A Proxy Network Topology and Reconfiguration Algorithm for Resistance to DoS Attacks*

Stephen Frechette
Riverside Research Institute
Lexington, MA USA
sfrechette@rri-usa.org

D.R. Avresky
Northeastern University
Network Computing Lab.
Electrical and Computer Engineering Department
Boston, MA USA
avresky@ece.neu.edu

Abstract

This paper proposes a novel proxy network topology. The proposed network topology exhibits several attributes that strengthen the proxy network's resistance to DoS attacks. Additionally, a novel reconfiguration algorithm for a class of proxy network topologies is proposed, and shown to decrease the topologies' vulnerability to DoS attacks. Proxy networks enable applications to communicate with users without disclosing their IP's. An application's resistance to DoS attacks is improved by hiding it behind a proxy network. We evaluate the proposed topology's fault tolerance and its effectiveness in the resistance to DoS attacks.

1 Introduction

The proxy network overlay provides a communication infrastructure that hides an application's location, therefore limiting the success of Denial-of-Service (DoS) attacks. We employ a circulant graph to create a proxy network that exhibits $maximum\ connectivity$. Given the same number of nodes and edges no other topology can tolerate more node failures without partitioning the network. The proposed n node topology distinguishes itself from others in that it exhibits $maximum\ connectivity$ for any value of $n \geq 21$ Theorem 3.1. Our proxy network topology is evaluated and compared to existing topologies using the criterion of $robustness$ and $vulnerability$ to DoS attacks. Additionally, the $diameter$ and $connectivity$ of the topologies are compared.

In previous works the authors created a Grid enabled proxy network, and monitoring software, that migrates a nodes of a proxy network from a host machine in response to network performance failures or a DoS attack [32]. Through the use of a generic DoS attack model, this paper examines proxy network topologies' ability to resist a DoS attack.

Alternate point-to-point paths among the Internet can increase the dependability of proxy networks. Data collected from a nine month sample of logs from three Internet Service Provider's backbone routers show that less than 35% of routes across the Internet are available more than 99.99% of the time [33]. This level of unreliability demonstrates the advantage of alternative paths from source to destination within a proxy network. Proxy network topologies should contain a large number of alternative paths, which serve to increase the fault tolerance of the proxy networks through redundancy.

The topology of a proxy network is an important aspect of its ability to self-protect. Our proposed proxy-network topology was chosen due to its $connectivity$, $diameter$, and resistance to DoS attacks. Additionally, the chosen topology exhibits properties that enable it to reconfigure and thus decrease its $vulnerability$ to DoS attack, although a tradeoff is an increase in message latency.

2 Paper Layout

In Section 3 the proposed graph topology is detailed. Section 4 compares the proposed topology with existing overlay network topologies using the criteria of resistance to DoS attacks. A means to guarantee a predetermined $vulnerability$ to DoS attack via a reconfiguration of the topology, for a class of proxy network topologies, is proposed in Section 5. Lastly, Section 6 presents our conclusions.

[0]This work was supported by the U.S. National Science Foundation under grant CCR-0004515

3 Overview of Selected Circulant Graph Topologies

Circulants are a class of symmetric graphs. A $circulant\ graph$ with n vertices and jumps $j_1, j_2, ..., j_m$ is an undirected graph in which each vertex v, $0 \leq v \leq n-1$, is adjacent to all the vertices $v \pm j_i$, mod n, for every positive integer i, in which $1 \leq i \leq m$. The circulant graph is denoted as $G = C_n \pm (j_1, j_2, ..., j_m)$. An example of a generic circulant graph is illustrated in Fig. 1.

3.1 Midihex Topology Definition

Within the class of circulant graphs there is a great variation in their graph $diameter$.

The $diameter$ of G is defined as the maximum of all the shortest paths from any one vertex of G to any other, i.e.,

$$d(G) = max\ d(G; x, y) : x, y \in V(G). \tag{1}$$

Since the $diameter$ can be considered a measure of transmission delay, a circulant graph that exhibits $maximum\ connectivity$ and contains a small $diameter$, is desirable. In our previous work, we employed a circulant graph in an interconnection network topology [11].

In this work we propose a novel 8 $degree$ graph, $degree$ is denoted by Δ, named the Midihex topology because its properties are similar to the $degree$ 4 Midimew graph [21, 22]. A 6 $degree$ circulant graph that can be represented by a hexagonal geometric representation [34], is equal to portions of our Midihex topology. A hexagonal tessellation upon $k+1$ levels is the geometric representation of our topology, and is illustrated in Fig. 2. The numbers within the hexagons in Fig. 2 represents the virtual IDs of the nodes. A geometric representation of our Midihex topology is a stack of the hexagonal topology defined in [34]. Our Midihex graph, of degree 8, is detailed below and is embedded into a proxy network. The Midihex graph and its $diameter$ is given in Theorem 3.1.

Theorem 3.1 *Midihex $G = C_n \pm (1, 3k+1, 3k+2, 3k^2+3k+1)$ is a circulant on n points with $n \geq 21$, $d(G) = k + \lceil \frac{k}{2} \rceil$, and $n = (2 * \lceil \frac{k}{2} \rceil + 1)(3k^2+3k+1)$. For k is any positive integer, $k \geq 1$.*

For the Midihex circulant graph described in 3.1, all vertices are reachable in $k+\lceil \frac{k}{2} \rceil$ steps and $d(G) = k+\lceil \frac{k}{2} \rceil$, the proof follows.

$Proof$: The Midihex topology, and all undirected circulant graphs, are $vertex\text{-}transitive$ [25]. Due to the $vertex\text{-}symmetry$ of the graph the calculation of the distances between vertex 0 and any other vertex in the graph may be transfered to all other vertices in the graph. If a graph is $vertex\text{-}transitive$ then the graph's $connectivity$, $diameter$, and average distance can be calculated through the examination of a distance, or the $connectivity$, of one predetermined vertex to any other [25]. The $order$, i.e. number of vertices, n, of the Midihex graph is calculated in terms of k in (3).

The number of vertices in Level 0, illustrated in Fig 2, reachable by a unique path in exactly k steps from vertex 0 is calculated in (2).

$$\begin{aligned} Level\ 0\ vertices &= 1 + 6\sum_{d=1}^{k} d \\ &= 1 + 6 * \left(\frac{k(k+1)}{2}\right) \\ &= 3 * (k^2 + k) + 1 \\ &= 3k^2 + 3k + 1 \end{aligned} \tag{2}$$

The number of vertices in the Midihex circulant graph, in terms k is:

$$\begin{aligned} n &= Level\ 0\ vertices\ +\ All\ other\ vertices \\ &= \left(3k^2+3k+1\right) + \left(2 * \left\lceil \frac{k}{2} \right\rceil\right)\left(3k^2+3k+1\right) \\ &= \left(2 * \left\lceil \frac{k}{2} \right\rceil + 1\right)\left(3k^2+3k+1\right) \end{aligned} \tag{3}$$

From vertex 0 all vertices on level 0 are reachable in k steps, and from any vertex in level 0 all other levels are reachable in $\lceil \frac{k}{2} \rceil$ steps. Thus, from vertex 0 all other vertices are reachable in a most $k+\lceil \frac{k}{2} \rceil$ steps. Since the graph is $vertex\ transitive$ thus $d(G) = k + \lceil \frac{k}{2} \rceil$, and the proof for the $diameter$ of the graph is complete.

The proof continues given k is any positive integer, $k \geq 1$. For the case $k = 1$, using (3), $n = 21$; therefore the Midihex topology must always exhibit an $order$ of $n \geq 21$. Thus the proof of Theorem 3.1 is complete.

The only other degree 8 circulant graph, known to the authors, which is composed of a jump sequence that is a direct function of its $diameter$, is given in [35]. The Midihex topology is novel in that it is less $vulnerable$ to DoS attack, for $n > 637$, than the previously mentioned $degree$ 8 circulant graph. Subsection 4.1 introduces the metric employed to determine a graph's $vulnerability$ to DoS attacks. The pseudo code for the creation of the Midihex topology $G = C_n \pm (1, 3k+1, 3k+2, 3k^2+3k+1)$, for any n number of nodes, is given in Fig. 3.

3.2 Additional Graph Theory Properties of Midihex

The $connectivity$ of a graph is the smallest number of vertices that, when removed, results in a disconnected graph [19]. The formal definition follows in (4).

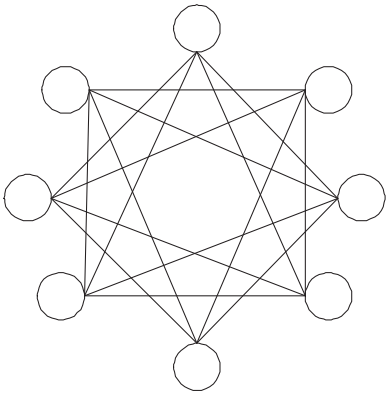


Figure 1. An example of a circulant graph, $C_8 \pm (2, 3)$.

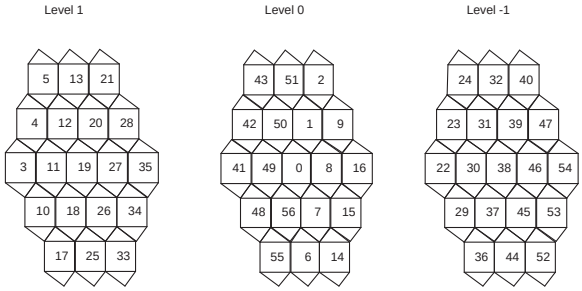


Figure 2. Geometric representation of the levels, which are stacked, of a Midihex graph $C_{57}\pm(1, 3k+1, 3k+2, 3k^2+3k+1)$ with $diameter$ of 3, i.e. $d(G_{57}) = k + \lceil \frac{k}{2} \rceil = 3$ for $k = 2$.

```
Initialize graph to be n isolated vertices labeled 0,.,n.
For i = 0 to n - 2
  For j = i + 1 to n - 1
    If j - i = 1 OR n + i - j = 1
      Create an edge between vertex i and j.
    If j - i = m OR n + i - j = (3k+1)
      Create an edge between vertex i and j.
    If j - i = (m + 1) OR n + i - j = (3k+2)
      Create an edge between vertex i and j.
    If j - i = (m + 2) OR n + i - j = (3k^2+3k+1)
       Create an edge between vertex i and j.
  END For
END For
```

Figure 3. Pseudo code for creation of Circulant graph $C_n \pm (1, 3k+1, 3k+2, 3k^2+3k+1)$, where $n \geq 21$, the $degree$ equals 8, and $d(G) = k + \lceil \frac{k}{2} \rceil$ is the graph $diameter$.

The $connectivity$ of G is

$$\kappa(G) = min\{|S| : S \subseteq V, \omega(G - S) > 1\}. \quad (4)$$

The Midihex topology, as with any circulant gaph, exhibits $maximum\ connectivity$. By definition the number of edges any circulant graph contains is $\lceil \frac{kn}{2} \rceil$, and all circulant graphs are k-$regular$. A graph is k-$regular$ if the $degree$ of each $vertex$ equals the set of edges incident upon each $vertex$ for every $vertex$ in the graph. The relation between the $degree$ of a k-regular graph its $robustness$ during a DoS attack is shown in subsection 4.1 eq. (6).

Since the $Midihex$ graph is a circulant graph, the Midihex topology contains the least number of edges necessary for the creation of a k-$connected$ graph. Because the number of edges within a $Midihex$ graph achieves the lower bound of $\lceil \frac{kn}{2} \rceil$ defined in [16], the k-$regular$ Midihex graph exhibits $maximum\ connectivity$.

The relation between graph $connectivity$ and the fault-tolerance of a network is described By Menger's Theorem (5). Menger's Theorem states that the following equation (5), below, holds for G is a connected undirected graph or a strongly connected digraph, in which x and y are two distinct vertices of G,

$$\zeta(G; x, y) = \kappa(G; x, y)\ if (x, y) \notin E(G)\ [20]. \quad (5)$$

and can be worded as follows: the $vertex\ connectivity$ is always equal to the maximum number of disjoint paths between two unconnected vertices. For the case of circulant graphs, the $vertex\ connectivity$ equals the $edge\ connectivity$. ζ is defined as the number of disjoint paths between two unconnected vertices. Two paths from u to v are defined as internally disjoint if they have no common internal vertices.

Since the Midihex graph is $maximally\ connected$ it contains the maximum number of disjoint paths between vertices for the given number of edges. Additionally, the n node Midihex graph achieves $maximum\ connectivity$ for any value of $n \geq 21$ Theorem 3.1. In comparison, a k-dimensional cube, or $hypercube$, achieves $maximum\ connectivity$ only for the cases of $n = 2^k$ [15].

A large number of disjoint paths in a network serves to alleviate congestion, and increase both the efficiency of transmission and the fault-tolerance of a network. A high level of network redundancy can increase communication efficiency because various routes to the destination may be examined, thus the least congested route can be selected.

4 Overlay Network Topologies

Generic fault-tolerant network designs have been comprehensively studied. Methods of graph augmenting

with spare nodes have also been applied to trees [5, 6, 7], rings, meshes, and hypercubes or variations of hypercubes [8, 9, 10, 26]. The addition of spare nodes and links within a hypercube, to maintain a specified level of service, is detailed in [29].

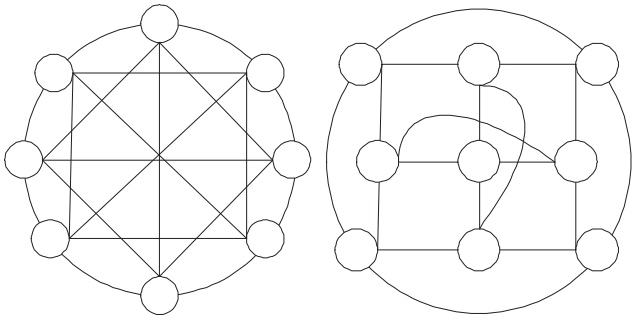
Our proposed Midihex topology's ability to resist DoS attack is compared to a few peer-to-peer and overlay networks' ability to resist DoS attacks. The use of existing distributed systems, such as Chord, has been proposed for location hiding [27, 28]. The Chord distributed lookup protocol addresses many of the problems that confront peer-to-peer applications [1]. Chord efficiently locates the node that stores a particular data item. As nodes leave and join the system Chord adapts efficiently to locate and retrieve data in a dynamic operational environment. Pastry, Tapestry, and CAN [2, 3, 14] are three lookup and routing protocols for overlay networks. These overlay networks emphasize self-organization for large-scale peer-to-peer applications. They implement a scalable, fault-tolerant distributed hash table. Using a small per-node routing table, items can be located within a small number of routing hops. A resilient overlay network (RON), which allows distributed Internet applications to detect and recover from path outages and periods of degraded performance, within a short period of time, is presented in [4]. The Chord overlay network employs a two-dimensional circular topology. The CAN overlay topology is a d-dimensional cartesian torus. Figures 4a and 4b respectively illustrate the Chord and CAN network topologies.

In the next subsection we examine the topological properties of the previous overlay network topologies with the Midihex topology, and compare their $vulnerability$ and $robustness$ to DoS attacks. The analysis of existing overlay networks is limited to their topological properties when employed as a proxy network. The examination of the partitioning of the overlay construct due to the rebalancing protocol, i.e., maintenence of routing tables, as nodes leave and join the system, e.g., during system churn, is out of the scope of this paper.

4.1 Midihex Proxy Network Topology

The Midihex network topology is evaluated for its $resistance$ and $vulnerability$ to DoS attacks. The scope of knowledge of each vertex of the Midihex topology is limited to the information associated with its neighbors, or connected vertices. We assume it is known when a node in the topology is attacked, or its integrity is compromised.

Without reconfiguration, a proxy network cannot effectively hide an application's location [17]. Proxy networks with proactive random proxy node migration can effectively prevent infrastructure-level DoS attacks [17]. The model employed in the evaluation of our Midihex



a) Chord Topology with $n = 8$.

b) CAN Topology with $n = 8$, $d = 2$.

Figure 4. Chord and CAN Network Topologies

topology is outlined in [17]. The model entails a pool of resources, or host machines, and a set of proxy servers. A node in the Midihex graph represents a proxy server. Proactive reconfiguration occurs when a proxy server migrates from one host machine to another. The model that the proxy server is under attack, or exposed to a node other than another proxy server, assumes that a proxy server can migrate to another host whose location is unknown to the attackers. An important assumption of the model is that the attack can only infiltrate a host machine, and not the proxy server. Therefore the proxy server's processes can be brought down or rendered inaccessible, but not hacked into, thus enabling a proxy server that is brought offline to reappear on another host machine.

An attack model and criterion for the evaluation of proxy-network overlays is detailed in [13]. We employ this attack model to evaluate the Midihex network topology. Several parameters are introduced, in [13], which describe characteristics of the attack. The generic attack model employed, and the corresponding chosen parameters, do not represent the characteristics of all DoS attacks, and is meant to provide insight into the proxy network topology's ability to resisit DoS attacks.

The model is represented by M(G,α,β,γ). G is the graph of the proxy network. At any time t every vertex in G is in one of three states - $intact$, $exposed$, and $compromised$. The vertices in graph G may simultaneously change their states at the end of each time step with the following probabilities: α is the probability that an $exposed$ vertex will be changed to the $compromised$ state, i.e. a node is successfully attacked during the time step. It corresponds to the attackers' capability, i.e. the rate at which hosts can be compromised. β is the probability a $compromised$ vertex will be changed into the $intact$ state, i.e. a successful proxy network reconfiguration during a time step. It corresponds to the defender's capability. γ is the probability an $exposed$

vertex will be changed into the $intact$ state. It represents the level of coordination among the attackers and the amount of memory available to the attackers.

The case of a fully coordinated attack, in which the attackers have access to infinite memory to keep and share the information about the location of all the $compromised$ and the $exposed$ nodes, is expressed as γ equals 1. Also, we choose β to equal 1. The goal of the attackers is to grow the population of the $exposed$ or $compromised$ nodes within the proxy network. Once the attacker traverses through the proxy network and reaches the application, service is denied to the user and the DoS attack is successful.

Using the model M(G,α,β,γ) a graph G is defined as $robust$ if all nodes in G can be changed into the $intact$ state after a long run. A graph G is defined as $vulnerable$ if there always exists a significant number of $compromised$ vertices in G at any time t. The problem of determining how $vulnerable$ or susceptible a given overlay network is to DoS attacks is formally defined as: Given parameters α, β and γ, characterize the class of graphs G that are $robust$ and the class that are $vulnerable$.

Two theorems are proven in [13] that characterize the ability of the attacker to propagate $exposed$ nodes throughout the proxy network. The theorems, expressed in (7) and (8), quantify some of the affects that the model parameters α, β, γ, and the Laplacian spectra, i.e. Laplacian eigenvalues of the adjacency matrix, of the network topology graph G have on the $robustness$ of the network topology.

For a Δ-regular graph, the largest standard eigenvalue of the adjacency matrix, σ_1, equals the $degree$ of the graph,

$$\sigma_1 = \Delta \tag{6}$$

Using the DoS attack model and the definition of a $robust$ graph in [13], a graph is $robust$ if

$$\frac{\beta(\alpha+\gamma)}{\alpha} > \sigma_1 \tag{7}$$

where σ_1 is the largest eigenvalue of the adjacency matrix [13].

For a Δ-regular graph, the Laplacian operator on the adjacency matrix A, is $L = I - \frac{1}{\Delta}A$, and $\lambda_i = 1 - \frac{1}{\Delta}\sigma_{n-i}$ for $0 \leq i \leq n-1$. I is the identity matrix.

The graph G is $vulnerable$ [13] if

$$\frac{\beta}{\alpha} < \frac{1}{\overline{\lambda}^2} - 1 \tag{8}$$

where

$$\overline{\lambda} = max_{i \neq 0} \parallel 1 - \lambda_i \parallel \tag{9}$$

and λ_i are the Laplacian eigenvalues of the graph G.

Equation 8 determines if a proxy network is unable to recover from a DoS attack, i.e. the attacker is able to gain knowledge of an application's IP address. When the defense speed, i.e. proxy migration rate β, is less than the right hand side of 8 times the attack speed, i.e. host compromize rate α, then the proxy network is unable to effectively hide an application's IP address from an attacker. Both σ_1 and $\overline{\lambda}$ characterize the rate at which attackers can traverse through the overlay network.

Using (7), the Midihex topology is $robust$ for the values of $\alpha < \frac{1}{7}$, α represents the rate at which the hosts can be comprised. The Midihex topology, after a reconfiguration detailed in Section 5, is not $vulnerable$ to DoS attacks, as defined by (8). Tables 1, 2, and 3 show that the Midihex topology is less $vulnerable$ to attacks than the Chord network topology and is closest to the properties of the CAN topology. The degree 8 Midihex circulant graph, for cases which $n > 637$, is less $vulnerable$ than any other $degree$ 8 circulant graphs that are composed of a jump sequence that is a direct function of its $diameter$. The graph $order$ of $n > 637$ is noted, because it is the graph $order$ at which the Midihex topology becomes less $vulnerable$ to DoS attack than all other known 8 $degree$ circulant graphs that are composed of a jump sequence that is a direct function of its $diameter$.

N	$diameter$	σ_1	$\frac{1}{\overline{\lambda}^2} - 1$
128	4	15	1.086
256	4	15	0.859
512	5	17	0.710
1024	5	19	0.604
2048	6	21	0.526

Table 1. Topological Properties of Chord [13]

N	$diameter$	σ_1	$\frac{1}{\overline{\lambda}^2} - 1$
128	7	8	≈0
256	8	8	≈0
512	10	8	≈0
1024	12	8	≈0
2048	14	8	≈0

Table 2. Topological Properties of CAN [13]

N	$diameter$	σ_1	$\frac{1}{\overline{\lambda}^2} - 1$
185	5	8	0.5799
305	6	8	0.3949
637	8	8	0.2366
1521	11	8	0.1252
1953	12	8	0.0960

Table 3. Topological Properties of Midihex Topology

The attacker's capability, represent by α, affects the rate at which a given host can be $compromised$. During the operation of the proxy network the attacker's capability may vary. Up to this point in our analysis of a proxy network's $vulnerability$ to DoS attacks, the proxy network topology remained unchanged, only the virtual IDs to physical machines/hosts were reconfigured. The network topologies, i.e., interconnections of the virtual IDs, must remain static throughout the runtime of the proxy network. Previous proxy network reconfigurations, represented by the probability β, were restricted to dynamic mappings of a virtual ID of the proxy network to a physical host. The next section presents a method that dynamically alters the topology, of virtual IDs, of the proxy network in response to DoS attacks.

5 Reconfiguration of Circulant Topologies in Response to DoS Attacks

This section presents a means to decrease the $vulnerability$ to DoS attack, although a tradeoff is a decrease in performance. The decrease in performance is due to the increase in the graph $diameter$, which causes in increase an transmission delay, i.e. message latency, as a result of additional hops through the network.

In previous works the authors implemented a deadlock free reconfiguration algorithm for the reconfiguration of any proxy network topology [32], and a dynamic network reconfiguration algorithm for any arbitrary topology [12]. In this work, the algorithm presented modifies a given circulant topology and creates a set of circulant topologies with a decreasing $vulnerability$ of DoS attack, and an increasing $diameter$.

The presented method for proxy network reconfiguration is limited to use by circulant graphs. For the special case of circulant graphs, the eigenvalues of their adjacency matrix can be calculated in polynomial time. Also, because the adjacency matrix and Laplacian of an adjacency matrix is Hermitian, i.e., its symetric elements are conjugate, all the eigenvalues of the matrix are real. The eigenvalues of any circulant graph's adjacency matrix, or the Laplacian of the adjacency matrix, can be calculated using only the first row of the adjacency matrix.

In the next subsection a polynomial time algorithm for the determination of a circulant proxy network's $vulnerability$ to DoS attacks is presented. Subsection 5.2 details an algorithm that modifies the Midihex topology and creates a generic circulant graph, which exhibits a decrease in $vulnerability$ to DoS attack.

5.1 Polynomial Time Calculation of the $Vulnerability$ of Circulant Graphs to DoS Attacks

The $vulnerability$ of any circulant graph proxy network topology, with the eigenvalues of the Laplacian of an adjacency matrix as a parameter, is calculated in (8) and (9). All the proceeding steps are toward the calculation of the eigenvalues, λ, of the Laplacian of an adjacency matrix of a Circulant graph in polynomial time. A polynomial time computation of the eigenvalues of the Laplacian of a Circulant graph's adjacency matrix, of size $n \times n$, via linear algebra and the n^{th} roots of unity, is partially detailed in [30], and a detailed explaination follows:

The n^{th} roots of unity, with $z = e^{i\theta}$, are

$$z^n = 1 \tag{10}$$

The n^{th} roots of unity are approximated via sine and cosine tables. The exact roots of unity are not determined, but the level of accuracy provided by sine and cosine table are acceptable for our application.

The roots of unity are approximated below in the set w=w_0,w_1,...,w_{N-1}, this set is of $order\ N$,

$$w_n = \cos\left(n\frac{2\pi}{N}\right) + \sin\left(n\frac{2\pi}{N}\right)i \tag{11}$$

where w_n is an approximation to the n^{th} root of unity.

The eigenvalues, λ, and eigenvectors, x, of matrix C, in this case C is the Laplacian of an adjacency matrix of a Circulant graph, are defined as follows:

$$Cx = \lambda x \tag{12}$$

Any $n \times n$ adjacency matrix of a Circulant graph can be represented by the polynomial q with a degree $n-1$, and evaluated for $q(t)$ [31]. The coefficients of the polynomial q are $a_{1,2,..,n}$, and are assigned to the first row of any given matrix that represents the Laplacian of an adjacency matrix of a Circulant graph., e.g. (13)

$$q(t) = a_1 + a_2 t + a_{...} t^{\cdots} + a_n t^{n-1} \tag{13}$$

where the set of values $\{a_1, a_2, a_{...}, a_n\}$ compose the first row of C, therefore only one row of the circulant matrix C is required to calculate the eigenvalues for any given $n \times n$ circulant matrix.

The eigenvalues of the matrix $q(C)$ are $q(\lambda)$ [30], and are defined below,

$$q(C)x = q(\lambda)x \tag{14}$$

The series of equations (15), calculates the eigenvalues of a circulant matrix, the values of $q(w)$ are the eigenvalues of a

corresponding $n \times n$ circulant matrix C,

$$\begin{aligned} q(w_1) &= a_1 + a_2 w_1 + a_{...} w_1^{...} + a_n w_1^{n-1} \\ q(w_2) &= a_1 + a_2 w_2 + a_{...} w_2^{...} + a_n w_2^{n-1} \\ q(w_{...}) &= a_1 + a_2 w_{...} + a_{...} w_{...}^{...} + a_n w_{...}^{n-1} \\ q(w_n) &= a_1 + a_2 w_n + a_{...} w_n^{...} + a_n w_n^{n-1} \end{aligned} \quad (15)$$

where w_i is given as the i^{th} roots of unity in (11), for $1 \leq i \leq n$, and $\{a_1, a_2, a_{...}, a_n\}$ compose the first row of the $n \times n$ circulant matrix C.

The ordered eigenvalues $\lambda_1 \leq \lambda_2 \leq ... \leq \lambda_n$ are within the unordered set $\{q(w_1), q(w_2), q(w_{...}), q(w_n)\}$ (15). λ_2 is always equal to λ_i of (9), and is used to determine $\overline{\lambda}$ in (8). Using only the value λ_2 the $vulnerability$ of the proxy network is calculated via (8) and (9).

5.2 Algorithm to Decrease the Midihex Proxy Network's $Vulnerability$ to DoS Attacks

In order to decrease a graph's $vulnerability$ to a DoS attack, the graph's $diameter$ must increase [17]. The jump sequences (j_1, j_2, j_3, j_4) of a circulant graph are defined as $C_n \pm (j_1, j_2, j_3, j_4)$. The Midihex topology jump sequences are defined as $G = C_n \pm (1, 3k+1, 3k+2, 3k^2+3k+1)$ in Theorem 3.1. A simple method to increase the graph $diameter$ of the Midihex topology is to converge the fourth jump, j_4, toward the third jump, j_3, by an increment of 1, i.e., $C_n \pm (j_1, j_2, j_3, j_4 - 1)$. The Midihex topology is altered and is now classified as only a circulant graph. The fourth jump sequence is decremented one step, the result is a possible increase in the circulant graph's $diameter$ and a decrease in its $vulnerability$ to DoS attack.

The second and fifth columns, respectively, of Table 4 demonstrate the possible increase in the graph $diameter$, and a definite decrease in $vulnerability$ when the fourth jump sequence, j_4, is decremented by a value of t, third column. The pseudo code for the reconfiguration algorithm is given in Fig. 5.

N	$diameter$	t	σ_1	$\frac{1}{\overline{\lambda}^2} - 1$
637	8	0	8	0.2366
637	8	1	8	0.2314
637	9	2	8	0.1598
637	9	3	8	0.1576
637	10	10	8	0.0776

Table 4. Topological Properties of Circulant Graphs that are slight variations of the Midihex Topology.

Subsection 5.1 detailed a polynomial time algorithm for the calculation of eigenvalues, of the Laplacian of a circulant graph's adjacency matrix of size $n \times n$. The iterative algorithm, presented in this subsection, takes as an input the proxy network topology and a parameter that represents the attacker's capability, α, and determines the $vulnerability$ of the proxy network topology. The algorithm iterates until an acceptable $vulnerability$ is achieved. The pseudo code for the reconfiguration algorithm is given in Fig. 5.

Reconfiguration Algorithm

INPUT: acceptable_vulnerability

attacker's capability α

graph adjacency matrix $C_n \pm (j_1, j_2, j_3, j_4)$

OUTPUT: graph adjacency matrix

1 DO

2 $C_n \pm (j_1, j_2, j_3, j_4) = C_n \pm (j_1, j_2, j_3, j_4 - 1)$

3 vulnerability = calculate_vulnerability(attacker's capability α, graph adjacency matrix $C_n \pm (j_1, j_2, j_3, j_4)$)

4 WHILE (vulnerability $>$ acceptable_vulnerability) AND $(j_4 \neq j_3 + 1)$

5 Reconfigure Proxy network to: $C_n \pm (j_1, j_2, j_3, j_4)$

Figure 5. Circulant proxy network reconfiguration algorithm.

6 Conclusion

A Midihex proxy-network topology is proposed for use in proxy networks because of its ability to resist DoS attacks. The Midihex topology is less $vulnerable$ to attacks than the Chord topology, and is closest to the properties of the CAN topology [14]. Unlike the CAN topology, the n node Midihex topology exhibits $maximum\ connectivity$ for all values of $n \geq 21$, Theorem 3.1. In the event of a DoS attack, through the use of the proposed reconfiguration algorithm, the $vulnerability$ of the Midihex topology can be further decreased. The novel Midihex circulant graph proxy network topology exhibits $maximum\ connectivity$, and after a reconfiguration detailed in Section 5, is not $vulnerable$ to DoS attacks.

References

[1] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, and H. Balakrishnan, "Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications," *SIGCOMM'01*, Aug. 2001.

[2] B.Y. Zhao, L. Huang, J. Stribling, S.C. Rhea, A.D. Joseph and J.D. Kubiatowicz, "Tapestry: A Resilient Global-scale Overlay for Service Deployment," *IEEE J. on Selected Areas in Communications*, 2003.

[3] A. Rowstron and P. Druschel, "Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems," *Proc. of the 18th IFIP/ACM Int'l Conf. on Distributed Systems Platforms (Middleware 2001)*, 2001.

[4] D. Andersen, H. Balakrishnan, M.F. Kaashoek, and R. Morris, "Resilient Overlay Networks," *18th ACM Symp. on Operating System Principles (SOSP)*, Oct. 2001.

[5] S. Dutt and J.P. Hayes, "On Desiging and Reconfiguring k-Fault Tolerant Tree Architectures," *IEEE Trans. on Computers*, vol. 39, no. 4, pp. 490-503, 1990.

[6] S. Dutt and J.P. Hayes, "Designing Fault-Tolerant Systems Using Automorphisms," *J. of Parallel and Distributed Computing*, Vol. 12, No.3, pp. 249-268, 1991.

[7] S. Dutt and J.P. Hayes, "Some Practical Issues in the Design of Fault-Tolerant Multiprocessors," *IEEE Trans. on Computers*, vol. 41, no.5, pp. 588-598, May 1992.

[8] F.T. Boesch and A. P. Felzer, "A General Class of Invulnerable Graphs," *Networks*, vol. 2, pp. 261-283, 1972.

[9] F.T. Boesch and R. Tindell, "Circulants and their Connectivities," *IEEE J. of Graph Theory*, vol. 8, pp. 487-499, 1984.

[10] F.T. Boesch and J. F. Wang, "Reliable Circulant Networks with Minimum Transmission Delay," *IEEE Trans. on Circuits and Systems*, CAS-32(12), pp. 1286-1291, 1985.

[11] D. Avresky and Y. Varoglu, "Survivable Computer Networks in the Presence of Multiple Faults," *IEEE Int. Workshop on Embedded Fault-Tolerant Systems (EFTS-2000)*, 2000, pp. 747-751.

[12] D.R. Avresky and N. Natchev, "Dynamic Reconfiguration in Computer Clusters with Irregular Topologies in the Presence of Multiple Node and Link Failures," *IEEE Trans. on Computers*, vol. 54, no. 5, pp. 603-615, 2005.

[13] J. Wang, L. Lu, and A. A. Chien. "Tolerating Denial-of-Service Attacks using Overlay Networks - Impact of Overlay Network Topology," *Proc. First ACM Workshop on Survivable and Self-Regenerative Systems*, 2003.

[14] S. Ratnasamy, P. Francis, M. Handley, R. Karp and S. Shenker "A Scalable Content-Addressable Network," *ACM SIGCOMM'01*, 2001.

[15] D. West *Introduction to Graph Theory.*, Sec. ed. Upper Saddle River, NJ.: Prentice Hall, pp. 150, 161-172, 461-463, 2001.

[16] F. Harary "The Maximum Connectivity of a Graph," *Proc. Nat. Acad. Sci. U.S.A. 48*, pp. 1142-1146, 1962.

[17] J. Wang, A. A. Chien. "Using Overlay Networks to Resist Denial-of-Service Attacks," Univ. of San Diego, California, Tech. Rep., 2003.

[18] C. Labovitz, R. Malan, and F. Jahanian. "Internet Routing Instability," *IEEE/ACM Trans. on Networking*, vol. 6, no. 5, pp. 515-528, Oct. 1998.

[19] H. Whitney "Congruent graphs and the connectivity of graphs," *American Journal of Math*, vol. 54, pp. 150-168, 1932.

[20] K. Menger "Zur allgemeinen Kurventheorie," *Fundamenta Mathematicae*, vol. 10, pp. 96-115, 1927.

[21] F. Boesch and J. Wang. "Reliable Circulant Networks With Minimum Transmission Delay," *IEEE/ACM Trans. on Networking*, vol. 32, no. 12, pp. 1286-1291, December 1985.

[22] R. Beivide, E. Herrada, J.L. Balczar and A. Arruabarrena. "Optimal Distance Networks of Low Degree for Parallel Computers," *IEEE Trans. on Computers*, vol. C-40, no. 10, pp. 1109-1124, 1991.

[23] C.K. Wong and D. Coppersmith. "A Combinatorial Problem Related to Multimode Memory Organizations," *J. Assoc. Comp. Mach.*, vol. 21, pp. 392-402, 1974.

[24] J.F. Wang and C.S. Yang. "On the Number of Spanning Trees in Circulant Graphs," *Int'l J. of Computer Mathematics*, vol. 16, pp. 1286-1291, 229-241, 1984.

[25] J. Xu *Topological Structure of Analysis of Interconnection Networks.*, Norwell, MA: Kluwer Academic Publishers, pp. 25,53-56,161, 2001.

[26] K. Efe, "A variation on the hypercube with lower diameter," *IEEE Trans. on Computers*, vol. 40, no. 11, pp. 1312-1316, 1991.

[27] A. D. Keromytis, V. Misra, and D. Rubenstein, "Sos: Secure overlay services," *ACM SIGCOMM'02*, 2002.

[28] I. Stoica, D. Adkins, S. Zhuang, S. Shenker, and S. Surana, "Internet indirection infrastructure," *ACM SIGCOMM'02*, 2002.

[29] T.C. Lee and J.P. Hayes, "Design of Gracefully Degradable Hypercube-Connected Systems," *J. of Parallel and Distributed Computing*, vol. 14, no. 4, pp. 390-401, 1992.

[30] D. Kalman and J.E. White, "Polynomial equations and circulant matrices," *American Math Monthly*, Nov. 2001. [Online]. Available: http://www.american.edu/academic.depts /cas/mathstat/People/kalman/pdffiles/circulant.pdf

[31] D. Frank, "Circulant Matrices and Polynomials," [Online]. Available: http://online.redwoods.cc.ca.us/instruct/darnold/laproj /Fall2002/dfrank/paper.pdf

[32] Stephen Frechette and D.R Avresky, "Method for Task Migration in Grid Environments," *4th IEEE Int'l Symp. on Network Computing and Applications (NCA05)*, 2005, pp. 49-56.

[33] C. Labovitz, A. Ahuja, and F. Jahanian, "Experimental Study of Internet Stability and Wide-Area Backbone Failures," University of Michigan, MI, Tech. Rep. CSE-TR-382-98, 1998.

[34] C.L.A Yebra, M.A. Fiol, P. Morillo, and I. Alegre, "The Diameter of Undirected Graphs associated to Plane Tessellations," *Ars Combin*, vol. 20B, pp. 159-171, 1985.

[35] C.K. Wong and D.A. Coppersmith, "Combinatorial Problem Related to Multimode Memory Organizations," *J. Assoc. Comp. Mach.*, vol. 21, pp. 392-402, 1974.