Extended Game Theoretic Dirichlet Based Collaborative Intrusion Detection Systems

Sayan Paul, Tushar Makkar and K. Chandrasekaran

Abstract Security has always been one of the key issues of any man-made system, this paved the way for a submodule or application or a device to monitor or system for malicious activities. This system or submodule or device is known as Intrusion Detection System (IDS). As technology evolves so does the associated threats and thus the intrusion detection system needs to evolve. Game theory throws in a different perspective which have not been looked upon much. Game theory provides a way of mathematically formalizing the decision making process of policy establishment and execution. Notion of game theory can be used in intrusion detection system in assisting in defining and reconfiguring security policies given the severity of attacks dynamically. We are trying to formulate a robust model for the theoretical limits of a game theoretic approach to IDS. The most important flaw of game theory is that it assumes the adversary's rationality and doesn't take into consideration multiple simultaneous attacks. Therefore, a collaborative trust and Dirichlet distribution based robust game theoretic approach is proposed which will try to resolve this issue. Reinforced learning approaches using Markov Decision Process will be utilized to make it robust to multiple simultaneous attacks.

Keywords Intrusion detection system · Dirichlet based trust management · Collaborative trust management · Game theory · Nash equilibrium

S. Paul (✉) · T. Makkar · K. Chandrasekaran
Department of Computer Science and Engineering, National Institute of Technology
Karnataka, Surathkal, India
e-mail: sayan.paul6@gmail.com

T. Makkar
e-mail: tusharmakkar08@gmail.com

K. Chandrasekaran
e-mail: kchnitk@ieee.org

M. Senthilkumar et al. (eds.), *Computational Intelligence, Cyber Security and Computational Models*, Advances in Intelligent Systems and Computing 412, DOI 10.1007/978-981-10-0251-9_32

1 Introduction

Intrusion Detection Systems plays a key role in security of modern day software applications/systems. They compare observable behaviour in the system against suspicious patterns to identify any kind of intrusions. There are two variances of IDS: Network based (NIDS) or Host based (HIDS). Traditional IDSs have a problem that they work in isolation and therefore have higher chance of getting compromised by unknown or new threats. A Collaborative IDS solves this problem by having peer IDS help each other out and get aided by shared collective knowledge and experience from peers. This increases both the accuracy and the ability to detect new intrusion threats. Collaborative IDS assumes that all IDSs will honestly cooperate. The lack of trust management leaves the system vulnerable to malicious peers [1].

Few IDSs have been produced to cooperate honestly based on trust and/or distributed trust models but they have not incorporated any kind of incentives for IDS collaboration. Incentives are important criteria any collaborative system otherwise it will suffer from "free rider problem" in which certain group of IDSs only keep on asking for assistance but may not actually contribute to the system. Thus, this leads to degradation of performance of the system. So we need to take care of incentives while designing such a system [2]. The distributed collaborative is preferred over centralized as it need rely on a central server to gather and analyze alerts and thus avoiding any bottleneck problems [3]. We just need to take care of any malicious or malfunctioning IDS which can degrade the performance of the system (Fig. 1).

In this paper, we propose a trust-based IDS collaboration network system with incentive based scheme for resource allocation. In this the amount of resources

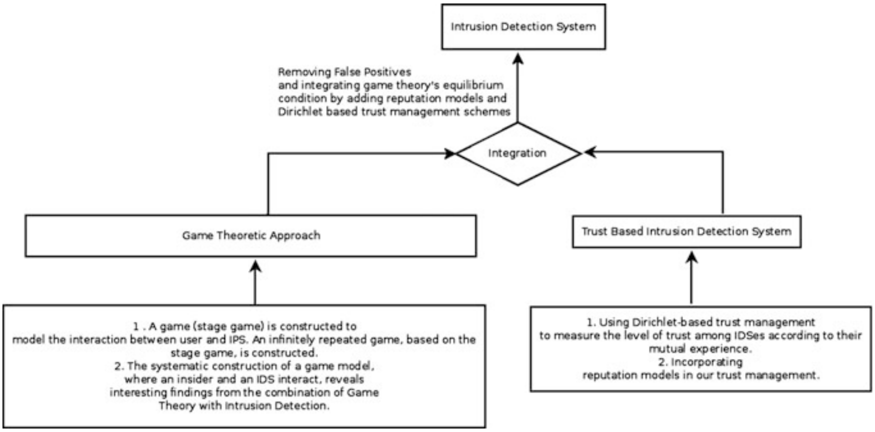
Intrusion Detection System
Removing False Positives
and integrating game theory's equilibrium
condition by adding reputation models and
Dirichlet based trust management schemes
Integration
Game Theoretic Approach
Trust Based Intrusion Detection System
1 . A game (stage game) is constructed to
model the interaction between user and IPS. An infinitely repeated game, based on the
stage game, is constructed.
2. The systematic construction of a game model,
where an insider and an IDS interact, reveals
interesting findings from the combination of Game
Theory with Intrusion Detection.
1. Using Dirichlet-based trust management
to measure the level of trust among IDSes according to their
mutual experience.
2. Incorporating
reputation models in our trust management.

Fig. 1 Overview of system

allocated by each IDSs to their neighbors is dependent on the trustworthiness and resources already allocated by its neighbors to help it.

An optimization problem is constructed to aid the IDS to optimally allocate resource to maximize the satisfaction level of each of its peers. We show that under certain controllable system conditions, there exists a unique Nash Equilibrium. We use a Bayesian trust management model based on Dirichlet family of probability density functions to predict the likely future behaviour of an IDS based on its past records.

The uncertainty associated with IDS gets pacified due to this model. Acquaintance is managed between the IDSs using the estimated trust values to enhance the accuracy of the system. Dirichlet function with game theoretic approaches makes the system even more robust and efficient. We now try to introduce the concept of reinforcement learning to make the system more secure and robust. Reinforcement learning takes environment into account to maximise the overall satisfaction levels. Markov decision process (MDP) are generally used to formulate the environment. Since Nash Equilibrium technique is limited for a single attack scenario we will be considering each attack as a separate state and model it as a MDP for effective detection of Intrusion in our network.

Section 2 tells us about the related work which have been done in this field. Section 3 discusses about the motivation to carry out this project. Section 4 describes the Architectural Overlay of the system. Section 5 discusses our proposed work in detail. Section 6 gives us an analysis of why the proposed work is better than any other current methods. Section 7 gives us the conclusion and the plans for future work.

2 Related Work

In one of the work presented by Zhu and Tamer [4], they propose a trust management system which involves IDSs to build trust rapport by exchanging test messages. In this each IDS sends a trace of possible attacks from its own database (one with risk level of each attack), to its acquaintances to test their trustworthiness. Each of these peers then sends back the risk values of each of those attack in trace. The sender then cross-checks these values with its own knowledge database and generates a satisfaction level for each feedback using “a satisfaction mapping function”. In [5], we see the use of a simple weighted average model to estimate the trust value while in [6] Bayesian statistics model is used to calculate the trust value.

In Bartos et al. [7], a distributed model is presented which helps to collaborate multiple ids sensors which are heterogeneous in nature. This model assumes to be able to monitor ids in different locations using multiple detection sensors. It uses game theoretic approaches in dynamic environments to optimize behavior among the sensors. They propose a hand between defenders and attackers as a model along with a trust based model e-fire to collaborate in such a highly dynamic environment while trying to prevent any kind of poisoning or manipulation by malicious attackers.

In Fung et al. [3], they propose a Trust management using Dirichlet distribution, to calculate trust based on mutual experience between ids. An acquaintance algorithm is proposes to manage its peers based on the trust value. Intrusion detection system is like a two player game between the attacker and the intrusion detection system as two opposing players. In Alpcan and Basar [8], a two person, finite game has been portrayed between each sensor of the ids based on cooperative game theory. In papers [9–11], we see the use of non-cooperative game frameworks in intrusion detection system. In Liu and Comaniciu [12], we can see the use of Bayesian game techniques in intrusion detection for ad hoc networks, using a two-person non-zero-sum incomplete information game as a framework for the system.

In Zhu et al. [2], they show that there exists a Nash equilibrium state and its unique, amongst the peers so they can communicate in cooperative manner. They were able to develop an algorithm which is iterative and converges geometrically to the equilibrium. In Allazawe et al. [13], we get an overview of traditional IDS and its challenges and how game theoretic approaches help and its limitations.

In Lye and Wing [14], they show the use of game theory in the field of security of computer networks. They construct a two-player stochastic game model to visualize the interactions between attacker and administrator. They use non-linear program to evaluate the Nash equilibrium state or the best possible strategies for both players taken into account. These strategies can then be used by administrators to improve the security of the system.

In Alpcan and Tamer [15], A game theoretic based model is made for the sensors observing and reporting attacks to the IDS as a finite Markov chain. Therefore a two player stochastic Markov game is observed depending on the information on the players. It captures various intricacies of the system. Both MDP and Q-learning methods are used to build the foundation for development of various strategies for the players. As we can see trust management and game theoretic approaches have not been used in together as a collaborative system to enhance the robustness of intrusion detection system as a whole.

3 Motivation

The most important flaw of Intrusion Detection Systems based out of game theory is that it assumes the adversary's rationality. It assumes that it would take steps to obtain a maximum gain (or near maximum) for itself or its interests. However, in reality, this may not always be the case as human behavior is still unpredictable. So it is hard to discern whether the users attack is rational or whether he/she is simply trying to confuse the IDS by employing another attack vector. Another area of weakness of the game theoretic approach to intrusion detection is the unsolved approach on how to detect and handle simultaneous attacks [14].

Most of the systems available are either optimized for Collaborative Intrusion Detection Networks [CIDN] (group of Intrusion Detection System (IDS)) or for a single IDS. There is no generalized system available for both CIDN and IDS.

4 Architecture

Our architecture can be quite similar to Fig. 2 and also to Fig. 3. The consolidated architecture can be described as network of different IDS. The system will have a group of IDS's who are connected to each other via Internet. Each IDS will in turn consist of group of computers which are mostly connected via LAN. So in short, there will be communication between clients in a network forming a IDS as well as multiple IDS communicating together.

There will be 2 types of messages which are being transferred through our system:

1. Local Messages
2. Global Messages

Local Messages are the messages which will be transferred in between a given IDS (LAN connected) and Global messages will be transferred in between different IDS. The messages which are transferred is explained in depth in the next section. Our system can be a mixed of Anomaly detection system and Misuse detection system.

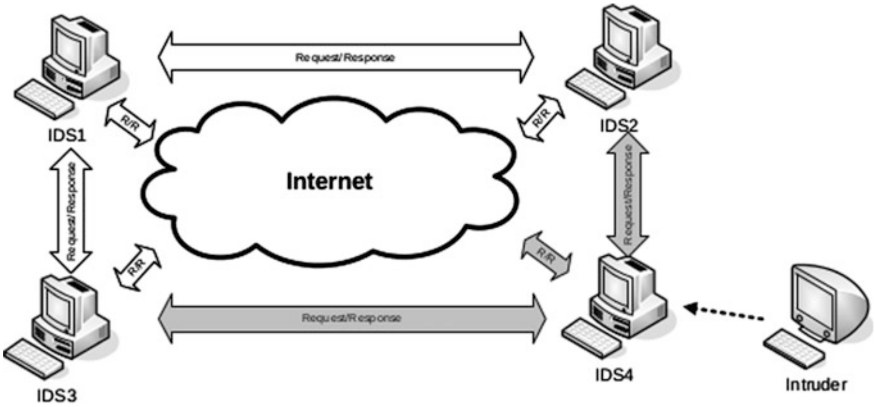

Fig. 2 Individual IDS

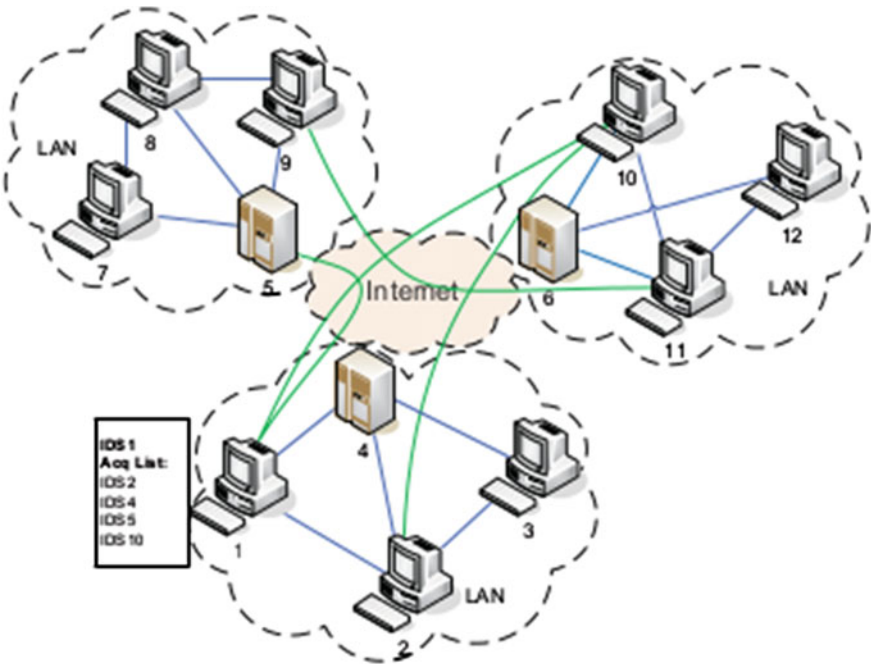

Fig. 3 Architecture overlay

5 Proposed Work

5.1 Dirichlet Based Collaborative Intrusion Detection System

We are connecting Intrusion Detection Systems to form a collaborative network. Here each IDS can choose its collaborative peers. The supporting peers will have varied expertise levels of detecting the intrusions. Our system has following features:

- An algorithm for intrusion detection systems which is effective, fair and incentivisable which helps in managing their acquaintances from which they can ask opinions about intrusions;
- A trust management model to reduce the negative impact of low expertise IDSes, dishonest IDSes and discover compromised ones
- Detection of Malicious insider activity
- System should be scalable and highly elastic in terms of trust evaluation, network size, and assessing the intrusion.

Links between IDSes indicate their collaborative relationships. Each node maintains a list of acquaintances whom it trusts the most and collaborates with. Nodes communicate by means of intrusion evaluation requests and corresponding feedback. There are two types of requests:

Intrusion Consultation and Evaluation Requests Whenever a suspicious behavior is detected by IDS and the expertise level still remains insufficient to make a decision, it sends other requests to the other friend IDSes for consultation. Feedback from the friend IDS's is cumulated and aggregated. A final conclusion is developed using those feedbacks. The information provided to friend IDS depends on the trust level of each friend.

Fake Test Messages Nodes in the Collaborative Intrusion Detection Network use these fake test messages for finding out the trust of IDS. These messages are "fake" consultation requests, which are formulated in a manner that makes them difficult to be distinguished from real consultation message requests [3].

The content of these messages depends on various factors. Some of them can be:

(1) Type of Attack
(2) Number of Peers
(3) Topology of Network etc.

A behavioral graph is made for describing the activities. The testing node has prior information about the true result of the fake testing message. It then uses the received feedback to derive at a trust value for the other nodes in the network. This can be done using standard machine learning and regression techniques. This will help us in identifying malicious nodes. IDSes use different metrics to rank and rate alerts. Let's assume there exists a function H, which maps Intrusion Detection System's alert ranking to a [0, 1] interval where 0 denotes minimal level of traffic and 1 highly dangerous intrusions. H follows more severe than partial order relationship which means if an alert a_j is more severe than alert a_i then H preserves that relationship by having $H(a_j) > H(a_i)$. The satisfaction of feedback is find out using these factors:

1. The received answer ($a \in [0, 1]$),
2. The difficulty level of the test message ($d \in [0, 1]$) and
3. The expected answer ($r \in [0, 1]$).

More the value of d, more difficult it would be to answer the request correctly. The difficulty of a test message can be determined by the age of signatures. The difficulty level is low for the messages generated from old signature; medium difficult for messages generated using new signature and high difficult for malicious traffic taken from previous attacks.

We can measure the quality of feedback using a function $Sat(r, a, d)$ ($\in [0, 1]$) for representing the level of satisfaction in the received answer which depends on the distance from the expected answer and difficulty of the message. It can be written as follows:

$$Sat(r,a,d) = \begin{cases} 1 - (\frac{a-r}{\max(c_1 r, 1-r)})^{d/c_2} & a > r \\ 1 - (\frac{c_1(r-a)}{\max(c_1 r, 1-r)})^{d/c_2} & a \leq r \end{cases} \tag{1}$$

where c_1 is used penalizing the wrong estimates. c_1 value is always >1 to show that the estimates which are lower than exact answer are penalized strongly than those that are higher. $c_2 \in R^+$ controls the satisfaction sensitivity, where large values means more sensitive to the distance between the correct and received answers. This equation makes sure that levels with low difficulty are more severe in their penalty than incorrect answers [3].

Our interest lies in finding out the distribution of the satisfaction levels in the answers provided by each peer IDS. We use this information for estimating the satisfaction level. We use a beta distribution with binary satisfaction level (satisfied, —satisfied). Here we are using Dirichlet distribution [4] for solving our problem which involves multi-valued satisfaction levels. This kind of distribution is most suited for our trust management model since the trust is updated based on the history of interactions.

We consider X as a discrete random variable which signifies the satisfaction level peer's feedback. X is chosen such that $X = \{x_1, x_2, \ldots, x_k\}$ ($x_i \in [0, 1]$, $x_{i+1} > x_i$) are the different levels of satisfaction. The trustworthiness of a given IDS or peer would be an input to our Game theoretic model for IDS.

$$T^{uv} = E[Y^{uv}] = \sum_{i=1}^{k} w_i E[p_i^{uv}] = \frac{1}{\gamma_0^{uv}} \sum_{i=1}^{k} w_i \gamma_i^{uv} \tag{2}$$

where,

- p_i^{uv}, denotes the probability that peer v provides answers to the requests sent by peer u with satisfaction level x_i.
- γ_i^{uv} is the cumulated evidence that v has replied to u with satisfaction level x_i.
- w_i, an associated weight of each satisfaction level x_i
- Y^{uv} be the random variable denoting the weighted average of the probability of each satisfaction level in p^{uv}.

5.2 Game Theoretical Model for Intrusion Detection System

Prevention of intrusion is just set of interaction between the IDS which protects a target system (TS) and the user. This situation can be studied in detail using Game Theory. A game (stage game) is constructed to model the interaction between user and IDS. It can be considered as an infinitely repeated game. The solutions to the stage game and to the repeated game are then given and interpreted. Using this model we can predict user intentions and preconditions for an attack and thus we can prevent any insider intrusions and outsider attacks.

We model the interactions using a two player stochastic game between the user and the IDS. A N-node intrusion detection network is considered in our model. Let the n nodes be denoted by N = {1, 2 ,…, N}. N_u^d will represent the set of neighbors for peer u with maximum distance d ∈ $R^{+,}$ i.e., N_u^d = {i ∈ N: dist(i, u) <= d, i <= u}, where dist: N N –> R^+ is a distance function measuring the distance between two nodes. N1 u will be same as N-u because it will contain all nodes except u. There is symmetric information flow in the network. R_u^v represents the set of resources demanded by v from u for its full satisfaction. Whereas the minimum acceptable set from u to v is represented by mv u. Let p_v^u ∈ R^+ be the set which u actually allocates to v. This parameter is decided by u and is private to u and v. Therefore, to satisfy v this should lie over the interval [m_u^v, r_u^v].

We assume that we are aware of trust values between each peer and its neighbors, as its a distributed trust management system. Let T^{uv} ∈ [0, 1] represent this trust value from u to v. p_{uv} parameter is dependent on this trust value T^{uv} perceived by u. Each of the peer will try to maximize its effort in order to satisfy its neighbors but having a capacity constraint C_u, determined by its own resource capacity such as bandwidth, CPU, memory, etc. Following relation will hold true:

$$\sum_{v\in\mathcal{N}_u^d} p_{uv} \leqslant C_u, \quad \text{for all } u \in \mathcal{N}. \tag{3}$$

In this model, an utility function NS_{uv} is defined to model the satisfaction level from a peer to its neighbors. It is defined as follows:

$$S_{uv} = \frac{\ln(\alpha \frac{p_{uv}-m_{vu}}{r_{vu}m_{vu}} + 1)}{\ln(\alpha + 1)} \tag{4}$$

where, a ∈ (0, 1), a system parameter to control satisfaction curve, ln(a + 1), the normalization factor, ln chosen because of its property of proportional fairness. We will set the net satisfaction S as Trust (which we got from Dirichlet Solution) multiplied by Satisfaction level of neighbors.

$$S_{uv} = NS_{uv} \times T^{uv} \tag{5}$$

Let U^u: $R_+^{L(u,d)} \rightarrow R_+$ be the peer u's aggregated altruistic utility, where L(u, d) = card(N_u^d), the cardinality of the set N_u^d. Let the payoff function, U_u, for u be given by:

$$U_u = \sum_{v\in\mathcal{N}_u^d} w_{uv} S_{uv} w_{uv} = T_v^u p_{vu} \tag{6}$$

where, w_{uv}, weight given on v's satisfaction level S_{uv}. More the trust, more is the weight. In this model, every peer u ϵ N tries to maximize U_u within its resource capacity. To find optimum value, following function can be devised:

$$\begin{aligned} \max_{\{p_{uv}, v \in \mathcal{N}_u^d\}} \quad & \sum_{v \in \mathcal{N}_u^d} w_{uv} S_{uv} \\ \text{s.t.} \quad & \sum_{v \in \mathcal{N}_u^d} p_{uv} \leqslant C_u \\ & m_{vu} \leqslant p_{uv} \leqslant r_{uv} \forall v \in \mathcal{N}_u^d \end{aligned} \tag{7}$$

where, S_{uv} and w_{uv} have been previously defined in Eqs. 2 and 3 respectively. As we observed earlier every peer needs to find an optimal value and thus an optimization problem (OP) to solve. This problem is a concave one in which the function is a concave function in p_{uv} constrained by the cardinality of the set N_u^d. We assume the size of whole network is large and peers within a radius d can only communicate with each other and thus N independent optimization problems are there. Therefore game can be modeled by triplet (N, A_u, U_u), where Au is action set for peer u for u ∈ N, U_u is the payoff function defined in Eq. 3 and N is the size of network [2]. Action here means allocation of resources. Action set, $A_u = \{p_u \in R^{L(u,d)+} - \sum v \in N_u^d\ p_{uv} <= C_u\} \cap \{p_u \in R^{L(u,d)+} - m_u^v <= p_{uv} <= r_{vu}, v \in N_u^d\}$. Following condition shows that action set is non-empty.

$$C_u \geqslant \sum_{v \in \mathcal{N}_u^d} m_{vu} \tag{8}$$

Lagrange relaxation can be used to solve for Nash equilibrium. Lagrangian of peer u's optimization problem based on three lagrangian multipliers can be used to devise a relaxed game model [2]. Using this relaxed model we can try to solve for Nash Equilibrium. First order KKT condition can then be applied to this optimization problem.

Since our system is comprised by taking the positive effects of Game Theory and Trust Management models, it should theoretically perform better than the available Intrusion Detection Systems. We can also refer from the results of Zhu et al. [1] and Fung et al. [13] for more introspection on the implementation details.

5.3 Extended Game Theoretical Model for Intrusion Detection System

The model proposed using game theoretic and trust management models can further be decomposed into smaller manageable components so we can figure out strategies individually for each sub model using Markov decision process along with game theoretic methods. Subgames can be defined using nearly isolated clustered state and MDP can be defined for states which has meaningful actions for only one player. Using the strategies from each sub model or components we can find the overall best-response for each player. The computation time is said to be reduced significantly using a such a decomposition method [1]. Even different attacks can be detected using Markov decision process.

We propose to use reinforcement learning to enhance the game theoretic model for IDS. Markov decision process is being used to solve reinforcement learning. In MDP, if the current state is some state s, an action available to s is then chosen by a decision maker a. The process randomly moves to a new state s′ with corresponding state transition function P_a (s, s′) and reward R_a (s, s′). Therefore, s′, the next state depends on decision maker a and the current state s. The state transitions satisfies the Markov property [2], which states that "effects of an action taken in a state depend only on that state and not on the prior history".

The MDP for our system is defined using filtering variables:

- S = State corresponding to one attack vector
- A = Actions which are either reporting attack or remaining silent
- P = Probability of transition is specific to the current state that is the attack vector.
- R = Reward is directly proportional to the trustworthiness factor taken from Dirichlet distribution
- γ = this depends on the Nash equilibrium stabilization time.

One of the most critical part in any MDP is the decision maker's policy [16]. This policy is defined by a function ∏ that allots an action ∏(s) to a state s. Policy function ∏ should be chosen in such a way to maximize sum cumulative function of the rewards. We need to take care of following criteria:

- The trustworthiness of the IDS
- The Nash equilibrium state
- Different attack attributes
- Rewards for moving from one state to another

Using the knowledge of the reward function R and the state transition function P, we try to devise a policy to maximize the discounted rewards.

Calculation of optimal policy can be done using standard set of algorithms which requires two arrays indexed by state: V, set of real values; ∏, the set of actions. The algorithm results to give ∏ the solution and V(s), the discounted sum of the rewards that can be gained by following that solution from state s [17].

The algorithm is a two-step one, these two steps are repeated for all states until the result becomes constant and no further changes are observed. They are defined as follows:

$$\pi(s) := \arg\max_a \left\{ \sum_{s'} P_a(s,s')(R_a(s,s') + \gamma V(s')) \right\} \tag{9}$$

$$V(s) := \sum_{s'} P_\pi(s,s')(R_\pi(s,s') + \gamma V(s')) \tag{10}$$

These steps can be done state by state or even all states at once or maybe even specifically more to certain states. The algorithm will converge to a optimal solution unless certain set is excluded all together. To resolve this a further function is defined which corresponds taking the action a and then continuing optimally:

$$Q(s,a) = \sum_{s'} P_a(s,s')(R_a(s,s') + \gamma(s')) \tag{11}$$

This above function is an unknown one but it learns based on (s, a) pairs with their outcomes s′. Thus, there is an array Q and "earns" to update it. This is known as Q-learning. Markov decision processes can be solved even without explicit specification of the transition probabilities using reinforcement learning. In this a simulator aids in accessing transition probabilities, which is generally restarted many times from a uniformly random initial state. As previously mentioned we propose a model by breaking it down to smaller sub module and solve it using MDP to find strategies for the game between the attacker and the IDS. Reinforcement learning enhances the MDP and thus helps in solving for an optimal state (Nash equilibrium). Thus, here we are able to extend upon the game theoretic approaches previously along with a Dirichlet based management system to make the system even more robust.

6 Analysis

We proposed two new models for Intrusion Detection Network and analyzed the previous available models.

Dirichlet Based Collaborative Intrusion Detection System is based using Dirichlet distribution as a trust distributing mechanism. Two types of requests are sent: Intrusion Consultation and Evaluation Requests and Fake Test Message request. A satisfaction function is formed using received feedback, expected answer and difficulty level of request. This helps in formulating a trust value for each peer. This method is generally fast but the accuracy is less than other systems.

Game Theoretical Model for Intrusion Detection System is made using the concept of Nash Equilibrium. Lagrange Multipliers were used to find the Nash Equilibrium state. The optimal strategy involves considering both the gameplay of individual player. This model can only be used when a single attacker is attacking the system. It also considers that the attacker always play using extreme rules that is he can't change from an attacker to a normal peer.

Game Theoretic Dirichlet Based Collaborative Intrusion Detection System uses the concept of Dirichlet Distribution based trust model along with Nash Equilibrium. We use the trust value which we get from Dirichlet Based Message Request and use them for formulating the Nash Equilibrium's Lagrange multipliers. This method has better accuracy than both the above methods and it takes into consideration that the attacker can change roles in between.

Table 1 Comparisons of different methodologies

Type of IDS	Features
Dirichlet based collaborative intrusion detection system	IDS built using Dirichlet distribution for distributing trust. Faster than conventional systems. Can handle only one attack at a time. Accuracy is less
Game theoretical model for collaborative intrusion detection system	IDS built using game theory and Nash equilibrium. Also handles one attack at a time. Considers attackers to attack in extreme fashion
Game theoretic Dirichlet based collaborative Intrusion detection system	IDS uses Dirichlet distribution along with Nash equilibrium. Trust derived from Dirichlet distribution and fed to Nash equilibrium. removes the flaw of game theoretical IDS and has better accuracy than trust based
Extended game theoretic Dirichlet based collaborative intrusion detection system	Uses game theory, Dirichlet distribution and Markov decision process. Better than all other alternatives as It considers all attack scenarios with high accuracy and power to counter simultaneous attacks. Slower than other systems

Extended Game Theoretic Dirichlet Based Collaborative Intrusion Detection System is basically the advanced version of the approach explained previously. It uses Markov Decision Process for modelling the Intrusion Detection system. Submodels are generated and reinforcement learning techniques are applied. This is the best model among all the proposed models. It even takes into consideration multi-attacker scenario. Time complexity of the system is high but it reduces the false positives which is a significant advantage. Due to the aforementioned features we can use it in high secure environments.

The summary of the analysis is done in following Table 1.

7 Conclusion

In this paper, we present an extended game theoretic approach along with Dirichlet based trust management model for an intrusion detection system. IDS are an important part of any software system and so also a hard task to make it efficient and robust. We first start off with a trust management model for Collaborative Intrusion Detection System. This model is based on Dirichlet density functions and it takes care of evaluating uncertainty in estimating future behavior of peers in IDS or between IDSes in an IDN. Measurement of this uncertainty aids to deploy an adaptive message exchange rate which then helps in making the system scalable. Along with the “forgetting factor”, it is robust against some common attacks and threats. We then next moved on to game theoretic approaches and showed the existence of Nash equilibrium in the system and its uniqueness. This takes care of the free rider problem in the IDS. Then finally we move on to MDP and reinforcement learning which helps in breaking the model into smaller sub models to find the optimal strategy for the game. All these techniques and methodologies when put together gives us a secure and robust Collaborative Intrusion Detection System which enhances the security of the network and the overall system.

References

1. Yegneswaran, V., Barford, P., Jha, S.: Global intrusion detection in the DOMINO overlay system. In: Proceedings of Network and Distributed System Security Symposium (NDSS04) (2004)
2. Zhu, Q., et al.: A game-theoretical approach to incentive design in collaborative intrusion detection networks. In: International Conference on Game Theory for Networks, 2009. GameNets' 09. IEEE (2009)
3. Fung, C.J., et al.: Dirichlet-based trust management for effective collaborative intrusion detection networks. IEEE Trans. Network Service Manage. **8.2**, 79–91 (2011)
4. Zhu, Q., Tamer, B.: Dynamic policy-based IDS configuration. In: Proceedings of the 48th IEEE Conference on Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. IEEE (2009)
5. Fung, C., Baysal, O., Zhang, J., Aib, I., Boutaba, R.: Trust management for host-based collaborative intrusion detection. In: 19th IFIP/IEEE International Workshop on Distributed Systems (2008)
6. Fung, C., Zhang, J., Aib, I., Boutaba, R.: Robust and scalable trust management for collaborative intrusion detection. In: 11th IFIP/IEEE International Symposium on Integrated Network Management (IM09), to appear (2009)
7. Karel, B1., Martin, R.: Trust-based solution for robust self-configuration of distributed intrusion detection systems. In: The 20th European Conference on Artificial Intelligence, ECAI (2012)
8. Alpcan, T., Basar, T.: A game theoretic approach to decision and analysis in network intrusion detection. In: Proceedings of the 42nd IEEE Conference on Decision and Control, Dec 2003
9. Alpcan, T., Basar, T.: A game theoretic analysis of intrusion detection in access control systems. In: 43rd IEEE Conference on Decision and Control, 2004. CDC, vol. 2. IEEE (2004)
10. Alpcan, T., Basar, T.: An intrusion detection game with limited observations. In: Proceedings of the 12th International Symposium on Dynamic Games and Applications (2006)
11. Nguyen, K.C., Alpcan, T., Basar, T.: Fictitious play with imperfect observations for network intrusion detection. In: Preprints of the 13th International Symposium Dynamic Games and Applications (ISDGA 2008). Wroclaw, Poland (2008)
12. Liu, H.M.Y., Comaniciu, C.: A Bayesian game approach for intrusion detection in wireless ad hoc networks. Valuetools, Oct 2006
13. Alazzawe, A., Asad N., Bayaraktar, M.M.: Game Theory and Intrusion Detection Systems. (2006)
14. Lye, K., Wing, J.M.: Game strategies in network security. Int. J. Inf. Secur. **4**(1–2), 71–86 (2005)
15. Alpcan, T., Basar, T.: An intrusion detection game with limited observations. In: Proceedings of the 12th Internationl Symposium on Dynamic Games and Applications (2006)
16. Wikipedia Contributors: Markov decision process. Wikipedia. The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 7 April 2015. Web.16 April 2015
17. Wikipedia Contributors: Reinforcement learning. Wikipedia, The Free Encyclopedia. Wikipedia. The Free Encyclopedia, 9 April 2015. Web. 16 April 2015