Our coalition formation process depends on the transmission rate table that has been stored according to the previous work done by [14].

In [14], we proposed an accumulative feedback adaptation transmission rate (AFAT). AFAT is a decentralized approach to ensure the communication of transmission rates between neighboring nodes in a network. The knowledge of neighbor's transmission rates helps a node to adjust its own rate accordingly. In other words, AFAT provides the maximum transmission rates for the nodes in order to meet the specific application bandwidth requirements. According to AFAT, the transmission rates of the nodes is 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 during every time instant.

The final outcome of the coalition formation process is to form a stable grand coalition which comprises of 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.

There are N nodes in the network, for any coalition, $C \epsilon 2^N$[6] As mentioned previously, many literature [11] [12] have made use of the characteristic function in modeling a coalition game. This function helps to calculate the payoff of

[4] Any subset of N is called a coalition, and the set involving all players is called the grand coalition.

[5] The characteristic function v: $2^N \rightarrow R$ assigns any coalition $C \subseteq N$ a real number $v(C)$, which is called the worth of coalition C.

[6] The number of nodes in C is $|C|$.

individual nodes such that they can see their joining the coalition as a rational decision since rationality is a key assumption in game theory. [7]

A node has neighbors in its transmission range that can testify about its cooperation based on the transmission rate table updated at every time-slot. This testimony means that these neighboring node can give a firsthand information about the node when queried. Let $|G_i|$ be the set of neighboring nodes in the transmission range of node i, therefore, at time slot t, the support rate for a node i in a coalition C, is:

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

The transmission rate, $T_t(C)$, of coalition C at time, t, is another important parameter in the characteristic function, Li et al [12] on the other hand made use of the overlapping distance. The nodes' sharing of their transmission rate is very key to their admittance into the small coalition. In other 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 with 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 in a coalition C is given by:

$$D_t(C) = max\{T_t(C)\} \tag{2}$$

According to [12] the maximal admitting probability is given by:

$$A_t(C) = max_{j\epsilon C}\{\frac{\sum_{i\epsilon C} P_{ij}}{|C|} | C = \{i | i\epsilon C, i \neq j, P_{ij} \neq 0\}\} \tag{3}$$

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

$$v_t(C) = \begin{cases} 0, & \text{if } |C| = 1 \\ \alpha S_t(C) + \beta A_t(C) + \gamma D_t(C), & \text{if } |C| \geq 1 \end{cases} \tag{4}$$

These weight parameters α, β and γ can be used to 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

[7] The security characteristic function's key parameters, support rate, maximum transmission rate and maximal admitting probability, captures the node mobility in the MANET, a property not included in [11, 12] . The support rate is the neighbors in the node's transmission range. The maximum transmission rate in the coalition is provided by AFAT while the maximal admitting probability or cooperation probability is unchanged.

Table 1: A summary of notations provided for reference

Notation	Definition
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 the 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 respectively

for the maximum transmission rate using γ. The weights would have an impact on the coalition as a whole. It is important for these weights to add up to 1 in order to allow prioritization based on the topology of the network. Because of the nature of our network, we will give the highest weight to the maximum transmission rate parameter.

$$\alpha + \beta + \gamma = 1 \tag{5}$$

New nodes are accepted into the grand coalition based on the testimony from intersecting nodes in the smaller coalition. Nodes take some time to gain a good reputation within the small coalition before it can be accepted into the grand coalition. There is a possibility that a new node might fail to enter into the grand coalition if it is out of range from the intersecting node when the smaller coalition is merged into a grand coalition. This merging process continues while there are intersecting nodes to testify about the new nodes which ensures that the grand coalition will continue to grow, thereby providing more robust security. Algorithm 1 shows the coalition formation process. The coalition formation is a dynamic process and 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 looks to find a partner. The grand coalition is eventually formed only when two conditions are met: presence of an intersecting node to aid the merging and if $v(N)$ is atleast greater than the individual payoff of any disjoint smaller coalition.

There are no fixed number of neighbors for a particular node because of the mobile nature of the wireless environment. From our proposed model the size of

the grand coalition could be any size of three nodes and above. For rationality sake it is important to show the individual payoff of the nodes so that they would have a basis for joining a coalition. The individual payoff share is also found in [15]. For any node $i \epsilon\ C$, $\mid C \mid > 1$, the individual payoff [8] share is defined in eqn 6

Algorithm 1 Algorithm for Coalition Formation

1: *Start* for all nodes, N
2: Begin the 1^{st} 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 [14] with the rate of newest members
11: Begin the 2^{nd} 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**

$$x_t(i) = \frac{1}{|C|}(\alpha S_t(C) + \beta A_t(C) + \gamma D_t(C)) \tag{6}$$

Based on the characteristic function used, we will be making use of the core. The core states that the sum of total payoff of all members of the coalition must be greater than the value of that single payoff of any individual node [15] [11]. Hence looking at equations 4 and 6, we should be able to conclude that:

$$\sum_{i \epsilon C} x_t(i) \geq v_t(C) \tag{7}$$

The game only has a core if it satisfies the concept of core of the coalition game [11].

[8] Payoff computation is calculated using any of core, shapley value, or nucleolus.

Network Assumptions We assume N mobile nodes with A attackers, where A is less than $N/2$. [9] Below are the assumptions under which we present our work:

- All players (or nodes) are rational (i.e. they would always choose the strategy that benefits them the most).
- The network model does not adopt a hierarchical organization, such as, leader-follower or centralized organization.
- 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.
- 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.
- A node's continuous membership in the grand coalition is dependent on its reputation value.

3.2 Jammer Model

The jammer type modeled in this section is a smart insider jammer who only launches its attack after collecting enough information to cause huge network disruptions. The jammer's goal is to launch a successful attack rather than building a very high reputation, however, it has to wait until it crosses the lower reputation threshold value, q_L before attempting to jam the network. The potential jammer is first a member of a smaller coalition where it earns a good reputation from its neighboring nodes. The attack is a combination of both subtle and palpable attacks as explained in [16]. The attacker passively scans the network as an eavesdropper while also sharing its transmission rate with all the neighbors in its range of transmission in the coalition. After a certain time, at which the attacker has gathered enough information about its neighbors and what channel they are transmitting on, the attacker stops sharing its own transmission rate because it needs enough power to jam the channel on which the best transmission rate is used.

The jammer would launch its attack when it knows that such an attack is feasible. By feasible, we mean that the jammer has the required jamming power, the chance of being detected is low and it has specific information about the channel on which the best transmission rate is used. The jammer would launch its palpable attack by intentionally sending a high-powered interference signal to that channel, thereby attempting to disrupt communication. The principal aim of jamming a selected channel is to disable the functionality of that channel. The complexity of the jamming can be seen in the fact the movement of the jammers may hinder the detection capability of the coalition. In figure 1, the jammers are part of two smaller coalitions which merged to become a grand coalition. The node marked yellow is the intersecting node for smaller coalitions.

4 Proposed Defense Model

4.1 Maintaining the Coalition through Reputation

We present a maintenance algorithm that employs the node reputation to track all the history of each node's cooperation as they broadcast their transmission

[9] The number of attackers should not exceed the number of legitimate nodes.

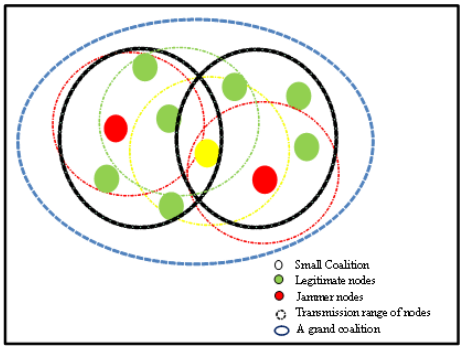

Fig. 1: A Coalition of ten (10) nodes with two (2) jammers

rate. Reputation is simply defined as the goodness of a node as observed by other neighbors in its transmission range or the coalition in general.[10] Specifically, we adapt the mechanism used for modeling increase and decrease of reputation values. The reputation of a node is maintained by nodes in the same transmission range as itself. Each node updates the reputation table every time slot.[11] When a node broadcasts it's transmission rate, it receives an increment and if it fails the opposite happens. A new node that joins the network can be assigned a neutral reputation q_N. All reputations would be 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 can be increased at the rate of σ and decreased at the rate of λ, where $\sigma, \lambda < 1$ and are both real numbers. For this algorithm, the two parameters are set equal to each other in order to ensure fairness. If these parameters are not made equal, for example when σ is larger than λ, there is the tendency for a node to quickly attain the maximum reputation value in a very short time and then lack the enthusiasm to continue sharing its transmission rate as it should be doing in order for network activity to continue. Also decreasing at a high rate also results in an undeserved punishment for any node in an unpleasant network location due to the mobility of the system.

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 i.e. 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 [17]. This algorithm makes use of only firsthand information as the support rate and the intersecting node is enough to cater for the need for a secondhand information.

[10] The maintenance algorithm was inspired by the the work done by [17].
[11] A time slot is defined as a period of time during which one transmission rate is shared.

Algorithm 2 Coalition Maintenance through Reputation

Assign values for σ and λ
Start for all nodes
Node i checks its transmission rate table to assign reputation value for neighbor j.
if j shares its transmission rate **then**
    compute reputation value according to:

$$v_{i,j}(y) = y/R_{i,j} \tag{8}$$

else
    Set $v_{i,j}(y) = 0$ if $y/R_{i,j} \leq b_f$
end if
if j refuses to share its transmission rate **then**
    compute reputation value according to

$$k_{i,j}(m) = m/R_{i,j} \tag{9}$$

else
    Set $k_{i,j}(m) = 0$ if $m/R_{i,j} \leq T_f$
end if
Node i updates node j's reputation value according to:

$$R_{i,j} = R^*_{i,j} + \sigma * (v_{i,j}(y)) - \lambda * (k_{i,j}(m)) \tag{10}$$

Store this reputation value in its reputation table
Share reputation table with neighbors at every time-slot.
return $R_{i,j}$
All nodes continue to update their reputation table.

4.2 Jammer's Exclusion from the Coalition

The jammer prevention algorithm aims to reduce the number of false positives. False positive occurs when a legitimate node is been classified as a jammer when it fails to share its transmission rate at a particular time-slot due to been out of range, which is typical of MANET. 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.

For our setup, an excluded node will not be granted re-entry. Algorithm 3 provides the needed self-dependency and self-organization in MANET.

5 Simulation and Results

We evaluate the performance of the reputation-based coalition game by conducting simulations in NS2. We compare the performance of the reputation-based coalition game with non-reputation based mechanism. The non-reputation based scheme is gotten when we remove the reputation mechanism in our coalition maintenance. The evaluation is based on four metrics: the detection accuracy, detection delay, the percentage of false positives and the detection time of the insider jammer.

5.1 Simulation Setup

Table II shows a list of the simulation parameters. Twenty percent of the nodes in the network are classified as the insider jammers.

Algorithm 3 Jammer Exclusion from the Coalition

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:

$$\begin{cases} jammer, & \text{if } R_{i,j} < q_L \\ regular, & \text{if } R_{i,j} \geq q_L \end{cases} \tag{11}$$

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

Table 2: Parameters for Simulation

Parameter	Level
Area	2300 x 1300
Speed	$15m/s$
Radio range	250m
Simulation time	130s
Number of mobile nodes	5, 10, 20, 40 and 80 nodes
Network interface & Channel type	Wireless
Transmission rate	1-11 Mbps
Percentage of jammer	20 percent
Thresholds, q_U & q_L	0.975 & 0.70 respectively

5.2 Results

In Fig. 2, we compare the detection accuracy of the reputation-based scheme with a non reputation-based scheme. The non-reputation based scheme only detects the insider jammer half of the time, our reputation-based scheme, however, performs better with increasing coalition size. In our simulation results, the scheme achieves the maximum accuracy with a coalition of 80 nodes. Detection accuracy is of utmost importance because it is the most important factor that helps to reduce the number of false positives and false negatives.

Fig. 3 illustrates the time taken by the coalition to detect the insider jammer. The support rate has an impact on the number of neighboring nodes which in turn affects the detection time. For the result shown in fig. 3, the number of

attackers is exactly twenty percent of the size of the coalition. The time taken to detect insider jammer reduces significantly with increasing number of nodes in the network.

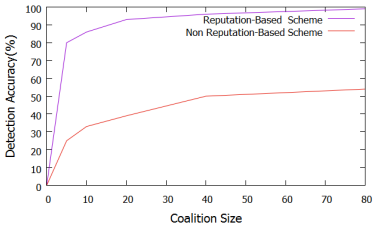

Fig. 2: Detection Accuracy

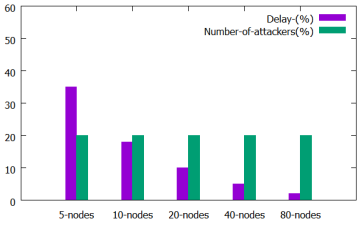

Fig. 3: Detection Delay

Fig. 4 compares false positives for the reputation-based model and the non reputation-based model. False positives are easily detected with our reputation-based mechanism because the rate of increase (σ) and decrease (λ) of reputation value is equal resulting in fewer instances of errors in detecting insider jammers. As observed in fig. 4, the 80 node coalition has the least false positive percentage.

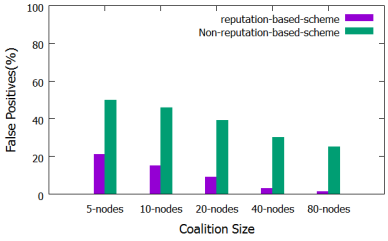

Fig. 4: False Positives

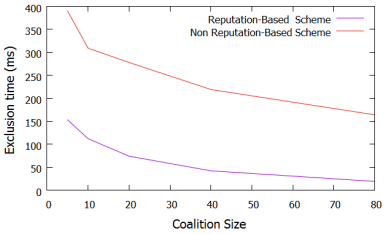

Fig. 5: Jammer Exclusion Time

Fig. 5 illustrates the time it takes to exclude the insider jammer from the grand coalition after detection. As the size of the coalition increases, the time taken to exclude insider jammers decreases because the jammer's neighboring nodes quickly raises an alarm when the reputation values fall below q_L.

6 Conclusion and Future Work

In this paper, we presented a reputation-based coalition game to detect insider threats in MANET. The key components of the game include algorithms for coalition formation, coalition maintenance and jammer exclusion and security characteristic function for admitting nodes into a coalition. Simulation results demonstrate the effectiveness of our reputation-based coalition game to detect insider jammers in a MANET. Specifically, the results demonstrate few false positives and small detection delay. In the future, we would like to investigate a case of a cooperative attacks that could occur when the excluded nodes form a coalition with the aim of jamming communication in the MANET.

Acknowledgment

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

References

1. A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A Survey on Jamming Attacks and Countermeasures in WSNs," *Communications Surveys & Tutorials, IEEE*, vol. 11, no. 4, pp. 42–56, 2009.
2. 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.
3. W. L. Stutzman and G. A. Thiele, *Antenna Theory and Design*. John Wiley & Sons, 2012.
4. 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.
5. H. Nguyen, T. Pongthawornkamol, and K. Nahrstedt, "ALIBI: A Novel Approach for Detecting Insider-based Jamming Attacks in Wireless Networks," *MILCOM Conference*, pp. 855–884, 2009.
6. L. Li, S. Zhu, D. Torrieri, and S. Jajodia, "Self-Healing Wireless Networks Under Insider Jamming Attacks," in *2014 IEEE Conference on CNS*. IEEE, 2014, pp. 220–228.
7. 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*. ACM, 2000, pp. 255–265.
8. 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*. Springer, 2002, pp. 107–121.
9. P. Michiardi and R. Molva, "A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad hoc Networks," in *WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, 2003, pp. 4–pages.
10. A. Peleteiro, J. C. Burguillo, J. L. Arcos, and J. A. Rodriguez-Aguilar, "Fostering Cooperation through Dynamic Coalition Formation and Partner Switching," *ACM (TAAS)*, vol. 9, no. 1, p. 1, 2014.
11. T. Ferguson, "Game Theory (2nd/ed)," *Mathematics Department, UCLA*, vol. 2014, 2014.
12. X. Li, "Achieving Secure and Cooperative Wireless Networks with Trust Modeling and Game Theory," 2009.
13. D. Gale and L. S. Shapley, "College Admissions and the Stability of Marriage," *The American Mathematical Monthly*, vol. 69, no. 1, pp. 9–15, 1962.
14. A. Al-Sharah and S. Shetty, "Accumulative Feedback Adaptation Transmission Rate in Mobile Ad-hoc Networks," in *2015 IEMCON*. IEEE, 2015, pp. 1–5.
15. W. Saad, Z. Han, M. Debbah, and A. Hjørungnes, "A Distributed Coalition Formation Framework for Fair User Cooperation in Wireless Networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 9, pp. 4580–4593, 2009.
16. X. Liao, D. Hao, and K. Sakurai, "Classification on Attacks in Wireless Ad hoc Networks: A Game Theoretic View," in *7th International Conference on NCM, 2011*. IEEE, 2011, pp. 144–149.
17. A. Balasubratuanian and J. Ghosh, "A Reputation Based Scheme for Stimulating Cooperation in MANETs," *Proc. of the 19th International Teletraffic Congress*, 2005.