ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Combined Transfer Routing and Circulation of Protection Services in Elevated Rapidity Networks

Bathala Subbarayudu
Assistant Professor,
Department of IT,
St Martin's Engineering College,
Hyderabad.

Dr. R.China Appala Naidu
Professor,
Department of CSE,
St Martin's Engineering College,
Hyderabad.

ABSTRACT:

The persistent detonation of new disease/caterpillar and other protection attacks in the Internet and the remarkable transmission rapidity of self-propagating attacks have lead to network protection being measured as a design measure rather than an addendum. Attack impediment, recognition, and easing mechanisms can be mostly classier as network based or host based. Network based Protection mechanisms have been shown to be much more valuable than host based mechanisms, mainly because of the former's ability in identifying attack traffic that is further upstream from the fatality and closer to the attack source.

In the context of network based mechanisms, we consider an edible overlay network of Protection systems running on top of programmable routers. Such as network based mechanisms inevitably decrease network performance as all packets are analyzed for malicious content before being forwarded. In this paper, we consider traffic routing, placement of active router nodes, and distribution of Protection services across such nodes so as to optimize certain objectives, including. The very high-speed Backbone Network Service (vBNS) came on line in April 1995 as part of a National Science Foundation (NSF) sponsored project to provide high-speed interconnection between NSF-sponsored supercomputing centers and select access points in the United States.

Keywords:

Traffic Engineering (TE), Security, Detection, Joint Optimization, High Speed Networks.

I. INTRODUCTION:

In earthquakes, although most of the human losses derive from damage to urban housing, the economic impact can instead arise from damage to critical transportation such as transport, energy and other utilities and the secondary effects of trouble to their functionality. Additionally, considerable interdependencies can exist between infrastructure systems in an urban area, meaning that damage to one system may result in disruption to other critical infrastructure. The financial industry requires better accepting of infrastructure behavior under seismic shocks in order to establish the right economic tackle for their supervision. The estimation of financial risk due to earthquakes recent developments show that communication networks cannot be secured by sporadic and ungraceful security devices like recalls at users and cooperates sites. Moreover, it cannot be expected that all users and administrators will be able to keep their structure sheltered and thus, we think that the protection of end systems should be done in the network.

We propose an edible overlay network of intrusion prevention systems (IPS) running on top of an active networking environment. Active networks consist of programmable nodes (active nodes) on which, for example, IPS services can be dynamically deployed for the purpose of creating overlay networks. In this paper, we remove respective assumptions in two previous approaches moreover the routes are given or position of security nodes is given and provide a framework for joint optimization of both design choices. We envisage that the contribution of this paper can be applied in a network planning setting where estimated traffic patterns can be used to deploy security services at selected nodes and provision paths for load-balanced routing in the network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We develop two mixed integer linear programming (MILP) formulations that assign the routes and simultaneously place programmable router nodes and distribute security ser-vices across these nodes so as to (i) minimize the number of nodes where programmable routers are deployed, or (ii) minimize the maximum utilization of any router node in the network. Any other linear objective function can also be accommodated. In the rest approach, the MILP calculates the optimal single path route for each source-destination pair in the network. In the second approach, the set of available routes for each source-destination pair is preened and multipath routing is allowed. Critical infrastructure networks are commonly referred to within the earthquake engineering and civil protection fields as lifelines, reflecting their role as lifelines to recovery.

2. LITERATURE REVIEW:

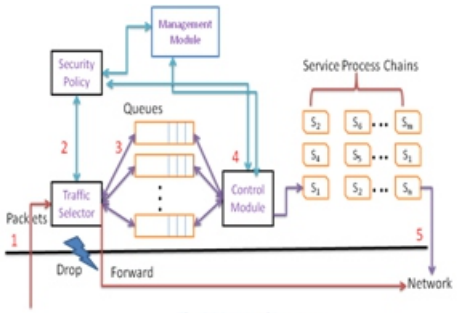
The literature review on lifeline response to seismic shocks has been broadly being divided into four categories: estimation of the damage to infrastructure components; estimation of infrastructure system performance; estimation of the economic losses associated with the response; and decision support methodologies for prioritizing infrastructure investment. Loss estimation, both direct and indirect (e.g. business interruption), is the primary focus of the financial industry in relation to lifeline response, whilst investment in infrastructure is important to improve its resilience and in doing so attempt to minimize potential economic losses and reduce premiums. The literature review is an evolving process but the following sections report on the progress thus far.

2.1 Network Reliability:

Methodologies for predicting network reliability fall into two categories: simulation-based models and analytical simulation based models involve the use of random sampling techniques and Monte Carlo simulation to approximate system functionality following an earthquake. When such methods are used, a metric for functionality is needed. Metrics used in the literature include availability and serviceability and fragility, quality, robustness and resilience. In these examples, availability is defined as the ratio of available pressure to required pressure in a water system; serviceability is the ratio of available flow to required flow in a water system; fragility is the percentage of outages relative to number of customers per area for an electricity network; robustness is ratio of post-event capacity to normal capacity for an electricity network and resilience is the integral of quality over time.

2.2. The FIDRAN Architecture:

This section briefly describes the FIDRAN architecture, for a detailed discussion we refer to the framework consists of core components which run permanently and of add-on gears the security services which are dynamically integrated into the system as needed. The core functionality comprises the traffic selector, the security policy, the control/management module and the default queuing discipline. Security services are implemented as loadable modules featuring IPS specific networking services. The capabilities provided by the underlying programmable networking infrastructure allow distributing the FIDRAN system on pro.



The FIDRAN Architecture

Gramm able routers. The dynamic creation of an IPS overlay network is thereby enabled. Secure communication between programmable nodes is also provided. All network traffic is redirected to the traffic selector, which according to the rules specified in the security policy assigns the traffic to one of the categories: forward, process or drop. Traffic that is assigned to the category forward is directly forwarded and not analyzed by any installed security service. It is either not necessary to check this traffic or another programmable node on the route to the end-system is in charge of doing so. Traffic in the category process is queued and analyzed by specific security services. The detailed proceeding for queuing and analysis as well as the reaction in case of a detected attack is also specified in the security policy. Finally, traffic belonging to the category drop is blocked altogether by the traffic selector. The management and the control modules are responsible for the configuration of the FIDRAN system. The management module is the interface between the overlay network of programmable routers and the FIDRAN system.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Hence, it is able to trigger the download of a security service from a service repository.

2.3 EMULATION:

The performance of FIDRAN was assessed on the Cyber Defense Technology Experimental Research tested which is a shared infrastructure designed for medium scale repeatable experiments in computer security. The tested provides a pool of over 300 computers of varying hardware which can be used to emulate networks. As scenario we chose the Abilene network depicted. For this network real world data traffic flows and link capacities is available on the project's web-site describes in detail the FIDRAN prototype implemented which includes a set of security services and which was used during the experiments. S2.

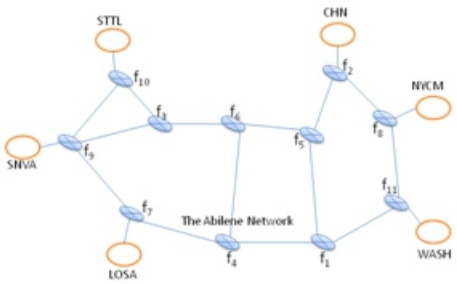


Table I represents the traffic matrix, the column index specifies the source and the row index the destination. Measurements of local-area and wide-area network traffic have shown that packet-switched data traffic is self-similar. Glen Kramer implemented a tool to synthetically generate self-similar network traffic traces by the superposition of a large number of 0/1 renewal processes whose ON and OFF periods are heavy tailed distributed. Finally, to avoid effects of congestion and flow control mechanisms all experiments were restricted to UDP-traffic. To consider the hardware resources provided by the DETER tested, the network was emulated on a scale of 1 : 100 which means that traffic rates were divided by 100 and accordingly the delays were multiplied by 100.

2.4 The Abilene Network:

In the network each subnet sends data to all other subnets resulting in an overall number of 30 traffic flows. The broadcast delay for each link was specified by dividing the distance from start node to end node by the speed of light.

Table I represents the traffic matrix, the column index specifies the source and the row index the destination. To generate the traffic each subnet is supplied with an UDP sender for each destination which generates self-similar traffic as described above. Each experiment lasted 1800s and contained the sending of over 7, 500,000 packets.

To -->	CHIN	LOSA	NYCM	SNVA	STTL	WASH
CHIN	X	35.53	6.77	3.75	8.37	14.77
LOSA	113.58	X	51.50	10.30	26.26	58.90
NYCM	71.82	64.68	X	1.44	31.91	108.35
SVNA	5.68	34.09	3.29	X	55.06	2.13
STTL	66.26	27.79	21.84	9.02	X	15.63
WASH	93.45	75.20	176.86	8.22	36.30	X

Table I: The Abilene Traffic Matrix [Mbps]

Each traffic flow must be analyzed by three security services, whereby the service processing times Ts were scaled as mentioned. We study the performance of the solutions obtained for both presented MILPs (single-path routing and multipath routing) with the objective of minimizing the maximum router utilization, and compare them to the solutions of the MILPs presented in extended to generalized topologies.

3. TRAFFIC MODELING:

The COST Action 253 is aiming to study high speed terrestrial (based on ATM technology) networks interconnected by non-GEO satellite constellations. The performance of these networks depends very much on the successful characterization and estimation of offered services and traffic loading, as well as on efficient management techniques for the integrated, terrestrial and space system.

3.1 Service Categories and Requirements:

The applications foreseen for LEO constellations interconnecting ATM networks can be different as:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

private voice-data lines, public voice-data lines, environment monitoring, broadcasting, messaging, remote control, Internet services, videoconferencing, file transfer, tale education etc. These services can be classified in two broad categories depending on the time constraints they can sustain.

a)Real time applications which can be modeled as CBR, VBR

b) Non-real time applications which can be modeled as UBR, VBR, ABR

1: The Constant Bit Rate (CBR) Service Category is used for connections that request a static amount of bandwidth continuously available during the connection. It is adequate for voice, video, and audio and is characterized by the Peak Cell Rate (PCR).

2: The Variable Bit Rate (VBR) Service is used for connecting sources alternating between active and silent periods or varying in bit rate continuously. Various parameters must be defined for the success of this service, like Peak Cell Rate (PCR), Sustainable Cell Rate (SCR), and Intrinsic Burst Tolerance (IBT). The service can be used for voice, video, data, audio etc.

The QoS parameters associated with every service category are given in Table.2: as they are recommended by ITU-T. 356 (U means unbounded).

	CTD	CDV	CLR
Default	No	No	No
Class1	400 msec	3 msec	3.10^{-7}
Class2	U	U	10^{-5}
	CER	CMR	SECBR
Dfault	4.10^{-7}	1/day	10^{-4}
Class1	Default	Default	Default
Class2	Default	Default	default

3.2 Source Modeling:

The activity of a source is a stochastic process that is a family of random variables which are functions of time. The classic way to characterize a source activity is by using a closed form probability distribution.

Markovian models:

Even for special cases the analytic solution is computationally intensive thus improving the computational complexity in such systems is a topic of active research. The well known model MMPP model: It is a multi-state process and has been widely used to characterize different types of traffic such as voice, video, and images. A Markov-modulated source is governed by an underlying continuous Markov chain, with state space S, which determines the current state of the source.

3.3 Aggregate Network Traffic Modeling:

Self Similar models: Recent analysis of real traffic traces clearly shows that Internet traffic exhibits self-similarity features. Precisely, let be the number of packets arriving in interval n and form the aggregated process consisting of the sample mean of non-overlapping intervals. The measured process is self-similar since is equal to in distributional sense. Therefore, the process looks like a fractal: no matter the time scale that we consider the distribution remains invariant. On the other hand, we note that the burrstones of the packet arrival process also remains invariant with increasing time scale, thus severely affecting network performance.

3.4 Gateway and on-board traffic modeling.:

The entire well known queuing models can be used for an approximated study of the on-board switch. The MMF model is considered to be very adequate for modeling the traffic of an on-board switch. The Gateway is essentially a multiplexer. Some models have been proposed in the literature to determine the loss probability at an ATM multiplexer. [9] Models are based on the assumption of MM arrival processes but the loss probability is computationally intensive and impractical, especially when the state space of the aggregate arrival process is large. This is the case of ATM networks where we expect to have a large number of sources.

3.5 Geographic Traffic Models:

They characterize the spatial and temporal distribution of the traffic intensity. Since satellite network planning concerns cells of very big coverage it is impossible to model subscribers separately.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Also, the movement of subscribers for LEO systems can be neglected in Comparison to the speed of satellite beams. Thus, to analyze the network load in global mobile satellite systems, a global geographic traffic model is needed to estimate the traffic as a function of various demographic and cultural data (population, income, mobiles penetration.

4. PERFORMANCE EVALUATION:

In this section, we present the evaluation of our algorithm NPCC, which is proposed for providing a reliable IPTV service. Our method guarantees the recovery from link and node failure at the DWDM layer with a fast restoration time. We compare our algorithm with the ESHN algorithm, which was reported to be the most efficient algorithm for dynamic multicast traffic protection in terms of resource utilization efficiency and blocking probability.In our simulation, we assumed that request arrival follows a Poisson process with an average arrival rate λ, and the request holding time follows an exponential distribution with an average holding time μ. Hence, the offered traffic load for the network is given by λμ.The COST-266 core topology contains 16 nodes and 23 links, with an average nodal degree of 2.88. The total number of p -cycles in this topology is 236 (118 p -cycles in each direction).

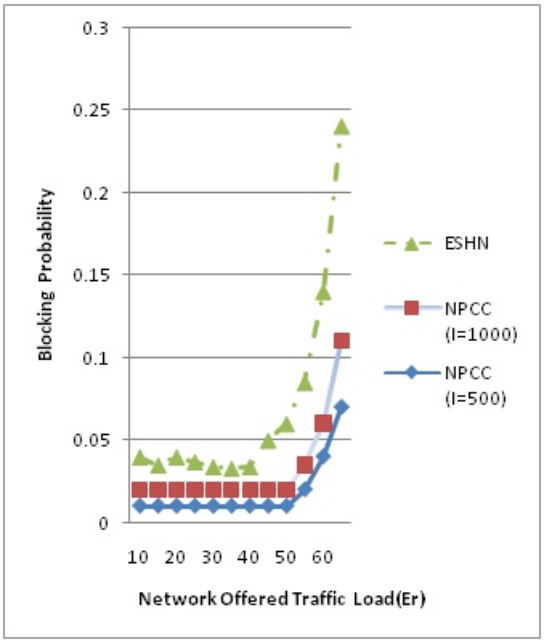


Fig 1: Comparison of the blocking probabilities BP for the COST – 239 networks

The COST-239 topology [12] contains 11 nodes and 26 links, with an average nodal degree of 4.727. The total number of p -cycles in this topology is 5,058 (2,029 p -cycles in each direction).In our study, without loss of generality, we assumed that each link has two fibers. The two fibers transmit in opposite directions; 16 wavelengths are available on each fiber. The source and the destinations of each multicast session are randomly selected (uniform distribution law). We chose the number of destinations in each multicast request D = 5, which seems to be reasonable as the total number of nodes in the used topologies is less than 16. We compared the performance of the algorithms using the following performance criteria: The blocking probability (BP), which is the percentage of requests that cannot be routed or protected among the total number of requests.The resource utilization (RU), which is the percentage of reserved wavelengths in the network among the total number of wavelength links.

$$RU = WR / E \times W$$

Where WR is the total number of wavelength links reserved in the network, E is the number of fibers in the network and W the number of wavelengths per fiber.• The average computation time (CT), which is required for routing and protecting a traffic request. Performance criteria BP, RU and CT were computed according to the traffic load. For each traffic load value, 5×105 requests were generated. This number of requests is enough to measure BP, RU and CT with a 95% confidence interval.

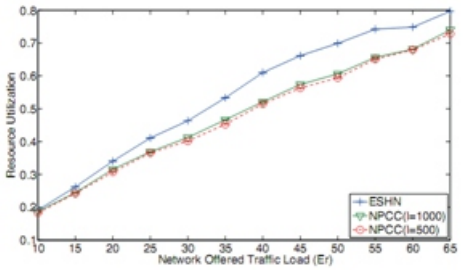
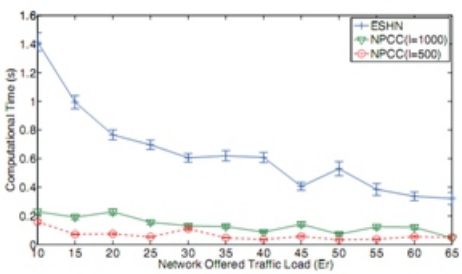


Figure 3 Comparison of resource utilization RU for the COST-239 Network.



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Figure 4 Comparison of the average computation time CT for Setting up a multicast request using the COST-239 Network.

First, we considered the COST-239 topology. The total number of p-cycles in this topology is 5,085. We ran the NPCC algorithm with two different values for the number of candidate p-cycles, l = 1000 and l = 500. The blocking probability measured for the COST-239 network is shown in Figure 9. For all the algorithms, the blocking probability increased when the traffic load was high. The NPCC algorithm, with both l = 1000 and l = 500, outperformed the ESHN algorithm having a lower blocking probability, especially when the traffic load was high. The NPCC algorithm with l = 1000 had the lowest blocking probability. When l = 500, the blocking probability of NPCC increased but remained lower than that of ESHN. This is because l = 500 is very low compared to the total number of p-cycles in the COST-239 network (5,058).Figure 3 shows the resource utilization of the algorithms. When the traffic load increases, the wavelength percentage reserved per link is higher for each algorithm.

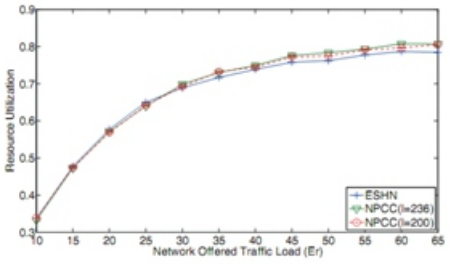


Figure 5 Comparison of resource utilization RU for the COST-266 Network.

Now, we consider the COST-266 topology. The total number of p-cycles in this topology is 236. We ran the NPCC algorithm with two different values for the number of candidate p-cycles, l = 236 and l = 200. Figure 4 shows the blocking probabilities for the COST-266 network.The connectivity of this topology is very low (2.88). Therefore the blocking probabilities of the algorithms are very high compared with those for the COST-239 topology for the same network traffic load. For all the algorithms, the blocking probability increased rapidly as the traffic load increased. The ESHN algorithm has a higher blocking probability than the NPCC algorithm with l = 236 or the NPCC algorithm with l = 200. The blocking probability of NPCC with l = 236 and the blocking probability of NPCC with l = 200 were very close since the values of l were close.

Figure 5 shows the resource utilization of the algorithms for the COST-266 topology. The wavelength percentage reserved by the algorithms was almost the same. The percentage of reserved wavelengths per link increased as the traffic load increased. Note that the resource utilization of the ESHN algorithm was slightly lower than that of our algorithm NPCC when the traffic load was higher than 35 eland. This is because the blocking probability was high. In other words, the probability of rejecting requests for ESHN increased and no resource had been reserved for the rejected requests. This reduced the resource utilization of ESHN.

5. CONCLUSION:

Providing security to communication networks requires that packets be inspected for malicious contents and, consequently, impacts normal network operation. In this paper we presented an optimization outline for joint traffic routing and service placement, which can be used to study that impact, while fulfilling a pre-defined objective. Here, we presented objective function that minimizes the amount of security-enabled routers or the maximum router load.

Using a scenario based on a real network we showed that the routing and deployment strategies obtained as solution to the problems formulated balance the network load and significantly reduce the overall dropping rate. We extended the concept of node protection using p-cycles to deal with multicast traffic. Our novel concept allows the protection capacity provided by a p-cycle to be used efficiently.

For the scenario under consideration, we also showed that the joint optimization of single path routing and service placement is a big improvement with respect to optimal service placement over routes calculated with the FIDREN Architecture, since the latter does not take the additional router load due to security processing into account. Reduces the computation time for setting up a multicast traffic request by enumerating a set of candidate p-cycles based on the PC score Good solutions were obtained for both presented strategies.

The single-path strategy tends to generate long paths to disburden heavy loaded routers. In contrast, the multi-path strategy splits huge flow into smaller ones and re-routes these over different paths. Both solutions show that they balance the load well.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

REFERENCES:

1.The Abilene Network. http://abilene.internet2.edu.

2.Glen Kramer. Synthetic traffic generation. http://www-csif.cs.ucdavis.edu/kramer/research.html.

3.Cyber Defense Technology Experimental Research. The deter testbed:

4.Overview. http://www.isi.edu/deter/docs/testbed.overview.htm, Oct. 2004.

5.A. Hess, S. Sengupta, V. P. Kumar, Joint traffic routing and distribution of security services in high speed networks, in: Proc. INFOCOM 2008, 2008, 2279-2287

6. M. Alicherry, M. Muthuprasanna, V. Kumar, High speed pattern matching for network IDS/IPS, IEEE Computer Society, 2006, 187-196.

7.D. Awduche, MPLS and traffic engineering in IP networks, IEEE Communications Magazine, Vol.37, No. 12, Dec. 1999, 42-47.

8.B. Fortz, M. Thorup, Optimizing OSPF/IS-IS weights in a changing world, IEEE JSAC, Vol. 20,No. 4, 2002, 756-767.

9.J. X. Chen, X. M.Wang, L. W. He, An architecture for differentiated security service, International Symposium on Electronic Commerce and Security, Aug. 2008, 301-304.

10.M. Ramesh Reddy, M.Tech, Distributed Detection of node replication attacks in DTNs, www.ijmetmr.com, Vol. 1, ISSUE No: 9, September 2014, 2348-4845.

11.J. Xu, B. Li, D. Lee, Placement problems for transparent data replication proxy services, IEEE JSAC, Vol. 20, No. 7, July 2002, 1383-1398.

12.Bhattacharyya S (2003) an overview of source-specific multicast (SSM).IETF RFC 3569.