Titre: Title:	A trust-based game theoretical model for cooperative intrusion detection in multi-cloud environments
Auteurs: Authors:	Adel Abusitta, Martine Bellaïche et Michel R. Dagenais
Date:	2018
Type:	Communication de conférence / Conference or workshop item
Référence: Citation:	Abusitta, A., Bellaïche, M. & Dagenais, M. R. (2018, février). *A trust-based game theoretical model for cooperative intrusion detection in multi-cloud environments.* Communication écrite présentée à 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN 2018), Paris, France (8 pages). doi:10.1109/icin.2018.8401625

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/4199/
Version:	Version finale avant publication / Accepted version Révisé par les pairs / Refereed
Conditions d'utilisation: Terms of Use:	Tous droits réservés / All rights reserved

Nom de la conférence: Conference Name:	21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN 2018)
Date et lieu: Date and Location:	19-22 février 2018, Paris, France
Maison d'édition: Publisher:	IEEE
URL officiel: Official URL:	https://doi.org/10.1109/icin.2018.8401625
Mention légale: Legal notice:	© 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

A Trust-based Game Theoretical Model for Cooperative Intrusion Detection in Multi-cloud Environments

Adel Abusitta, Martine Bellaiche, and Michel Dagenais
Department of Computer and Software Engineering
Ecole Polytechnique de Montreal
Montreal, Canada
{adel.abusitta,martine.bellaiche,michel.dagenais}@polymtl.ca

***Abstract*—Cloud systems are becoming more complex and vulnerable to attacks. Cyber attacks are also becoming more sophisticated and harder to detect. Therefore, it is increasingly difficult for a single cloud-based intrusion detection system (IDS) to detect all attacks, because of limited and incomplete knowledge about attacks. The recent researches in cyber-security have shown that a co-operation among IDSs can bring higher detection accuracy in such complex computer systems. Through collaboration, a cloud-based IDS can consult other IDSs about suspicious intrusions and increase the decision accuracy. The problem of existing cooperative IDS approaches is that they overlook having untrusted (malicious or not) IDSs that may negatively effect the decision about suspicious intrusions in the cloud. Moreover, they rely on a centralized architecture in which a central agent regulates the cooperation, which contradicts the distributed nature of the cloud. In this paper, we propose a framework that enables IDSs to distributively form trustworthy IDSs communities. We devise a novel decentralized algorithm, based on coalitional game theory, that allows a set of cloud-based IDSs to cooperatively set up their coalition in such a way to make their individual detection accuracy increase, even in the presence of untrusted IDSs.**

***Keywords*-Intrusion detection systems; game theory; cloud computing; security; trust.**

I. Introduction

Cloud-based cyber-attacks are known to be more complex and harder to detect. It became significantly more difficult for a traditional single intrusion detection system, whether it is network-based, hypervisor-based, or VM-based, to detect all attacks, due to limited knowledge about attacks. Collaboration among intrusion detection systems (IDSs) can be exploited to gain higher detection accuracy as compared to traditional single IDS [1]. Through collaboration, IDSs in different regions, and possibly, belonging to different Cloud Providers (CPs) can cooperate in such a way that makes them utilize the expertise of each other to cover and identify unknown attack patterns.

A cloud-based IDS can be classified into two types; signature-based and anomaly-based [2]. The former compares suspicious behavior with known attack patterns. In order to make signature-based effective, the signature database should be updated frequently. On the other hand, anomaly-based IDS raises alarms when unusual and/or unexpected observations are detected. Anomaly-based IDSs are effective to detect unknown attacks. Moreover, they do not need a database of known attacks. However, the shortcoming of using anomaly-based detection is the relative high false positive rate compared to the signature-based technique [1]. IDSs may adopt both techniques to have improved detection accuracy. However, the detection accuracy is limited by the amount of knowledge they have (e.g., their security vendors have). Recent research [1] [3] shows that the collaborative detection can enhance the detection rate up to 60%. Through collaboration, an IDS can benefit from other IDSs expertise by consulting them about suspicious behavior. The feedback received can be then used to decide whether to rise an alarm or not.

The main limitation of existing cloud-based cooperative IDS (e.g. [4] [5] [6] [7] [8] [9]) is that they work under the assumption that all IDSs are trustable, which lets their collaboration systems vulnerable to untrusted (malicious or not) insiders.

To address the aforementioned problems, we propose a trust-based framework for cooperative IDS in a multi-cloud environment. The framework can be summarized as follows. We enable an IDS to evaluate other IDSs' trustworthiness. This is done by considering its personal experience using bayesian inference. After obtaining IDSs' trust values, a coalition formation algorithm is used, that is based on the coalitional game theory [10]. The algorithm enables IDSs to leave or join a given coalition in such a way that enhances its chance to work with trusted IDSs. Thereafter, we propose a feedback aggregation algorithm, that is based on the

Dempster-Shafer Theory (DST) [11], to enable an IDS inside a coalition to aggregate feedbacks from different IDSs about suspicious intruders, which helps make the optimal decision in terms of detection accuracy.

Unlike similar proposals (e.g. [12]), we adopt a distributed approach in which each IDS autonomously makes its own decisions. This, in turn, avoids the problem of finding a third party that is agreed by all the IDSs. Also, it reduces the instability inside the coalition due to a single point of failure. In summary, our work consists of the following contributions:

- Modeling and proposing a framework that enables cloud-based IDSs to distributively form trustworthy IDS communities. More specifically, we present a systematic approach that considers the trustworthiness of IDSs through creating cooperative IDS.
- Proposing a new trust evaluation approach, based on Bayesian inference, that enables a cloud-based IDS to evaluate another IDS's trustworthiness based on its personal experiences.
- Devising an algorithm, based on coalitional game theory, that enables a set of cloud-based IDSs to cooperatively establish their coalition in such a way to increase their individual detection accuracy in the presence of untrusted IDSs. The proposed algorithm converges to a Nash-stable situation; that is, no IDS has an incentive to leave its current coalition to move to another coalition.

The rest of this paper is organized as follows. In Section II, we discuss the related work. We present the trust-based cooperative intrusion detection system in Section III. In Section IV, we present our empirical results to show the effectiveness of the proposed approach. Finally, Section V concludes the paper.

II. Related Work

Cloud-based cooperative IDSs have been proposed in many works in the past. For example, Lo et al. [13] propose a cooperative detection approach within the cloud computing environment. Alerts are exchanged between the cloud environment nodes (i.e., hosts) whenever an attack gets detected. They use a rule-based technique to detect TCP SYN attacks by fetching the threshold for rule patterns through the initial rule establishment phase. The main advantage of this approach is that it is able to distribute the detection overhead between the cloud nodes. Recently, Teng et al. [14] proposed an approach that combines two detectors: a feature detector and a statistical detector. The feature detector uses SNORT to separate events based on network protocols (e.g., TCP). The statistical detector cooperates with the feature detector by using data packets from it to determine whether an event is an attack or not. If the rate of packets obtained exceeds the predefine threshold, then this case will be considered as an attack.

Man and Huh [4] and Singh et al. [5] proposed a cooperative IDS between cloud computing regions. Their method allows exchanging alerts from multiple elementary detectors. In addition, they enable the exchange of knowledge between interconnected clouds. Ghribi [6] proposed a middleware IDS. The approach enables a cooperation between cloud IDS layers: Hypervisor-based IDS, Network-based IDS and VM-based IDS. If an attack is detected in a layer, the attack cannot be executed in the other layers. Chiba et al. [7] introduced a cooperative network-based cooperative intrusion detection system to identify network attacks in the cloud environment. This can be done by monitoring network traffic while maintaining performance and service quality.

The main limitation of the above mentioned approaches is that they work in the assumption that all IDSs are trustable, which makes their collaboration systems vulnerable to malicious insiders. The aim of this paper is to present a systematic approach to build a cloud-based cooperative IDS that adopts trust assessment mechanisms and supports trustworthy aggregation decisions. The proposed approach should work in the presence of untrusted cloud-based IDSs .

In a multi-cloud environment, Dermott et al. [12] proposed a cooperative intrusion detection in federated cloud environments. They use the Dempster-Shafer theory of evidence to collect the beliefs provided by the watching entities. The collected beliefs are used to make the final decision regarding a possible attack. The main limitation of this approach is that it is based on a centralized architecture, whereby a trusted third-party called broker is responsible for collecting feedback and managing intrusion detection.

In a non-cloud environment, a cooperative IDS has also been recently proposed in [15] [16] [17] [18] [19] [20] [21] [22]. However, these works also have the limitation of the above mentioned approaches, since they rely on the assumption that all IDSs are trustable, which makes their collaboration system vulnerable to malicious insiders.

A trust-based cooperative IDS has been proposed in a non-cloud environment. For example, Fung and Zhu [1] present a trust-based collaborative decision framework. Through cooperation, a local intrusion detection system (IDS) can detect new attacks that may be known to other IDSs, which may be from different security vendors. They study how to utilize the diagnosis from different IDSs to perform intrusion detection. They present a system architecture of a collaborative IDS in which trustworthy feedback aggregation is a key component. Similarly, Zhu et al. [23] [24] proposed an incentive-based communication protocol, which provides IDS nodes incentives to send feedbacks to their peers, and thus to prevent malicious behaviors. The main limitation of the existing trust-based cooperative IDS is that it considers a consultation request to be sent to many IDSs in order to get a feedback. This in turn causes extra overhead, through consulting needlessly some IDSs (i.e., untrusted IDSs). This is unlike our approach, where we use a coalitional game, in order to construct a set of trusted IDSs and thus minimise the number of consultation requests while guaranteeing higher detection accuracy.

In general, for a multi-cloud environment, a decentralized framework that considers trustworthiness of IDSs during the cooperation had yet to be addressed. Thus, in this paper, we present a trust-based cooperative IDS in a multi cloud environment. This in turn, enhances the detection accuracy compared to the existing cooperative and non-cooperative IDSs.

III. The Proposed Trust-based Cooperative IDS

In this section, we present a trust-based cooperative IDS in a multi-cloud environment. The section is divided into the following subsections: trust evaluation, trust-based coalition formation algorithm and feedback aggregation (Fig. 1).

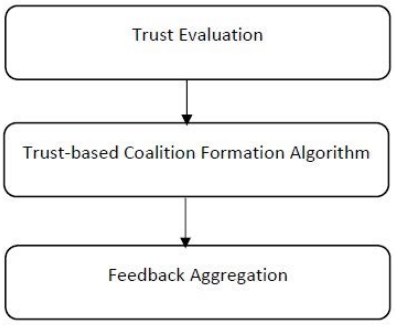

Fig. 1: Proposed Methodology

A. Trust Evaluation

A cloud-based IDS can evaluate the trust value of another IDS based on its personal experience with that IDS. We adopt a Bayesian inference approach to compute the trust value of an IDS [25]. The Bayesian inference was chosen because it is well-founded to derive trust values [26]. When the cloud-based IDS consults another IDS regarding a suspicious intruder, the received feedback and the revealed result (i.e., attack or not) are used to update the trust value of the consulted IDS. The trust value can be promoted if the IDS successfully diagnosed the consultation request about a suspicious intruder and it can be demoted otherwise. The trust value here represents and shows the accuracy of the IDS diagnosing suspicious attacks. An IDS $i \in \mathscr{N}$, where $\mathscr{N}$ is a set of IDSs, is endowed with a belief function, which computes the trust level of another IDS $j \in \mathscr{N}$. The new trust value t'_j is derived from the old trust value t_j as follows:

$$t'_j = F(t_j; \alpha_j, \beta_j) \tag{1}$$

where F is the regularized incomplete beta function [25], which is also the cumulative beta distribution function of the following beta probability density function:

$$f(x; \alpha_j, \beta_j) = \frac{x^{\alpha_j - 1}(1-x)^{\beta_j - 1}}{\mathbf{B}(\alpha_j, \beta_j)} \tag{2}$$

B represents the complete beta function. The value of α_j and β_j are updated after receiving the feedback from an IDS j. β_j is increased when the IDS j successfully diagnoses the consultation request. Equation (4) describes the update of β_j.

$$\beta_j = \beta_j \times (1 + \rho_j) \tag{3}$$

where ρ_j represents the weight of the diagnosed consultation request if it is successful and 0 if not.

Equation (4) describes the update of α_j.

$$\alpha_j = \alpha_j \times (1 + \gamma_j) \tag{4}$$

where γ_j denotes the weight of the diagnosed consultation request if it is unsuccessful and 0 if not.

The values of ρ_j and γ_j should be carefully set by an IDS i who is requesting feedback about a suspicious attack from other IDSs. These values reflect the detection difficulty degree of the suspicious intruder. A higher value of β_j will increase the trust of an IDS j while a higher value of α_j will decrease it.

The initial trust value t_j is obtained at the beginning during the testing period. The total reported diagnosis data from peer IDS j is denoted by the set $\mathscr{M}_j$. The initial trust value represents the total number of consultation requests that have been successfully diagnosed over the total number of consultation requests:

$$t_j = \frac{\sum\limits_{k \in \mathscr{M}_j} r_{j,k}}{|\mathscr{M}_j|} \tag{5}$$

Where the parameter $r_{j,k}$ is the revealed result of the k-th diagnosis request: $r_{j,k}$ =1 indicates successful diagnosis of the k-th request. $r_{j,k}$ =0 indicates otherwise.

The initial value of α and β can be obtained as follows:

$$\alpha_j = \sum_{k \in \mathscr{M}_j} (1 - r_{j,k}) \tag{6}$$

$$\beta_j = \sum_{k \in \mathscr{M}_j} (r_{j,k}) \tag{7}$$

B. A Trust-based Coalition Formation

In this section, we model the problem of cooperative IDS as a coalition formation cooperative game with non-transferable utility [27].

1) Characterization: The proposed coalition formation algorithm is a hedonic coalitional game [27], [28] [29] [30], a category of coalition formation games [10], [28], [31] in which each agent (i.e. IDS) acts selfishly, and its preferences for a coalition depend only on the members of that coalition. A hedonic game is used due to the fact that finding the optimal coalition structure, in coalition formation, is NP-complete [32]. Therefore, a hedonic game, which satisfies stability features was used. Stability indicates that none of the coalition members (i.e. IDSs) finds an incentive to leave its current coalition and join another one.

To establish the model, a preference relation function is defined. This allows each IDS to order and to compare all the possible coalitions it belongs in order to make preferences over them. For any IDS $i \in \mathscr{N}$, where $\mathscr{N}$ is a set of IDSs, a preference relation $\succ_i$ is defined as a transitive binary relation over the set of all coalitions that IDS i can form [27]. Specifically, for any IDS $i \in \mathscr{N}$, and given two coalitions C_1, C_2, the notation $C_1 \succ_i C_2$ means that IDS i prefers being a member of C_1 rather than C_2.

In our coalition formation game, the preference function of the IDSs can be defined as follows:

$$C_1 \succeq_i C_2 \Longleftrightarrow f_i(C_1) \geq f_i(C_2) \tag{8}$$

where C_1, $C_2 \subseteq \mathscr{N}$ are two coalitions containing IDS i, and $f_i(.)$ is a preference function defined as follows:

$$f_i(C_k) = Utility_i(C_k) = \prod_{j \in C_k} T_i^j \tag{9}$$

$\prod_{j \in C_k} T_i^j$ is denoted as the coalition trust criterion. T_i^j is denoted as IDS i beliefs in IDS $j \in \mathscr{N}$. IDS i's beliefs in C_k's members is obtained using Bayesian inference as in (1). We use the product of IDSs trust values instead of their summation in the definition of the coalition trust criterion in order to conserve the effect of small trust values on the global coalitions trust value. That way, the impact of a small trust value will not be mitigated by a higher one.

2) The Proposed Coalition Formation Algorithm: The algorithm (Algorithm 1) that we propose is based on the hedonic shift rule [27]: let $\Pi = \{C_1, ..., C_l\}$ represent the set of coalition partitions. That is, for k = {1, 2, . . . , l}, each $C_k \subseteq \mathscr{N}$ is a disjoint coalition. Each IDS $i \in \mathscr{N}$ decides to leave its current coalition $C_\Pi(i)$ to join another one $C_k \in \Pi \cup \phi$ if and only if its coalition trust criterion (i.e., $U_i(C_k) = \prod_{j \in C_k} T_i^j$) in the new coalition exceeds the one it obtains in its current coalition. Leaving and joining decisions are considered selfish decisions. This means that they are made without considering their effect on the other IDSs.

Algorithm 1: Trust-based Coalition Formation Algorithm

```
Given the current coalition partition
  $\Pi_c = \{C_1, ..., C_l\}$, each IDS $i$ evaluates possible
  shift from its current coalition as follows:
repeat
    foreach $C_k \in \Pi_c \cup \phi$ do
        foreach IDS $j \in C_k$ do
            • calculate the trust value
              of IDS $j$.
    calculate $U_i(C_k \cup \{i\})$ and $U_i(C_{\Pi_c}(i))$
    if $U_i(C_k \cup \{i\}) > U_i(C_{\Pi_c}(i))$ then
        • IDS $i$ leaves its current
          coalition $C_{\Pi_c}(i)$ and
          joins the new coalition.
        • $\Pi_c$ is updated:
          $\Pi_{c+1} := (\Pi_c \setminus \{C_{\Pi_c}(i), C_k\})$
          $\cup \{C_{\Pi_c}(i) \setminus \{i\}, C_k \cup \{i\}\}$.
        else
            • IDS $i$ remains in the
              same coalition so that:
              $\Pi_{c+1} := \Pi_c$
until $\varepsilon$ elapses;
```

In Algorithm 1, an IDS i evaluates all of the possible coalitions it can join or form, beginning by leaving its current coalition C_Π(i) to join another already existing coalition C_k. The algorithm computes the trust value for each IDS $j \in C_k$ as in (1). Then, the algorithm determines the coalition trust criterion $U_i(C_\Pi(i))$ of its current coalition C_Π(i) as in (9) and compares it with the coalition trust criterion $U_i(C_k)$ of the coalition C_k. If the coalition trust criterion of the current coalition is greater than that of the coalition C_k, then the IDS i leaves its current coalition to join C_k. Otherwise, IDS i remains in its current coalition. One should note that, after a certain fixed period of time ε, the whole process is repeated, in order to obtain the changes that may happen in the current coalition partition Π_c. These changes include changes in the IDSs trust values, the departure of existing IDSs and the arrival of new IDSs.

The main complexity of Algorithm 1 lies in the shifting operations, i.e. the process of finding a new coalition to join, which equals $O(|\Pi_c|)$, where $|\Pi_c|$ is the number of coalitions in the current coalition partition.

The algorithm can be implemented in a distributed manner, given that each IDS can act autonomously and independently from any other IDSs in the system. However, it is important to provide appropriate actions based on [33] for:

- State recovery: the algorithm assumes that each IDS is able to retrieve the current coalition partition Π_c. Any state retrieval algorithm available in the state-of-the-art (e.g. [34], [35]) can be used for this purpose;
- Atomic state update: to guarantee correctness, Π_c must not change while IDS i moves from its current coalition C_Π(i) and joins another one. Distributed mutual exclusion algorithms (e.g. [36]) can be used for this purpose.

C. Trust Aggregation

In the previous section, we presented a trust-based coalition formation model that enables a set of cloud-based IDSs to cooperatively set up their coalitions. The output of the coalition formation algorithm (Algorithm 1) is a set of coalitions, where each coalition consists of a set of IDSs that prefer to work with each other. In this section, we show how an IDS inside a coalition can aggregate feedbacks received from other IDSs in the same coalition. For this purpose, we use the Dempster-Shafer Theory (DST) for feedback aggregation. DST was selected for the following two reasons: (1) unlike other aggregation models (e.g. Bayesian aggregation model) that demand complete information of prior probabilities, DST can handle a lack of complete information (i.e. uncertainty), and (2) it has the property of preventing collusion attacks, which occur when several malicious IDSs collaborate to give misleading judgments.

In our model, the frame of discernment, which describes the status of a suspicious intrusion (hypothesis) is $\Omega = \{1, 0, U\}$. In this set, 1 means that IDS j decides and reports to IDS i that there is an intrusion, 0 means that IDS j decides and reports to IDS i that there is no intrusion, and U shows that IDS j is uncertain whether there is an intrusion or not. Each hypothesis is assigned a basic probability value (bpv) between 0 and 1, which is equal to the credibility score believed by the IDS giving the judgement.

DST combines multiple IDSs beliefs under the condition that evidences from different IDSs are independent. For example, if IDS_i wants to combine the belief of two IDSs IDS_1 and IDS_2 over the same frame of discernment Ω, the combined belief of IDS_1 and IDS_2 is calculated as follows [37]:

$$\begin{aligned} m_{IDS_1}(1) \oplus m_{IDS_2}(1) = \frac{1}{K}[m_{IDS_1}(1)m_{IDS_2}(1) + \\ m_{IDS_1}(1)m_{IDS_2}(U) + m_{IDS_1}(U)m_{IDS_2}(1)] \end{aligned} \tag{10}$$

$$\begin{aligned} & m_{IDS_1}(0) \oplus m_{IDS_2}(0) = \\ & \frac{1}{K}[m_{IDS_1}(0)m_{IDS_2}(0) \\ & + m_{IDS_1}(0)m_{IDS_2}(U) + m_{IDS_1}(U)m_{IDS_2}(0)] \end{aligned} \tag{11}$$

$$m_{IDS_1}(U) \oplus m_{IDS_2}(U) = \frac{1}{K}[m_{IDS_1}(U)m_{IDS_2}(U)] \tag{12}$$

where,

$$\begin{aligned} K = & m_{IDS_1}(1) + m_{IDS_2}(1) + m_{IDS_1}(1) + m_{IDS_2}(U) \\ & + m_{IDS_1}(U) + m_{IDS_2}(U) + m_{IDS_1}(U) + m_{IDS_2}(1) \\ & + m_{IDS_1}(U) + m_{IDS_2}(0) + m_{IDS_1}(0) + m_{IDS_2}(0) \\ & + m_{IDS_1}(0) + m_{IDS_2}(U) \end{aligned} \tag{13}$$

Here is an example. Assume the following:
$m_{IDS_1}(1)$ = 0.75 $m_{IDS_1}(0)$ = 0 $m_{IDS_1}(U)$ = 0.25
$m_{IDS_2}(1)$ = 0.6 $m_{IDS_2}(0)$ = 0 $m_{IDS_2}(U)$ = 0.4
by combining the above two belief functions, we can obtain the result as follows:
$belief(1) = (0.75 * 0.6) + (0.75 * 0.4) + (0.6 * 0.25) = 0.9$
$belief(0) = (0 * 0) + (0 * 0.4) + (0 * 0.25) = 0$
$belief(U) = (0.25 * 0.4) = 0.1$
Since $belief(1) > belief(0) > belief(U)$, IDS i will decide that an attack exists.

IV. Experimental Evaluation

In this section, we first explain the experimental setup used to perform our experimentation and then study the performance of the proposed cooperative intrusion detection approach.

A. Experimental Setup

We implemented our framework in a 64-bit Windows 8 environment on a host equipped with an Intel Core i7-4790 CPU 3.60 GHz Processor and 16 GB RAM. We used Matlab for implementing our model.

The simulation environment uses 100 cloud-based IDSs. Each IDS is represented by two parameters, trust value t and decision threshold τ. The trust value represents the expertise level of the IDS, which in turn represents the ability of the IDS to catch suspicious traces from a given observation. The threshold τ represents the sensitivity (i.e., accuracy) of the IDS. Lower values of τ indicate a more sensitive IDS.

We use a Beta density function to reflect the intrusion detection capability of each IDS. A Beta density function is given by:

$$\begin{aligned} f(z|\alpha,\beta) &= \frac{1}{B(\alpha,\beta) z^{\alpha-1}(1-z)^{\beta-1}} \\ B(\alpha,\beta) &= \int_0^1 x^{\alpha-1}(1-x)^{\beta-1}dx \end{aligned} \tag{14}$$

$$\begin{aligned} \alpha &= 1+\frac{t(1-d)}{d(1-t)}r \\ \beta &= 1+\frac{t(1-d)}{d(1-t)}(1-r) \end{aligned} \tag{15}$$

where $z \in [0, 1]$ is the assessment result from the IDS about the likelihood of intrusion, and f $(z|\alpha,\beta)$ is the distribution of assessment z from an IDS with trust level t to an intrusion with difficulty level $d \in [0, 1]$. The trust level in the distribution can represent the expertise level of the IDS. Higher values of d represent these attacks that are difficult to detect. Higher values of t indicate a higher probability of generating correct intrusion assessments. $r \in \{0, 1\}$ is the expected result of detection. r = 1 means that there is an intrusion and r = 0 means otherwise.

In order to evaluate the ability of the proposed model in the presence of an untrusted environment, We made the percentage of untrusted IDSs 70% (trust level $t \leq 0.2$). We argue, based on the recent literature [38], that the percentage of untrusted nodes tends to form the majority compared to that of trusted nodes. We applied the proposed coalition formation algorithm (Algorithm 1) on the considered IDSs. We compared the proposed aggregation approach with other known aggregation approaches in the state-of-the-art: Majority aggregation model [13] and the weighted average aggregation model [39]. In the majority model, the IDS collects feedback from IDSs about suspicious behaviour and the decision is made (i.e., attack or not) according to the majority. However, in the weighted average aggregation model, weights W are assigned to feedbacks from different IDSs to distinguish their detection capability. Highly trusted IDSs are assigned with larger weights compared to low trusted IDSs. The decision is made according to the following equation. If $(\Sigma_{k=1}^{N}\ W_k y_k)$ / $(\Sigma_{k=1}^{N}\ W_k) \geq \tau$, the decision is *the existence of an attack*. Otherwise, the decision is that *there is no attack*, where W_k is the weight of the k-th IDS and y_k is the feedback from the k-th IDS.

B. Experimental Results

In Fig. 2, we observe that the proposed aggregation model (i.e., Dempster-Shafer aggregation approach) shows significant improvement for the false negative rate, compared to the weighted and majority aggregation model at different threshold values τ. Similarly, in Fig. 3, our model yields significant improvement for the false positive rate, compared to the other two models. This is due to the fact that Dempster-Shafer ignores the untrustworthy feedbacks upon making the final decisions. Moreover, Dempster-Shafer gives a weight for each feedback according to the trustworthiness level of the IDS giving this feedback.

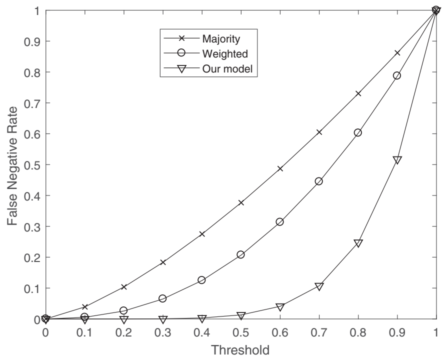

Fig. 2: Comparison of three aggregation models (False Negative Rate).

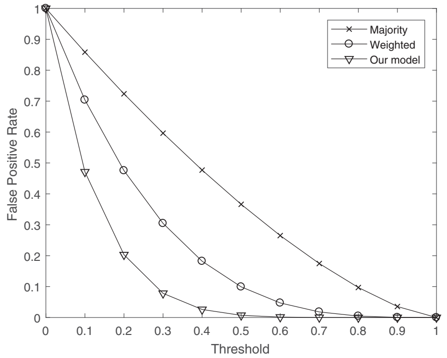

Fig. 3: Comparison of three aggregation models (False Positive Rate).

In Fig. 4 and Fig. 5, we also study the effect of the trust value (i.e., expertise level) on the accuracy of the detection. To this end, we run our Algorithm (Algorithm 1) many times. Each time, we let IDSs have different values of t. The study is conducted at different threshold values τ. Fig. 4 shows that the false negative decreases when the trustworthiness level of an IDS increases. Similarly, Fig. 5 shows that the false positive decreases when the trustworthiness level of an IDS increases. This is justified by the fact that whenever an IDS becomes more trusted, it will be able to give a right feedback about suspicious attacks.

Fig. 6 gives a comparison between the proposed trust-based coalitional game approach and the trust-based grand coalition approach. The latter considers all

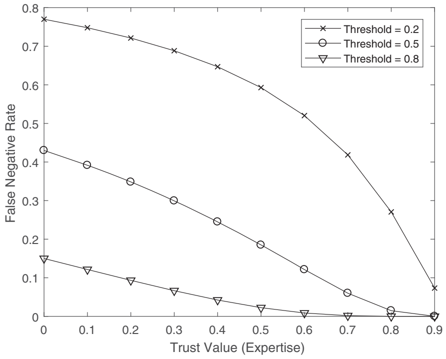

Fig. 4: False Negative vs. Trust Value t .

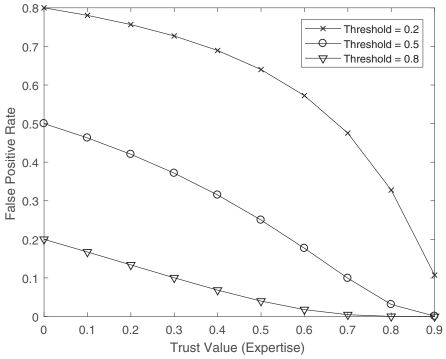

Fig. 5: False Positive vs. Trust Value t.

existing IDSs during the cooperation. In other words, the coalition is done among all IDSs. Thus, the feedback is received from all IDSs and the final decisions are made using the same proposed aggregation model (i.e., Dempster-Shafer). This is unlike our approach where we first run a coalition formation Algorithm (Algorithm 1) and minimise the number of IDSs inside the coalition. The figure shows the superiority of the proposed model for both the false positive and false negative rates. This is due to the fact that the proposed coalition approach minimises the number of untrusted IDSs inside each generated coalition. Thus, the received feedback is more likely to reflect the real status of any suspicious behaviour, whether it is a real attack or not. However, for the grand coalition approach, the feedback is received from every existing IDS. Therefore, there will be a chance of receiving incorrect feedback from untrusted IDSs. Fig. 6 also studies the cost associated with using each approach. The cost represents the time needed to make a judgment about a suspicious attack. The result is projected in a range between 0 and 1. Our model yields a minimum overhead compared to the grand coalition approach. The reason is that our model minimises unnecessary consultation requests by consulting only those trusted IDSs in the final coalition. This is unlike the grand coalition approach where a consultation request is sent to all existing IDSs.

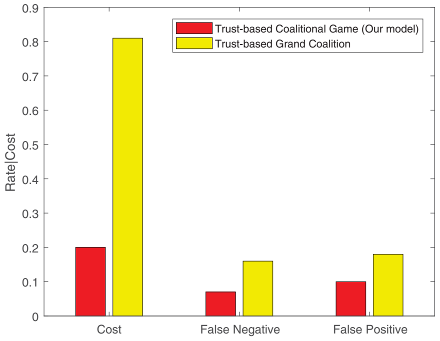

Fig. 6: Comparison of two coalition formation models.

V. Conclusion

This paper investigates a novel trust-based cooperative IDS in a multi-cloud environment. We propose a coalitional game-theoretic framework. The framework enables an IDS to evaluate the trust value of other IDSs using bayesian inference. We devise a coalition formation algorithm, that is based on the coalitional game theory. The algorithm enables IDSs to leave or join a given coalition in such a way that enhances their ability to work with trusted IDSs. The proposed algorithm converges to a Nash-stable situation; that is, no IDS has an incentive to leave its current coalition to move to another coalition. Furthermore, we propose a feedback aggregation algorithm, that is based on Dempster-Shafer Theory (DST), to enable an IDS inside a coalition to aggregate feedbacks about suspicious attacks in order to make the optimal decision in terms of detection accuracy. Numerical results show the effectiveness of the proposed approach in terms of false positive and false negative rates, and cost.

Acknowledgment

The financial support of the Natural Sciences and Engineering Research Council of Canada is gratefully acknowledged.

References

[1] C. J. Fung and Q. Zhu, "Facid: A trust-based collaborative decision framework for intrusion detection networks," *Ad Hoc Networks*, vol. 53, pp. 17–31, 2016.

[2] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

[3] C. J. Fung, D. Y. Lam, and R. Boutaba, "Revmatch: An efficient and robust decision model for collaborative malware detection," in *Network Operations and Management Symposium (NOMS), 2014 IEEE*. IEEE, 2014, pp. 1–9.

[4] N. D. Man and E.-N. Huh, “A collaborative intrusion detection system framework for cloud computing,” in *Proceedings of the International Conference on IT Convergence and Security 2011*. Springer, 2012, pp. 91–109.

[5] D. Singh, D. Patel, B. Borisaniya, and C. Modi, “Collaborative ids framework for cloud,” *International Journal of Network Security*, vol. 18, no. 4, pp. 699–709, 2016.

[6] S. Ghribi, “Distributed and cooperative intrusion detection in cloud networks,” in *Proceedings of the Doctoral Symposium of the 17th International Middleware Conference*. ACM, 2016, p. 7.

[7] Z. Chiba, N. Abghour, K. Moussaid, M. Rida *et al.*, “A co-operative and hybrid network intrusion detection framework in cloud computing based on snort and optimized back propagation neural network,” *Procedia Computer Science*, vol. 83, pp. 1200–1206, 2016.

[8] Z. Al-Mousa and Q. Nasir, “cl-cidps: A cloud computing based cooperative intrusion detection and prevention system framework,” in *International Conference on Future Network Systems and Security*. Springer, 2015, pp. 181–194.

[9] H. A. Kholidy and F. Baiardi, “Cids: A framework for intrusion detection in cloud systems,” in *Information Technology: New Generations (ITNG), 2012 Ninth International Conference on*. IEEE, 2012, pp. 379–385.

[10] D. Ray, *A game-theoretic perspective on coalition formation*. Oxford University Press, 2007.

[11] G. Shafer, “Dempster-shafer theory,” *Encyclopedia of artificial intelligence*, pp. 330–331, 1992.

[12] Á. Dermott, Q. Shi, and K. Kifayat, “Collaborative intrusion detection in federated cloud environments,” *Journal of Computer Sciences and Applications*, vol. 3, no. 3A, pp. 10–20, 2015.

[13] C.-C. Lo, C.-C. Huang, and J. Ku, “A cooperative intrusion detection system framework for cloud computing networks,” in *Parallel processing workshops (ICPPW), 2010 39th international conference on*. IEEE, 2010, pp. 280–284.

[14] S. Teng, C. Zheng, H. Zhu, D. Liu, and W. Zhang, “A cooperative intrusion detection model for cloud computing networks,” *International Journal of Security and its applications*, vol. 8, no. 3, pp. 107–118, 2014.

[15] M. E. Locasto, J. J. Parekh, A. D. Keromytis, and S. J. Stolfo, “Towards collaborative security and p2p intrusion detection,” in *Information Assurance Workshop, 2005. IAW’05. Proceedings from the Sixth Annual IEEE SMC*. IEEE, 2005, pp. 333–339.

[16] C. G. Cordero, E. Vasilomanolakis, M. Mühlhäuser, and M. Fischer, “Community-based collaborative intrusion detection.” in *SecureComm*, 2015, pp. 665–681.

[17] V. Yegneswaran, P. Barford, and S. Jha, “Global intrusion detection in the domino overlay system.” in *NDSS*, 2004.

[18] M. Cai, K. Hwang, Y.-K. Kwok, S. Song, and Y. Chen, “Collaborative internet worm containment,” *IEEE Security & Privacy*, vol. 3, no. 3, pp. 25–33, 2005.

[19] X. Liu, P. Zhu, Y. Zhang, and K. Chen, “A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure,” *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2435–2443, 2015.

[20] A. Patel, H. Alhussian, J. M. Pedersen, B. Bounabat, J. C. Júnior, and S. Katsikas, “A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems,” *Computers & Security*, vol. 64, pp. 92–109, 2017.

[21] N.-F. Huang, C. Wang, I.-J. Liao, C.-W. Lin, and C.-N. Kao, “An openflow-based collaborative intrusion prevention system for cloud networking,” in *Communication Software and Networks (ICCSN), 2015 IEEE International Conference on*. IEEE, 2015, pp. 85–92.

[22] H. Sedjelmaci and S. M. Senouci, “An accurate and efficient collaborative intrusion detection framework to secure vehicular networks,” *Computers & Electrical Engineering*, vol. 43, pp. 33–47, 2015.

[23] Q. Zhu, C. Fung, R. Boutaba, and T. Basar, “A game-theoretical approach to incentive design in collaborative intrusion detection networks,” in *Game Theory for Networks, 2009. GameNets’ 09. International Conference on*. IEEE, 2009, pp. 384–392.

[24] ——, “Guidex: A game-theoretic incentive-based mechanism for intrusion detection networks,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 11, pp. 2220–2230, 2012.

[25] A. Josang and R. Ismail, “The beta reputation system,” in *Proceedings of the 15th bled electronic commerce conference*, vol. 5, 2002, pp. 2502–2511.

[26] H. Yahyaoui, “A trust-based game theoretical model for web services collaboration,” *Knowledge-Based Systems*, vol. 27, pp. 162–169, 2012.

[27] A. Bogomolnaia and M. O. Jackson, “The stability of hedonic coalition structures,” *Games and Economic Behavior*, vol. 38, no. 2, pp. 201–230, 2002.

[28] J. H. Dreze and J. Greenberg, “Hedonic coalitions: Optimality and stability,” *Econometrica: Journal of the Econometric Society*, pp. 987–1003, 1980.

[29] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, “Towards trustworthy multi-cloud services communities: A trust-based hedonic coalitional game,” *IEEE Transactions on Services Computing*, 2016.

[30] ——, “Optimal load distribution for the detection of vm-based ddos attacks in the cloud,” *IEEE Transactions on Services Computing*, 2017.

[31] K. R. Apt and A. Witzel, “A generic approach to coalition formation,” *International Game Theory Review*, vol. 11, no. 03, pp. 347–367, 2009.

[32] T. Sandholm, K. Larson, M. Andersson, O. Shehory, and F. Tohmé, “Coalition structure generation with worst case guarantees,” *Artificial Intelligence*, vol. 111, no. 1-2, pp. 209–238, 1999.

[33] M. Guazzone, C. Anglano, and M. Sereno, “A game-theoretic approach to coalition formation in green cloud federations,” in *Cluster, Cloud and Grid Computing (CCGrid), 2014 14th IEEE/ACM International Symposium on*. IEEE, 2014, pp. 618–625.

[34] P. K. Sinha, *Distributed operating systems: concepts and design*. PHI Learning Pvt. Ltd., 1998.

[35] M. Wooldridge, *An introduction to multiagent systems*. John Wiley & Sons, 2009.

[36] A. D. Kshemkalyani and M. Singhal, *Distributed computing: principles, algorithms, and systems*. Cambridge University Press, 2011.

[37] B. Yu and M. P. Singh, “An evidential model of distributed reputation management,” in *Proceedings of the first international joint conference on Autonomous Agents and Multiagent Systems: Part 1*. ACM, 2002, pp. 294–301.

[38] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, “A survey on trust and reputation models for web services: Single, composite, and communities,” *Decision Support Systems*, vol. 74, pp. 121–134, 2015.

[39] C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, “Robust and scalable trust management for collaborative intrusion detection,” in *Integrated Network Management, 2009. IM’09. IFIP/IEEE International Symposium on*. IEEE, 2009, pp. 33–40.