Research Article

Design of an Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN) Using Cooperative Overlay Network

V. Akilandeswari and S. Mercy Shalinie

Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, Tamil Nadu 625010, India

Correspondence should be addressed to V. Akilandeswari; akilasenthil07@gmail.com

Received 8 October 2013; Revised 4 February 2014; Accepted 5 February 2014; Published 30 March 2014

Academic Editor: Neil Y. Yen

Copyright © 2014 V. Akilandeswari and S. Mercy Shalinie. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The main objective of this paper is to propose Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN) which includes self-management and self-defense in the network. The proposed network has the following considerations. (1) Dynamic coevolution is elucidated with interaction between independent rational strategies and structure of overlay network. (2) Evolutionary Game Theory (EGT) specific to overlay network is adopted with the combination of network reciprocity and group selection mechanism. (3) The cooperative efficient network structure is put forth by the multinode link-formation game. In this network, each node will be trained independently based on Naïve Bayes classification algorithm to react against any critical services in the network. The proposed network's significant characteristics are self-learning, independent training, collaborative detection, reaction to critical services, protecting the target machine before being collapsed, and maintaining the network performance without any hindrances. It controls the flow of high rate critical services such as Distributed Denial of Services (DDoS) flooding attacks and blocks the unwarranted services without any interruption to legitimate users. Hence, there is no doubt that this self-managed and self-defensive system will move from realm of fiction to real-time network engineering with high detection accuracy (98.3%), classification rate up to 99%, and improved clustering coefficient.

1. Introduction

A network is nothing but billions of tightly connected and distributed heterogeneous systems. The network systems are vulnerable to getting affected by some source of abnormalities, which results due to attacks launched by set of compromised computer systems, otherwise known as “zombies.” A compromised computer system operates through a simultaneous interaction among large number of hosts which are distributed through the Internet [1]. Zombies normally throw an extremely high volume stream of packets towards the target machine. Various kinds of abnormalities will create some critical situations which will end up in a network node failure. Most of the critical network services consume the bandwidth resources of the network or the computing resources at the target system.

Providing security to all the internet communication machines against the network critical services is unrealistic and also remains as an unsolved problem. It is true to say that popular websites handle these critical network attacks by protection system with abundant resources. Even the protection systems will sometime fail when the attacks become highly intensified.

Dynamic defense mechanism helps to detect the network attacks and respond by dropping the excess traffic. The ideal defense mechanism detects the abnormality before reaction mechanisms realize that an attack must be detected before a response can be mounted [2]. This may be achieved even though when there are no common characteristics on attack traffic to detect the nature of attacks near the source [3]. At this juncture, the dynamic defense mechanism should make unsupervised changes in the compromised computing environment. Hence this type of defense mechanism will possibly stop the attack closest to the source. Moreover, this will not disturb the network resources and network
An overlay network is a virtual topology found on the top of the current underlying infrastructure, which consists of autonomous systems and independent nodes [3]. The overlay network nodes are locally interactive and need the collaboration of its autonomous level system and numerous constituent parts of independent nodes for effective functioning. Most of the participating nodes contribute some of their resources; while some of the nodes show unwillingness to contribute their resources, the implications of the selfish behavior can be found in the overlay networks. In reality, many nodes show selfish behavior to maximize their own utility by exploiting the system without contributing among them [4].

The concept of having overlay network is an effective technique to support new application as well as protocols without any changes in the underlying network layer. This concept is helpful in finding Quality of Service (QoS) and multicast services in the light weight traffic differentiation schemes without any significant complexity. It also helps in providing virtual network infrastructure for each user and application.

The Internet is organized as an independent operating Autonomous System (AS). In this architecture, the detailed routing information is maintained only within a single AS and across its constituent networks [5, 6]. The AS can be independently administered and configured and that is why it is operated by some network service providers in other networks. However, using Border Gateway Protocol 4 (BGP-4), the information shared with other service providers and the AS can be heavily filtered and summarized by having border router connected to AS. This BGP hides many topological details due to its heavy cost [7].

The overlay topology can significantly impact the overlay routing in terms of routing performance and routing overhead. Mainly, physical topology information can benefit by constructing an efficient topology. The improved routing performance can be obtained within the overlay network by using the better topology construction. Several different overlay network services are available such as Resilient Overlay Network (RON) [8], Service Overlay Network (SON) [9], QoS-aware Routing for Overlay Networks (QROS) [10], and OverQoS [11]. Unfortunately, these overlay network nodes are selfish and strive to maximize their own utility by exploiting the system without contributing much for it [4]. The selfish behavior in overlay networks has important implications, that is, the nodes’ unwillingness to contribute bandwidth or memory. Most of the aforementioned existing approaches are based on the growth rules that depend on the instantaneous and full topological properties of the network and devoid of the coevolution between the network structure and individual rational behaviors.

For this purpose, we design an Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN) using evolutionary algorithm. It tries to detect and react to the DDoS attacks at the intermediate level. This network focuses on effective information sharing by providing current incoming traffic attack messages, which is generated by detection algorithm through the overlay network. The algorithm helps in deriving the accuracy of classification and clustering coefficient. The Evolutionary Game Theory- (EGT-) based overlay topology provides high-level global network efficiency and widespread cooperation among the independent nodes. Further, it improves the accuracy of DDoS detection.
in the intermediate networks using the machine learning approach. In AD-CERN system, the resilient and scalable communication mechanism can be obtained to exchange the attack information within the large scale networks and by designing sharing gossip and warning messages the overhead information sharing can also be reduced.

The main objective of this paper is to design an overlay network with an Evolutionary Game Theory- (EGT-) based overlay topology evolution scheme and include this infrastructure into our proposed AD-CERN system with the following features:

(i) EGT-based overlay network brings the cooperation between individual nodes and prevents the nodes from indulging in selfish behavior;
(ii) using entire cooperative overlay network with increased network efficiency;
(iii) higher detection rate and improved classification accuracy;
(iv) with the power of adaptivity, the network reacts to the attack at an early stage;
(v) protecting the network with machine learning-based training and learning;
(vi) finally, with improved performance potential, AD-CERN system should be deployed for self-management and self-defense.

The rest of this paper is organized as follows. Section 2 briefly reviews some essential notations, including evolution of cooperation, network reciprocity, group selection, and multinode link-formation game theory; Section 3 discusses design of EGT-based overlay topology and their evolutionary operation of individual nodes. Section 4 proposes Adaptive Distributed Critical-Care Extensive Response network (AD-CERN) with machine learning-based Naïve Bayes classification algorithm. Section 5 theoretically analyzes the EGT-based overlay network performances. Section 6 discusses the design of AD-CERN system, operation, and efficiency evaluation. Section 7 compares the evaluation results in the existing overlay network. Section 8 concludes this paper with self-defense and self-management nature of AD-CERN system and possible future extensions.

2. Preliminaries

The cooperation means selfish replicators which should forgo some of their reproductive potential to help one another [12]. Unfortunately, in reality, many existing overlay network nodes are selfish and maximizing their own utility. Generally, natural selection implies competition between nodes and therefore nodes oppose cooperation unless a specific mechanism is at work. Figure 2 shows the declining process of average fitness without involving the evolution of cooperation C and natural selection of defectors D.

A cooperator C is someone who pays cost c for another individual to receive a benefit b. A defector D has no cost and does not deal out the benefits. Cost c and benefits b are measured in terms of fitness as:

$$\text{fitness} = \frac{(\text{Own contribution} + \text{Contribution of relatives})}{\text{Average contribution of the population}}$$

(1)

In any mixed population, defectors d have a higher average fitness than the cooperators c. The natural selection process acts to increase the relative abundance of defectors which helps in establishing cooperation [12].

2.1. Evolution of Cooperation. Evolution is based on the brutal competition between the individuals and should therefore reward only selfish behavior [12]. In reality, every organism is designed to promote its own evolutionary success at the expense of its competitors. Biological and social science model behaviors are expressed in the form of evolutionary algorithms [13]. These entities are represented as interacting, mutable, and reproducing. These entities are also represented as a computational model. Such models are coevolutionary in nature, which means individual entities expose some kind of interaction with other evolving entities in the population [4]. Generally it includes three phases: interaction phase, reproduction phase, and mutation phase.

Interaction Phase. It specifies the rule of entities which interacts and gains some rewards.

Reproduction Phase. Each agent differently reproduces offspring based on its utility. It can be genetic or cultural reproduction.

Mutation Phase. In the reproduction stage, with a very small probability, the agents change their structure to incorporate innovation.

Cultural reproduction entities are seen as behaviors that can horizontally replicate between nodes within a generation. This interpretation is accommodated within the overlay network structure evolution. In [12], the author discusses the five mechanisms for the evolution of cooperation such as kin selection, direct reciprocity, indirect reciprocity, network reciprocity, and group selection. A simple rule is derived from each aforementioned mechanism which specifies whether natural selection can lead to cooperation or not. The network reciprocity and group selection mechanisms are found to be perfect for constructed EGT-based overlay topology with an adaptive distributive nature.

In network reciprocity, the natural selection of defection is based on a well-mixed population, where everybody interacts equally with each other. Figure 3 includes the
mechanisms of network reciprocity which means the cluster of cooperators outcompete defectors [4, 12].

The real world interactions are often restricted to small local groups, because real populations are not mixed. Spatial structures or social networks imply that some individuals interact more often than others. Evolutionary Graph Theory allows us to study how a spatial structure affects evolutionary and ecological dynamics [14].

The network reciprocity equally interacts with every node in the overlay network. Individuals occupy the vertices of the graph and the edges denote who interact with whom. The graph is fixed for the duration of evolutionary dynamics [15, 16]. This evolutionary dynamics on graphs can favor operation over defection if the benefit-to-cost ratio $b/c$ of the altruistic act that exceeds the average number of neighbors, $K$, per individual is

$$\frac{b}{c} > K. \quad (2)$$

This result is given as the generalization of "spatial reciprocity."

In the overlay network construction, nodes’ interaction is constrained to its neighbors instead of fixed network of some duration. In coevolutionary model, links are removed based on the members of the population with respect to time [17].

The main objective of group selection is to form a close relationship with the individual group nodes and to find out more suitable groups of nodes. Group selection refers to the process of natural selection which favors the characteristics in individuals and increases the fitness of the group individuals [12]. Figure 4 shows the idea of group selection competitions, which is not only between individuals but also between the groups.

Group selection splits up the population into groups, which determines the interaction scope of the agents. Individually reproduced proportional payoff and its offspring are added to the same group. If the group reaches certain size, it can split up into two with a certain probability.

The perfect cooperator groups grow faster than pure defector groups, whereas, in any mixed group, defectors reproduce faster than the cooperators. Therefore, the selection on the lower level (within group) favors defectors, as the selection on higher level (between groups) favors cooperators. Hence, under some conditions, well-performing groups can survive and the agents of groups providing poor conditions will be eliminated automatically [18].

The authors consider that if $n$ is the maximum number of group sizes and $m$ is the number of groups, then group selection allows for the evolution of cooperation, provided that

$$\left(\frac{b}{c}\right) > 1 + \frac{n}{m}. \quad (3)$$

Group selection is a fully decentralized mechanism that focuses on the dynamic view of groups and iteratively guides its evolution towards more optimal configurations.

The node’s neighbor views the group and the reproduction phase. It is imitated to join the filter group attacks. Furthermore, explicit investigation on evolution of the adaptive distributed overlay network structure based on the node’s local interaction is carried out.

2.2 Multinode Link-Formation Game. Multinode link-formation game [4] is an overlay network which characterizes self-interested nodes to form links in the overlay network. Each node keeps one link to a cooperative neighbor node in its neighborhood node which can slightly speed up the convergence cooperation and increases the network efficiency. Individual nodes are capable of making rational choices to establish new links or to give up existing links. Social dilemma of forming links in an overlay network says the aggregation of payoffs by mutual cooperation nodes and the aggregated payoff is always better than higher payoffs given by deflection node [12]. Cooperative overlay network evolution is analyzed by coupling the network formation rules with dynamic states of the elements in the system. Dynamic evolution of the network can be evolved similar to biological method, using the design of multinode link-formation game with their neighbor nodes, and each node preferentially links to the more suitable node with higher
utility and joins the group selection to form the similar neighborhood.

Here, we combine the network reciprocity, group selection, and multinode link-formation game to evolve the arbitrary EGT-based overlay topology for achievement of “Adaptive Distributed Critical-Care Extensive Response Network” (AD-CERN).

3. Construction of EGT-Based Overlay Network

In this section, the effect of cooperation and rational behaviors on the overlay network nodes is theoretically analyzed. For the evolution process, the evolutionary mechanisms [4] are adopted for the construction of EGT-based overlay network topology such as network reciprocity [12], group selection [12], and multinode link-formation game [4]; these are described in Section 2.

3.1. Cooperation among Overlay Network. Cooperation is needed to obtain the dynamic co-evolution between independent nodes on the overlay networks. The overlay network operates based on the principle of cooperation and it has an ability to run an application in particular node. A cooperator C is someone who pays a cost $\hat{c}$ for another individual to receive a benefit $b$. The cooperator behavior brings cooperator cost $\hat{c}$ and brings its partner the benefit, that is, 1. The defect node D faces no cost because it will not use a resource to provide any service for its partner. In general, most of the aforementioned existing overlay network nodes are based on growth properties and it neglects the coevolution between the network structure and individual rational behaviors [3, 19, 20].

3.2. Rational Behavior of Overlay Network Nodes. According to the general concept of EGT, individual nodes will imitate the behavior of other nodes that has the higher utility. Including the same, the node can randomly discover the other nodes from the entire overlay network and compare the utility with them.

Moreover, nodes can change its strategy and drop/make links to other nodes based on the comparison of utility. Mainly, we consider this rational behavior to deal with the selfish behavior in overlay network topology formation using the fact “Tragedy of Commons” [21]. It aims to produce a simple generalized topology evolution scheme that is scaled well and functions under a reasonable selfish assumption.

3.3. Evolutionary Mechanism. The evolutionary mechanism decorates the overlay network as convergence of autonomous and rational nodes into a cooperative network structure. Network reciprocity forces an overlay network as cooperative by means of simple interaction among autonomous and rational nodes.

First, the overlay network is constructed with the following structure. Let us consider the population of $N$ nodes consisting of cooperative C and defect D nodes; initially all nodes randomly form connections as in Figure 5, and all nodes adopt the “defect” D strategy except the nodes having the “cooperative” C strategy. A cooperative node helps all neighbors to bring cooperator to some cost, which is forwarding packets or answering queries for its neighbors or sharing information to all neighbors [4, 22]. Any two nodes can make a connection without loss of generality; the cooperative C node brings cooperator cost $\hat{c}$ and gives its partner the benefit $b$, that is, 1. The defect node D faces no cost, because it will not use any resource to provide any service for its partner.

$\hat{c}$ is decided by specific scenarios and varied according to different nodes. Here the maximum cost nodes are assigned to $\hat{c}$ as $\hat{C}$ = maximum cost of nodes.

Thus, at each step, neighboring node calculates payoffs from Table 1 according to their strategies, that is, cooperative C and defect D, where $H = [(b - c)k - 2c]/(k + 1)(k - 2)$ and K is the number of neighbors.

Each matrix is helped to derive the necessary conditions for evolution of cooperation. It simply specifies the interaction between cooperators C and defectors D. The payoffs elements are summarized in Table 2, which are derived between neighbor node i and node j ($\hat{C}$ is constant).

In Figure 5, the connection between network nodes is fixed. Here the main issue is how to construct an overlay
network with minimized average neighbor distance. Initial stages of randomly selecting neighbors may result in more links between far away host and fewer links between nearby hosts. The resulting average neighbor distance would be relatively long. It degrades the network efficiency [7, 23]. The simple multinode link-formation game is used to capture the intrinsic problem of link creation among the overlay network nodes. It is very much different from Bilateral Connection Game (BCG) [24, 25]. The multinode link-formation game is proposed to characterize the topology formed by selfish nodes, in which each node attempts to minimize nodes and minimize costs by minimizing the number of connections. In addition, each node establishes a sum of the costs of reaching all other nodes. Multinode link-formation game shows that is very difficult for each node to utilize local information based on global network topology. The partial view of overlay structure and the local interaction with the neighbors are combined to obtain its utility.

This link-formation game concept is more feasible for large scale and dynamic p2p network nodes to obtain overlay approach.

Here, nodes locally interact with a small subset of partners defined by current network topology. Every step of interaction, individual node, and its neighbors invoke their strategies to get the utility using Tables 1 and 2. This iterative interaction calculates an individual’s payoff which is sum of the payoffs obtained across the bilateral game [4]. Thus, it is named as multinode link-formation game. An individual node’s utility is determined by the following factors:

1. (1) degree of the node;
2. (2) strategies of the neighbor nodes.

The multinode link-formation game implies the following factors.

If node i is cooperative, then node i’s utility \( U_i(G) \) in the formed overlay network graph \( G \) can be denoted as follows:

\[
U_i(G) = (1 - \delta) n^c_i(G) - \delta n^nc_i(G) = n^c_i(G) - \delta \eta_i(G). \tag{4}
\]

If node i is noncooperative, then its utility is

\[
U_i(G) = n^c_i(G), \tag{5}
\]

where \( \eta_i(G) \), \( r^c_i(G) \), and \( n^nc_i(G) \) represent the number of node i’s total neighbors, node i’s cooperative neighbors, and node i’s noncooperative neighbors in the formed overlay network structure \( G \), respectively.

In the evolutionary phase, the multinode link-formation game designated defect node’s utility is 1, and this node is compared with the cooperative node. It is illustrated in Figure 6. If the cooperative node’s C utility \( (2 - 2\delta) \) exceeds 1, then the designated defect node D will copy the designated cooperative node’s C strategy and the resulting link structure will add an extra link to the right side node [4].

Figure 7 shows the formation of the nodes connectivity in the overlay network which evolves from the above multinode link-formation game. The dotted lines represent the added links in the evolutionary phase. Thus, the structure characterizes the social dilemma of forming links in an overlay network, and it incorporates individual rational decisions. In addition, individual node preferentially links to the more suitable nodes with higher utility and forms the group.

Normally, a group consists of a set of nodes that are close to each other. For any positions, \( P \), in the physical network, if the distance between \( P \) and node i and the distance between \( P \) and node j are the same, then they are likely to form a group. Assume that nodes i and j are in the same group. Here, the distance between two nodes can be network latency, or round trip time, or minimum bandwidth on the links along a path between the two nodes, or some user-defined cost functions between the two nodes. A group can exchange messages with several other groups, which are referred to as neighbor groups. The neighbor groups in this overlay are the groups that are nearby the underlying physical network.

3.4 Operation of Evolutionary Game Theory (EGT-) Based Overlay Topology. Figure 8 shows the operation of individual EGT-based overlay network node. In this scheme, nodes are randomly bootstrapped into an arbitrary network structure. In the beginning, 10% of the nodes are cooperative in nature; then the three phases of evolutionary algorithm such as interaction phase, evolution phase, and mutation phase are included for entire cooperative overlay network.

In the interaction phase, initially, each node and its neighbors are connected by the current network structure with their strategies and get payoffs as per Tables 1 and 2.
Secondly, by applying the evolution phase according to their satisfactory condition, the node is reallocated to a new neighborhood view. It happens when the node \( i \) is failed to find a suitable node in the overlay network and then the node \( i \) skips the operation in this round and directly goes to the mutation phase as in step 9 of Figure 8. In addition, each node drops its neighborhood view and randomly selects nodes to form a group. In mutation phase, the creation of a brand new group, that is, node \( i \) which discards its current group and randomly selects a node to form a link. As a result, the other nodes migrate to the seed group in the future and increase the group size. Hence, the introduction of mutation in cooperative and defect strategies is unnecessary for the emergence of cooperative/coordination.

The interpretation of cultural reproduction is accommodated in the overlay network structure. In our proposed technique, reproduction phase will help to produce a counterpart of the existing overlay network by either rewiring the nodes or changing the topology of the network. It is a simple logical process in which nodes drop, copy, or exchange symbolic links [4, 12].

Here multinode link-formation game can be done as pairwise, which means two nodes should provide mutual consent in the formation of a link connection [4]. Hence intuitively, each node will form a link with another node. The former node should persuade the latter to accept this connection. Therefore, based on the simple economic strategy in the node’s evolutionary phase, the node will keep the link to one cooperative node in its original neighborhood view as shown in Figure 7. On the whole, this process will facilitate the evolution of an overlay network structure.

4. Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN)

Machine learning and data mining theories provide the relevance of self-management and self-defense to the networks and its distributed systems. For the proposed AD-CERN, EGT based on efficient overlay network has been used and the details of which are mentioned in the Section 3. Nodes in this EGT-based overlay network will be inducted with detection and classification capabilities. They cooperatively detect and react to critical behaviors before specific response mounts in the target machine or network performance degradation. The machine learning induction provides the power of adaptivity in particular application techniques [26].

This AD-CERN node includes detection, classification, information sharing, network learning, and training phase as in Figure 9.

4.1. Detection Algorithm. In this phase, each node is equipped to detect whether current incoming network traffic represents the normal or critical situation in the system. Here, the “IP address-based high rate flooding attack detection” algorithm [1] is included to detect the traffic behavior changes in the specific traffic measures and send gossip to the classification phase. Inclusion of multiple detection algorithms in every node helps to achieve higher detection rate.

4.2. Classification Algorithm. This phase has high sensitivity than all other ones and also called as detection-and-reaction phase. When the gossip message arrives, the accumulated mean for its destination is renewed and a gossip is added for that destination. Then each node gathers self-gossip and neighbor-gossip as shown in Figure 9. After this, classifier node will evaluate message attributes like <source, warning, destination, gossip>.

It uses the statistical or machine learning classifiers to produce predictions about the incoming traffic. It distinguishes the critical traffic patterns from normal traffic patterns. The well-known Naïve Bayes method [27] is used to integrate and share local traffic information with neighbors. Here network reciprocity is adopted for equal interaction among the nodes.
4.3. Information Sharing. The information sharing improves the classification with the two kinds of messages. These messages are shared between nodes to update the maximum global knowledge about traffic. In the first step, gossips help to indicate suspicion of flooding attack. It is sent and received to/from the neighbors in any direction of the overlay network. In the second step, warning, it is another message which helps to indicate high certainty of an ongoing attack. It is sent only in the direction of attackers, in order to strangle attacks as close as possible to the source.

4.4. Network Learning and Training. Generally, overlay network nodes have different characteristics depending on the context and the network situation. Here the classifier accuracy itself seems to be a problem; hence it can be resolved by adjusting the classifiers according to their detection algorithm, maintenance level of trust to a concrete gossip, and checking the amount or type of usual traffic which passes through the node.

Thus, the network nodes are equipped with a learner/classifier. With the machine learning technique each node’s ability should be trained to adapt their thresholds of gossips trusting and detection mechanisms for each target node. Now a perfect training is given to the node which is similar to its situations denoting it as critical.

In the Naïve Bayes method, different message attributes are supposed to be statistically independent. The description of this method uses the two numbers $a$ and $b$, and they are denoted as a destination warning, gossip, respectively,

\[
a < b = \begin{cases} \{1 & \text{if } a > b \} \\ \{0 & \text{if } a < b \} \end{cases}
\]

Given a traffic $T$, regarded a tuple $<\text{source, warning, destination, gossip}>$, the Naïve Bayes method estimates of $P(\text{Attack} | T)$ and $P(\text{Non_Attack} | T)$ and simply predicts “Critical” status when $P(\text{Attack} | T) \leq P(\text{Non_Attack} | T)$ and, otherwise, it says “Normal” status [27]. These two probabilities are computed using Bayes theorem; that is,

\[
P(\text{Attack} | T) = \frac{P(T | \text{Attack}) \cdot P(\text{Attack})}{P(T)}.
\]

The observed $P(T)$ can be disregarded because it only cares with the ratio of $P(\text{Attack} | T)$ and $P(\text{Non_Attack} | T) \cdot P(\text{Non_Attack} | T)$ and $P(\text{Non_Attack} | T)$ can be estimated from training data, locally to each node.

To estimate $P(T \mid \text{Attack})$, use the independence assumption, as follows:

\[
P(\text{source, warning} | \text{Attack}) = \frac{P(\text{source, warning, attack})}{P(\text{Attack})},
\]

\[
P(\text{Destination, Gossip} | \text{Attack}) = \frac{P(\text{Destination, Gossip, Attack})}{P(\text{Attack})},
\]

where $P(\text{Attack})$ is the attack ratio at this node.

We train the network node by enabling the gossips and at the same time warnings must be disabled. In total, the Naïve Bayes machine was found to be learned the following things which (1) increases the “Critical” status warning probability and decreases the “Normal” status warning probability; (2) the probabilities remain stable until a relative high number of gossips get decrease, where the “Critical” status probability increases, and “Normal” status warning probability becomes zero. It means that the False Positive Rate (FPR) and True Positive Rate (TPR) rate are rich and False Negative Rate (FNR) is zero in every node of AD-CERN system.

If the critical services appearance is suspected, this status will help to determine whether a message to a particular node should be forwarded or blocked. The entire cooperative
network drives overlay network nodes to learn about the behavior of its portion of network by adjusting its classifier to its own location in the network traffic. As in Figure 10, overlay network nodes can exchange gossiping and warnings about the declared critical attack service. When the warning arrives to the border-gate nodes, it curtails the attacks whichever is very close to the source, while the gossips keep all the border-gate nodes. Every node in an overlay network is nothing but a key node and the nodes which receive the more request than the other are only facing enormous attacks. Hence, in the overlay network, the node should maintain the detection mechanism even during the abnormal situation and further it should exchange and aggregate the information about traffic condition in all different parts of the network system. In order to restrict the attack strike to the network borders, a backward warning system is included to the source which is as close as possible. By implementing this method, our network elements will learn to determine whether the situation is normal or critical. Even though the attacks are found very close to the border gate of the network; it can be curtailed before reaching the victim.

After this operation, EGT-based overlay network is able to stop and avoid distributed critical services, like high rate flooding, abuse, or failures. Each node shares with its neighbor's node the status of the network and aggregates its local information using the nature of evolution of cooperation. It includes every node into the convergence of cooperation and increases network efficiency. As a result of the above discussed facts, the present AD-CERN system comes into existence. Now the AD-CERN will work in self-optimizing, self-organizing, self-healing, and self-defending methodology, in order to protect networks against critical network service attacks and network node failures. Here, each node is allowed to make unsupervised changes in the computing environment. This permission will definitely increase the ability of AD-CERN system, particularly, while independent learning during any critical situation. Hence, this network is named as an “Adaptive Distributed Critical-Care Extensive Response Network” (AD-CERN).

4.5. Performance Analysis of Evolutionary Game Theory-(EGT-) Based Overlay Network. In this section, the proposed EGT-based overlay network is considered as a connected graph as in Figure 11(a), where each node in the graph represents a group in the overlay network and neighbor relationship between two groups is represented by edges between two nodes in the overlay. In Figure 11(b), the overlay network nodes are arranged in the tree structure [7]. The root of the tree is node A as in level 0.

Node A’s direct neighbors, B, C, and D, are one hop away and are placed below node A (at level 1). Here, the node A is the parent of nodes B, C, D and nodes C and D, are children of node A. Then, each node adds its neighbor into the tree. This process is repeated until all nodes are included in the tree structure.

The proposed overlay network’s performance is analyzed with average neighbor distance \( N(E) \), network efficiency \( E(G) \), and average clustering coefficient \( C(G) \).

4.5.1. Average Neighbor Distance (AND). The AND \( D \) of our proposed EGT-based overlay network is theoretically calculated using the formula:

\[
D = \frac{D_i \cdot (N \cdot n \cdot m) + D_b \cdot (N \cdot M)}{((N \cdot n \cdot m) + (N \cdot M)) / 2}
\]

\[
D = \frac{D_i \cdot n \cdot m + D_b \cdot M}{n \cdot m + M}
\]

\( \text{Figure 10: Overall operation of Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN) during critical services.} \)
The EGT-based overlay network contains the $N$ groups and each group consists of $n$ hosts. Every group has $M$ neighbor, in which each host has $m$ neighbor hosts. The average distance between neighbor groups is denoted as $D_b$ and the average distance between two hosts in the same group is denoted as $D_i$. The total number of intragroup neighborhood links is $n \cdot (m/2)$. The total number of intergroup neighborhood links is $N \cdot (M/2)$.

The proposed EGT-based overlay network will prove the shorter average neighbor distance as in Figure 12 and this will be comparable with Randomly Connected Overlay (RCO) Network.

This could be attained with the concept of group selection mechanism as discussed in Section 2 which allows for the evolution of cooperation. It focuses on the dynamic view of group selection and iteratively guides its evolution towards more optical configuration. Moreover, it decreases the $D_b$ with the shortened neighbor links between different groups. It increases them with more neighbors in the same group. Finally, it helps to place the hosts to their proper group and further increases the $D_i$ so that $(D_i = D'_i)$.

4.5.2. Network Efficiency $E(G)$. The measurement of network efficiency [7] $E$ shows how efficiently the network exchanges the information between the nodes. The efficiency $\varepsilon(G, j, K)$ in the communication between the two points $j$ and $K$ is defined as the inverse of the shortest path length $d(G, j, K)$, and the efficiency of $G$ is the average of $\varepsilon(G, j, K)$; that is,

$$E(G) = \frac{1}{N(N-1)} \sum_{j \neq k \in G} \varepsilon(G, j, k)$$

In the Randomly Connected Overlay Network, that is, the nonconnected graphs, there is no path between the two points $j$ and $K$, $\varepsilon(G, j, K) = 0$, and $d(G, j, K) = +\infty$. For that reason, EGT adopts the network reciprocity for equal interaction with every node $N$ in the overlay network.

4.5.3. Average Clustering Coefficient $C(G)$. The calculation of clustering coefficient [4] $C(G)$ of node $i$ is defined as

$$C_i = \frac{\text{Number of edges in } G_i}{\text{Maximum possible number of edges in } G_i}$$

$$= \frac{\text{Number of edges in } G_i}{K_i(K_i - 1)/2}$$

where $G_i$ is the subgraph of neighbors of $i$ and $K_i$ is the number of neighbors of node $i$.

5. Simulations

5.1. Network Topology. In this work, two topology models are used in the simulation. The first overlay network is constructed randomly, and nearby hosts in the overlay network may actually be far away in the underlying network (Figure 1).

In another network topology, network is equipped with the intermediate network nodes and border-gate nodes with the detection mechanisms and classification technique. The nodes can exchange gossiping and warnings about the
declared critical attacks. The main aspect is that all routing nodes from the network should be passed only through the overlay networks. But this may be unfeasible in practice. Hence, considering this difficulty, the cooperative overlay network is constructed as in Figure 13.

5.2. Dataset. Using our proposed network topology as in Figure 13, HTTP server collects the normal and attack traffic. Normal traffic is generated between the victim and nodes in the intermediate network. For the attack traffic, Stacheldraht [28] is used to generate distributed denial-of-service attack traffic. During this attack period, all nodes receive the generated attack traffic.

The Stacheldraht is selected because it is a more matured attacking tool compared to other attacking tools, such as TFN, TFN2k, or Trinoo. The Stacheldraht is composed of handler (master) and agent (daemon) programs [29]. The handler system scans vulnerabilities of the victim before ending an attack command to the corresponding multiple agent systems. Agent systems produce a large flood of packets targeting the victim. It interrupts the system resources and network resources. For the evaluation of network, two types of flooding attacks are collected for some periods: TCP-SYN flooding and UDP flooding. Attack traffic profiles are gathered during the attack period. The parameters are depicted in Table 3. Figure 14 shows a typical traffic behavior in border-gate nodes.

| Attack profile | SYN flooding | UDP flooding |
|----------------|--------------|--------------|
| Period 1       | 95%          | 78%          |
| Period 2       | 87%          | 76%          |
| Period 3       | 85%          | 78%          |

Table 3: TCP SYN and UDP flooding attacks at border-gate nodes.

6. Network Evaluation

6.1. Randomly Connected Overlay Network (RON). The individual nodes are equipped with detection algorithm and placed in the egress routers of an autonomous system, which collect meaningful information and locally detect Distributed Denial of Service (DDoS) attacks. The system shares the attack information using gossip protocol within the next-step-node only. Detection algorithm will detect any local attacks and the local decision will be sent to the cooperative detection engine [3, 19]. It combines these local decisions from the neighboring nodes. Finally, the detection decision will take appropriate action to defend the attack. In Figure 15, the TCP SYN attacks and UDP attack have moderate detection rate as 65% and 45%, respectively, and also depend on the local detection algorithm.

6.2. Evolutionary Game Theory-(EGT-) Based Overlay Network. This network will run in the normal status until a critical service appears, like DDoS flooding attacks. It attacks the path to the service and also interferes with normal
The detector ingests every incoming traffic $T$ to the victim in an abnormal way. A gossip will spread among the neighbors to indicate the victim which is in attack. The network reciprocity mechanism helps the overlay nodes to interact equally with every node in the overlay network. In connection to this, all the neighbors will receive the gossip. The gossip message contains the possible victim ID and the confirmation. At this time, classifier determines that the victim is under attack, and immediately a warning is sent to the node from where the message is received and sent to every node. Each node uses the aggregated gossips and warnings to provide high confidence of classification accuracy. For the performance evaluation, the classification accuracy [19] is calculated using

$$\text{Classification Accuracy} = \frac{\sum_{i=1}^{n} T_i}{\sum_{i=1}^{n} I_i}, \quad (12)$$

where $I$ is an individual attack traffic record in the corresponding attack class and $T$ is the correctly classified attack traffic record. As shown in Table 4, the Naïve Bayes overall classification accuracy is above 99.3%. The result indicates that the proposed Naïve Bayes mechanism classifies attacks into detailed attack types with acceptable accuracy. It identifies the TCP-SYN attacks and UDP attacks with less false positives. At the same time, it shows mistake in false negative and absolutely there are no issues in false positives.

The EGT-based overlay network operated in the following scheme is with the warning-victim-closest nodes will indicate to the border-gate nodes to stop the attack flow and with the gossips the nodes closest to the source will indicate to the intermediate network nodes [30]. It means that the aggregated traffic is still attempting to enter the network. The result should improve the accuracy in classification and also in attack detection to stop undesired traffic as close to the sources as possible.

### 7. Performance Evaluation of Randomly Connected Overlay Network (RON) and Evolutionary Game Theory- (EGT-) Based Overlay Network

The Randomly Connected Overlay Network provides decentralized certificate authority to the nodes. The EGT-based overlay network nodes share digitally signed messages to the other nodes. By this way, it allows other nodes to validate the authenticity of sending nodes. EGT-based overlay network nodes spread their gossip among all the neighbors with network reciprocity, whereas the randomly connected nodes spread only the next-step node. Hence local anomaly can only be detected.

In EGT-based overlay network, the accuracy of the classification is very high due to the global level sharing of gossips and detection accuracy is very fast with the multinode link-formation game connectivity among network nodes. Figure 16 shows EGT-based overlay network nodes functions with 85%, 90%, and 95% detection accuracy. Table 5 lists values of True Positive Rate (TPR), False Positive Rate (FPR), and False Negative Rate (FNR). Both are rich in EGT-based overlay network.

This connectivity increases the interaction among the nodes to define the strategies of the node and to select the path to send the warning message to the node from where the message was received. In the random connection overlay network nodes, the links are completely saturated during a DDoS attack [3]. Unfortunately, standard packet flooding attacks effectively remove some sets of nodes from the infrastructure. This cooperation brings the detection and defense process before a response can be mounted to particular victim.
application-level multicasting, and media distribution. Of AD-CERN, in applications such as media streaming, real attack. We are also planning to explore exciting usages of rigid to malleability characteristics of unstructured overlay network. The AD-CERN greatly increases the network efficiency and convergence of cooperation. In addition, we are planning to deploy our gossip and warning, which will reduce the information offiction to real-time network engineering. The link-formation game connectivity maintains all the components in all critical services, so that the EGT-based overlay networks obtain the cooperative nature of infrastructure. Further, it maintains its robustness in the removal of nodes by failures or attacks. Thus the EGT-based overlay network relatively gives high level of tolerance in the network critical services. The EGT-based overlay network nodes are protected from the large amounts of data to and from the compromised overlay node.

### 8. Conclusion

In order to include the self-management and self-defense in network engineering, "Adaptive Distributed Critical-Care Extensive Response Network" (AD-CERN) is designed using evolution of cooperation mechanism. The AD-CERN is invented from two innovative techniques. At first level, the free-form and flexible structure of overlay network is included. This structure recovers the rigid nature of existing overlay network. Here, the EGT-based overlay network is adopted for the achievement of entire cooperation among the autonomous nodes. The multinode link-formation game keeps one link to the cooperative node in the nodes' original group, which leads to the formation of efficient cooperative network structure. The combination of network reciprocity and group selection mechanisms is considered for the evolution of cooperation in the overlay network.

In the second level, every node is fed with the ability to adapt. Each node gets a learning component with a mechanism for information sharing and classification techniques. The machine learning and data mining techniques use Naïve Bayes classification algorithm. Here, the evolutionary mechanism leads to the global optimization procedure.

In the network evaluation, the proposed AD-CERN system detects the distributed critical attack points which are found to be closer to the service. This system achieves 99% average detection rate and 98.3% classification accuracy with very high global level sharing of gossips and warning. Moreover, it provides the highest detection accuracy in both TCP SYN and UDP flooding attacks. The FPR and TPR rate is rich in every node of AD-CERN system.

Our work is a significant step towards the exploration of rigid to malleability characteristics of unstructured overlay network. The AD-CERN greatly increases the network efficiency and convergence of cooperation. In addition, we utilize the property of physical network with shorter average neighbor distance. The robustness of network is also maintained even in the high flooding rate attacks. Thus, self-management and self-defense method is moved from realm of fiction to real-time network engineering.

In future, we are trying to utilize the more intelligent gossip and warning, which will reduce the information sharing overheard. In addition, we are planning to deploy our network structure in a real-time large scale environment with real attack. We are also planning to explore exciting usages of AD-CERN, in applications such as media streaming, application-level multicasting, and media distribution.

The link-formation game connectivity maintains all the components in all critical services, so that the EGT-based overlay networks obtain the cooperative nature of infrastructure. Further, it maintains its robustness in the removal of nodes by failures or attacks. Thus the EGT-based overlay network relatively gives high level of tolerance in the network critical services. The EGT-based overlay network nodes are protected from the large amounts of data to and from the compromised overlay node.

### Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

### Acknowledgments

The authors would like to thank their institutional authorities for extending unmatched cooperation in making available all educational materials and infrastructure required to undertake this study. Not to mention, their encouragement and moral support in helping them conducting this study successfully. Further, they would like to place on record their sincere thanks and gratitude to Tata Consultancy Services, Chennai, for their generous financial assistance to their study.

### References

[1] E. Ahmed, G. Mohay, A. Tickle, and S. Bhatia, “Use of IP addresses for high rate flooding attack detection,” in *Security and Privacy-Silver Linings in the Cloud*, vol. 330, pp. 124–135, Springer, Berlin, Germany, 2010.

[2] M. E. Locasto, “Self-healing: science, engineering, and fiction,” in *Proceedings of the Workshop on New Security Paradigms (NSPW ‘07)*, pp. 43–48, New York, NY, USA, September 2007.

[3] G. Zhang and M. Parashar, “Cooperative defence against DDoS attacks,” *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, pp. 69–83, 2006.

[4] Y. Wang and A. Nakao, “On cooperative and efficient overlay network evolution based on a group selection pattern,” *IEEE Transactions on Systems, Man, and Cybernetics B: Cybernetics*, vol. 40, no. 2, pp. 493–504, 2010.

[5] A. Castelucio, A. Ziviani, and R. Salles, “An AS-level overlay network for IP traceback,” *IEEE Network*, vol. 23, no. 1, pp. 36–41, 2009.

[6] E. S. Pilli, R. C. Joshi, and R. Niyogi, “An IP traceback model for network forensics,” in *Digital Forensics and Cyber Crime*, vol.
