A Cooperative Approach for Analyzing Intrusions in Mobile Ad hoc Networks

Hadi Otrok, Mourad Debbabi, Chadi Assi and Prabir Bhattacharya
Computer Security Laboratory
Concordia Institute for Information Systems Engineering (CIISE)
Concordia University, Montreal (QC), Canada
E-mail: {h_otrok, debbabi, assi, prabir}@ciise.concordia.ca

Abstract

In this paper, we consider the problem of reducing the number of false positives generated by cooperative Intrusion Detection Systems (IDSs) in Mobile Ad hoc Networks (MANETs). We define a flexible scheme using security classes, where an IDS is able to operate in different modes at each security class. This scheme helps in minimizing false alarms and informing the prevention system accurately about the severity of an intrusion. Shapley value is used to formally express the cooperation among all the nodes. To the best of our knowledge, there has not been any study for the case where the intrusions in MANETs are analyzed, in order to decrease false positives, using cooperative game theory. Our game theoretic model assists in analyzing the contribution of each mobile node on each security class in order to decrease false positives taking into consideration the reputation of nodes. Simulation results are given to validate the efficiency of our model in detecting intrusions and reducing false positives.

1. Introduction

In MANET, decision-making, key-distribution, routing and forwarding packets are usually decentralized and many of them depend on the cooperative participation among all nodes [15]. This dependency of MANET on a decentralized paradigm allows an adversary to exploit new type of attacks that are designed to destroy the cooperative algorithms used in ad hoc networks [10]. MANET is particularly susceptible to several attacks ranging from passive eavesdropping to active interfering due to their open medium; this is in contrast to wired networks, where an adversary must gain physical access to the network wires to be able to make such type of attacks. Most ad hoc routing protocols rely on the cooperation between all mobile nodes that exploit new form of attacks that does not exist in wired networks [5]. An intruder that compromises a mobile node can destroy the communication by broadcasting false routing information, providing incorrect link state information, and overflowing other nodes with unnecessary routing traffic [14]. Ultimately, this could lead to a Denial of Service (DoS) attack. Firewalls and encryption techniques are no longer sufficient and effective for protecting MANETs due to the large number of attacks that could be initiated by an intruder. A cooperative intrusion detection system is needed to detect intrusions and consequently generate an appropriate response [7]. Detecting an unusual activity will be done through monitoring the network [13]. False-alarms are considered as one of the main problems that IDS is facing, significantly making it less trustworthy. The IDS will generate false-alarms or false positives when it considers normal data or traffic as intrusions [15]. For example, an IDS might consider a large number of routing requests received by a mobile node as intrusion. While these routing requests are generated due to a loss of many links or many nodes are no more participating.

Our main contribution in this paper is to increase the efficiency of intrusion detection system, in MANET, by decreasing the false-positives. Cooperative game theory (Shapley value) [3] is used to analyze the contribution of each node in detecting an intrusion. Here, we specifically consider cache poisoning and malicious flooding intrusions [6]. In the former, an adversary can compromise the information in the routing table by modifying its content, deleting information from it, or by injecting false information. The latter is flooding the whole network or some victim nodes with large amount of data or control packets. This leads to DoS via consuming the victim nodes’ resources (e.g., battery, CPU). In our study, we introduce an aggregate function to calculate the severity of the intrusion according to the values reported by the nodes. Moreover, we consider the reputation of the nodes in the aggregate function. The reputation of a node reflects its behavior when...
detecting an intrusion. Then, we introduce a set of security classes depending on the value of the function. The security classes help on reducing false positives by choosing a security class according to the severity of the intrusion. According to the selected class an appropriate response is taken. Shapley value helps in analyzing the contribution of each mobile node on each security class in order to decrease the false positives. Finally, we present our simulation results to validate our model.

This paper is organized as follows: Section 2 presents related work done on IDS and game theory. Section 3 presents the cooperative intrusion detection in MANET. This section presents our proposed model in MANET, our security classes, and the game theoretic framework followed by an illustrative example and simulation results. Section 4 illustrates our conclusion.

2. Related Work

The security difference between wired infrastructure networks and mobile ad hoc networks [10] motivated researchers to model an IDS that can handle the new security challenges such as securing routing protocols. A cooperative intrusion detection model has been proposed in [15], where every node participates in running its IDS in order to collect and identify possible intrusions. If an anomaly is detected with weak evidence, a global detection process is initiated for further investigation about the intrusion through a secure channel. This model suffers from performance penalties and false alarm rates. An extension of this model was proposed in [6], where a set of intrusions can be identified with their corresponding source. Moreover, authors addressed the problem of run-time resource constraint by IDS through modeling a repeatable and random head cluster election framework. Watchdog and pathrater were proposed in [11] to improve the throughput in MANET in the presence of misbehaving nodes. Watchdog goal is to identify the compromised nodes in the network while pathrater goal is to notify the routing protocols from using misbehaving nodes. This model did not propose any punishment procedure that could motivate nodes to behave normally. Hence, misbehaving nodes can continue operating in the network and benefiting from others’ services. CORE [9] is a cooperative enforcement mechanism based on a monitoring and reputation systems. The goal of this model is to detect selfish nodes and enforce them to cooperate. Each node keeps track of other nodes’ cooperation using reputation as the cooperation metric. CORE ensures that misbehaving nodes are punished by gradually stopping communication services and provides incentives for nodes, in the form of reputation, to cooperate. Note that, reputation is calculated based on data monitored by local node and information provided by other nodes involved in each operation.

Game theory [12] was successfully used in many disciplines including economics, political science and computer science. Currently, it has been used to address problems where multiple players with different objectives can compete and interact with each other [1]. To predicate the optimal strategy used by intruders to attack a network, the authors of [8] modeled a non-cooperative game theoretic model to analyze the interaction between intruders and IDS in wired infrastructure networks. In [2], the authors aimed at demonstrating the suitability of game theory for development of various decision, analysis, and control algorithms in intrusion detection. They accomplished this by addressing some of the basic network security tradeoffs, and giving illustrative examples in different platforms. They proposed two different schemes, based on game theoretic techniques. They considered a generic model of a distributed IDS with a network of sensors. Finally, one can conclude that game theory is a strong candidate to provide the much-needed mathematical framework for analyzing the interaction between the IDSs in MANET to reduce false positives.

3. A Cooperative Approach for Analyzing Intrusions

In this section, we present the model under which our cooperative intrusion detection will work. Additionally, security classes that will be used by the IDS to determine the severity of the intrusion. Finally, our game theoretic framework is presented with an illustrative example followed by simulation results.

3.1. The Model

Our MANET is modeled as an undirected graph \( G = (N, E) \), where \( N = \{N_1, ..., N_l\} \) is the set of mobile nodes. We describe our model as a cooperative distributed intrusion detection system, where every node in the network participates in detecting and responding to intrusions. Furthermore, every mobile node runs an IDS locally to perform local data collection and anomaly detection. Cooperative detection is needed between mobile nodes due to the characteristics of MANET [16]. In our study, we take into consideration two common intrusions: Cache poisoning and malicious flooding. In the former, an adversary can compromise the information in the routing table through modifying its content, deleting information from it, or by injecting fake information. Malicious flooding is to flood the whole network or some victim nodes with large amount of data or control packets. This leads to DoS via consuming the victim’s resources (e.g. battery). Here, cooperation between mobile nodes is needed to detect the intrusion with low false positives. This model is illustrated in Figure 1.
We define respectively the sets of cache poisoning and malicious flooding as follows: \( C = \{0, 1\} \) and \( M = \{0, 1\} \). Each node is able to detect both intrusions. We define a one-to-one mapping \( O \) from the set of nodes \( N \) to \( C \times M \), i.e. \( O : N \rightarrow C \times M \), where \( O(N_i) = (c_i, m_i) \) means node \( N_i \) has detected cache poisoning (malicious flooding) attack, if \( c_i (m_i) \) is equal to one and has not detected otherwise. These sets will be used later on to indicate whether a node has sensed an intrusion or not. For example, if cache poisoning has been detected by a node then \( c_i \) is equal to one and zero otherwise. This result varies from one node to another according to how much the node cares for detecting an intrusion that was not directly initiated to it but rather could have some impact on it.

### 3.2. Security Classes of the IDS

False-alarms are considered as one of the main problems that IDS is facing, significantly making it less trustworthy. Our objective in this paper is to increase the efficiency of intrusion detection system by decreasing the false-positives. This will be achieved by proposing a function \( f \) that represents both attacks (malicious flooding and cache poisoning) and mapping the severity of an intrusion to its corresponding security class. Moreover, a set of thresholds is used to tune the security classes in order to have a trustworthy IDS.

Using the model in the previous subsection, now we introduce the function \( f : N \rightarrow \mathbb{R}^* \) to be the following:

\[
 f(N_i) = c_i \frac{NFP(N_i)}{NR\_ack(N_i)} + m_i \frac{NRP(N_i)}{ENRP(N_i)}
\]

where,

- \( NFP(N_i) \) is the number of packets forwarded by node \( N_i \).
- \( NR\_ack(N_i) \) is the number of received acknowledgments by node \( N_i \).
- \( NRP(N_i) \) is the number of received packets by node \( N_i \).
- \( ENRP(N_i) \) is the expected number of received packets by node \( N_i \). In [6], it is defined as MaxCount.

This function aggregates both the cache poisoning and malicious flooding attacks in order to detect an intrusion (with respect to a corresponding node). If the node does not receive any acknowledgments for the packets it sent, it would assume that the packets did not reach their destinations and therefore \( NR\_ack \) will be less than \( NFP \). This means that there is a problem in the routing protocol that could be due to a cache poisoning attack. The higher the loss rate is, the higher is the probability of the cache poisoning. For example, if \( NFP(N_i) \) is equal to 20 and \( NR\_ack(N_i) \) is equal to 5 then the ratio is 4 while in normal cases the ratio must be equal to 1. This fraction is multiplied by \( c_i \) since node \( N_i \) can have a ratio which is greater than 1 but at the same time the node does not need to participate in detecting that intrusion for many reasons, such as being a selfish node.

On the other hand, if the node is receiving packets with a rate that is greater than the expected rate, i.e., \( NRP(N_i) > ENRP(N_i) \), then it would assume that there is a risk of malicious flooding attack. The higher the loss rate, the higher is the probability of malicious flooding. For example, if \( NRP(N_i) \) is equal to 40 and \( ENRP\_ack(N_i) \) is equal to 10 then the ratio is equal to 4 while in normal cases the ratio must be equal to 1. This indicates the possibility of malicious flooding attack. Note that, the value of \( ENRP(N_i) \) depends on a previously trained data that was practiced under different circumstances. The fraction \( \frac{NRP(N_i)}{ENRP(N_i)} \) is multiplied by \( m_i \) since node \( N_i \) can have a ratio which is greater than 1 but at the same time \( N_i \) does not need to participate in detecting that intrusion for many reasons, such as being a selfish node. The function \( f(N_i) \) reflects the severity of the attack sensed by node \( N_i \). Note that, this function is easily extendable, if one needs to study other kinds of attacks. Our objective behind this work is to study how we can decrease the false positives by analyzing the intrusions reported by the mobile nodes in the network.

To decrease false positives, we propose the concept of security classes to be \( CL = \{c_{l1}, \ldots, c_{lk}\} \). This enables us to respond better to an intrusion depending on which security class it belongs to. Our IDS is made up of \( k \) security classes, each class representing the severity of the attack. We introduce the set of \( k - 1 \) thresholds \( T \) to categorize the security classes, where \( T = \{t_1, \ldots, t_{k-1}\} \). Now, we
introduce the aggregate function to be:

\[ F(N) = \sum_{N_i \in N} r_{N_i} \times f(N_i) \]  

where \( r_{N_i} \) is the reputation for node \( N_i \). This reputation is calculated in the same way as in [9]. This function, \( F(N) \), will be calculated by a node that suspects an intrusion and has asked other nodes to sense it. Moreover, it sums up the severity of the attack reported by each node, \( N_i \), in a cluster, \( N \), while considering the reputation of each node. The reputation, \( r_{N_i} \), will be valued according to statistical data depending on the nodes’ previous behavior as in [9]. The value of \( r_{N_i} \) is normalized between 0 and 1. Now, we categorize the security classes as follows:

\[
CL = \begin{cases} 
  c_l & \text{if } F(N) < t_1 \\
  c_{l_i} & \text{if } t_{i-1} \leq F(N) < t_i; \ i \in [2, k-1] \\
  c_{l_k} & \text{if } F(N) \geq t_{k-1}
\end{cases}
\]

(3)

Categorizing the severity of an intrusion with respect to different security classes will help in decreasing the probability of the false positives and give the response system much more accurate information about the intrusion. We can use statistically trained data to assign values to thresholds \( T \) and security classes \( CL \) in order to have better results (i.e., to reduce false positives). Here, cooperative game theory will be used to formally illustrate the problem.

3.3. Cooperative Game Theory

The design and analysis of our proposed model will be done using cooperative game theory [3]. The \( l \) mobile nodes will be modeled as a set \( N \) of \( l \) players in an \( N \)-person game with \( N = \{N_1, \ldots, N_l\} \) [12]. We introduce a coalition in cooperative game theory to be:

\[ \Delta \subseteq N \text{ and } \forall x \in \Delta, \]

\[ O(x) = (1, 1) \text{ or } O(x) = (0, 1) \text{ or } O(x) = (1, 0) \]

(4)

In other words, we define a coalition to be a set of nodes, where each node reports at least one type of intrusion. Therefore, each node in \( \Delta \) reports a risk in the MANET. Let \( \delta \) be the number of elements in a coalition in the MANET. We use the aggregate function over \( \Delta \),

\[
\sum_{x \in \Delta} r_x \times f(x)
\]

to assign the intrusion to its equivalent security class \( cl_j \).

Assigning an anticipated marginal contribution to each player (node) in the game with respect to a uniform distribution over the set of all permutations on the set of players will be presented by Shapley value [3]. To find the contribution of node \( N_i \) in coalition \( \Delta \), we consider all the different permutations for the nodes, \( \Pi_\Delta \), in the coalition. Then we calculate the difference between the function including all nodes in the permutation before node \( N_i \), including \( N_i \), and the function of all nodes prior to \( N_i \), excluding \( N_i \). We define \( P_{\pi N_i}^N \) to be the set of nodes before the node \( N_i \) in the permutation \( \pi \in \Pi_\Delta \). Then taking the average of all these differences, we get the marginal contribution of node \( N_i \) in coalition \( \Delta \). In other words, the contribution would be the following:

\[
\phi_{N_i}(\Delta) = \frac{1}{\delta!} \sum_{\pi \in \Pi_\Delta} F(P_{\pi N_i}^N \cup \{N_i\}) - F(P_{\pi N_i}^N) \tag{5}
\]

Replacing \( F(P_{\pi N_i}^N \cup \{N_i\}) \) by \( \sum_{x \in P_{\pi N_i}^N \cup \{N_i\}} r_x \times f(x) \) and \( F(P_{\pi N_i}^N) \) by \( \sum_{x \in P_{\pi N_i}^N} r_x \times f(x) \), Equation (5), then reduces to the following:

\[
\phi_{N_i}(\Delta) = \frac{1}{\delta!} \sum_{\pi \in \Pi_\Delta} F(\{N_i\}) \tag{6}
\]

which simply reduces to the following:

\[
\phi_{N_i}(\Delta) = F(\{N_i\}) \tag{7}
\]

Now, to calculate the marginal contribution (Shapley value) of node \( N_i \), in the MANET, we should take the average of this value over all possible coalitions, which is:

\[
\phi_{N_i} = \frac{1}{\gamma} \sum_{N_i \in \Delta, \Delta \in N} F(\{N_i\}) \tag{8}
\]

where \( \gamma \) is the number of possible coalitions in the MANET. Coalitions with enough power to impose a decision collectively are called winning coalitions. Here, a coalition is a winning coalition if the aggregation of their values can change the security class. Therefore, the value of a coalition corresponding to a class is either zero or one. It is one in the case of a winning coalition and zero otherwise. Thus, the effect of node \( N_i \) on security class \( cl_j \) can be written as \( \frac{1}{|\Delta'|} \), where \( \Delta' \) is the set of the winning coalitions: i.e. \( \sum_{N_i \in \Delta'} F(\Delta') \geq t_i \).
Using equation 8, we calculate in the following table the contribution of each node on each security class as shown in Figure 3. In this Figure for example, the contribution of node $N_3$, with other nodes in the coalition, changes the security class of the cooperative IDS from $cl_3$ to $cl_4$, which means that the risk behind the detected intrusion is high and an immediate cooperative or local response is needed. Now, we use $\sum_{N_i \in \Delta'} F(\Delta') \geq t_i$ to find the winning coalitions. For example, the winning coalitions that decide the change from security class $cl_3$ to security class $cl_4$, where $N_3$ belongs to these coalitions is the following set: $\{\{N_2, N_3, N_5\}, \{N_1, N_2, N_3, N_5\}, \{N_2, N_3, N_4, N_5\}, \{N_1, N_2, N_3, N_4, N_5\}\}$. 

3.4. Illustrative Example

Consider five mobile nodes communicating with each other in MANET as shown in Figure 2. One of the mobile nodes received abnormal number of route-requests from other nodes asking for routing information. The node that received such type of abnormal number of route-requests has to check whether this amount is due to loosing many links in the network, many nodes are no more participating, or due to malicious flooding. So, the node has to cooperate with its neighbor nodes to decide if it is under attack or not.

Consider that we have four security classes $CL = \{cl_1, cl_2, cl_3, cl_4\}$. The threshold set $T = \{2, 4, 6\}$, the security classes $CL$ are classified as follows: $cl_1 < 2$, $2 \leq cl_2 < 4$, $4 \leq cl_3 < 6$, $cl_4 \geq 6$, the reputation of nodes $r_1 = 0.5$, $r_2 = 0.8$, $r_3 = 0.2$, $r_4 = 0.5$, $r_5 = 0.6$, and $f(1) = 3$, $f(2) = 4$, $f(3) = 1$, $f(4) = 2$, $f(5) = 5$. Using equation 8, we calculate in the following table the participation of each node in detecting the intrusion.

<table>
<thead>
<tr>
<th>Nodes</th>
<th>N1</th>
<th>N2</th>
<th>N3</th>
<th>N4</th>
<th>N5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contriibution value</td>
<td>19.2</td>
<td>40.96</td>
<td>2.56</td>
<td>12.8</td>
<td>38.4</td>
</tr>
</tbody>
</table>

Moreover, using $\frac{1}{|\Delta'|}$, we evaluate the contribution of each node on each security class as shown in Figure 3. In this Figure for example, the contribution of nodes received abnormal number of route-requests from other nodes asking for routing information. The node that receives such amount has to check whether this amount is due to losing many links in the network, many nodes are no more participating, or due to malicious flooding. So, the node has to cooperate with its neighbor nodes to decide if it is under attack or not.
Our simulation results are given in Figure 4. This figure illustrates a comparison between our model and the classical one. It is clear from the figure that our model has better results with respect to false positives and efficiency in detecting intrusions. This is because we analyze the contribution of nodes in detecting an intrusion using game theory taking into consideration the reputation of the nodes. According to the analyzed results a security class is chosen and an immediate response is generated. The security class model helps in classifying the severity of an intrusion. On the other hand, the classical model does not support different security classes and cannot analyze the contribution of the nodes in detecting an intrusion.

4. Conclusion

We considered the problem of decreasing false positives generated by cooperative IDS in MANETs. We analyzed the intrusion detected by mobile nodes within a cooperative game theoretic framework. Furthermore, we introduced an aggregate function to measure the severity of the intrusion reported by the nodes in MANET. We devised a flexible scheme using security classes with the IDS being able to operate in different modes at each security class. This helped on decreasing the number of false positives. Our function, classifies the intrusion into one of our predefined security classes with its associated intrusion response. We tuned the thresholds for the security classes, using previous trained data, in order to decrease the number of false alarms. In our study, we specifically took into consideration cache poisoning and malicious flooding intrusions. Finally, Shapley value was used to formally express the contribution of each node in detecting an intrusion in MANETs. Our simulation results showed that our model provides better results compared to a classical one.

References


