Peer to Peer Reputation Management

Deepti Yadav[#1], Shraddha Tagde[#2], Deepa Kale[#3], Neha Ramteke[#4], Vishakha Borkar[#5]

Department of Computer Science & Engineering
G.H.Raisoni College of Engineering & Technology for Women,
Nagpur , Maharashtra, India.

deeptichetanyadav@gmail.com[#1]
shraddha.tagde17@gmail.com[#2]
deepa.04@hotmail.com[#3]
neha.ramteke1@gmail.com[#4]
vishakhaborkar7@gmail.com[#5]

***Abstract*- Every years, the Internet and, by extension, the web gets bigger and better, As the Internet takes an increasingly central role in our communications infrastructure, the slow convergence of routing protocols after a network failure becomes a growing problem. To assure fast recovery from link and node failures in IP networks, we present a new recovery method called Multiple Routing Configurations (MRC). Our propose method guarantees recovery in all single failure scenarios, using a single mechanism to handle both link and node failures, and without knowing the root cause of the failure. MRC is based on keeping additional routing information in the routers, and allows packet forwarding to continue on an alternative output link immediately after the detection of a failure. In this paper we present MRC, and analyze its performance with respect to scalability, backup path lengths. An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malwarer and/or disgruntled employees. IDS cannot directly detect attacks within properly encrypted traffic.**

***Keywords*— Availability, Peer-to-Peer Networks System, Reputation, Computer network reliability, Communication system fault tolerance, Communication system routing, protection.**

I. INTRODUCTION

The Internet is a globally distributed network , comprising many voluntarily interconnected autonomous networks. In networking the slow convergence of routing protocols after a network failure becomes a growing problem. The ability to recover from failures has always been a central design goal in the Internet. IP networks are intrinsically robust, since IGP routing protocols like OSPF are designed to update the forwarding information based on the changed topology after a failure. This re-convergence assumes full distribution of the new link state to all routers in the network domain. When the new state information is distributed, each router individually calculates new valid routing tables. This network-wide IP re-convergence is a time consuming process, and a link or node failure is typically followed by a period of routing instability. During this period, packets may be dropped due to invalid routes. Much effort has been devoted to optimizing the different steps of the convergence of IP routing, i.e., detection, dissemination of information and shortest path calculation, but the convergence time is still too large for applications with real time demands. A key problem is that since most network failures are short lived, too rapid triggering of the re-convergence process can cause route flapping and increased network instability. In this paper we present a new method for handling link and node failures in IP networks. Multiple Routing Configurations (MRC) is a proactive and local protection mechanism that allows recovery in the range of milliseconds. MRC allows packet forwarding to continue over preconfigured alternative next-hops immediately after the detection of the failure. Using MRC as a first line of defense against network failures, the normal IP convergence process can be put on hold. MRC guarantees recovery from any single link or node failure, which constitutes a large majority of the failures experienced in a network . MRC makes no assumptions with respect to the root cause of failure, e.g., whether the packet forwarding is disrupted due to a failed link or a failed router.

The goal of intrusion detection is to monitor network assets to detect anomalous behavior and misuse. This concept has been around for nearly twenty years but only recently has it seen a dramatic rise in popularity and incorporation into the overall information security infrastructure. In the last few years, the Intrusion Detection(ID) field has grown considerably and therefore a large number of Intrusion Detection Systems (IDS) have been developed to address specific needs The initial ID systems were once anomaly detection tools but today, misuse detection tools dominate the market. With an increasingly growing number of computer systems connected to networks, ID has become a necessity. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses.

An intrusion detection system is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding.

II. PROPOSED SYSTEM

We present a new scheme for handling link and node failures in IP networks. Multiple Routing Configurations (MRC) is a proactive and local protection mechanism that allows recovery in the range of milliseconds. MRC allows packet forwarding to continue over preconfigured alternative next-hops immediately after the detection of the failure. Recovery in all single failure scenarios without knowing root cause of the failure. Each and Every Node having Preconfigured Backup Path. That Backup path maintains the routing table. MRC assumes only destination of hop by hop forwarding.

III. GENERATING BACKUP CONFIGURATIONS FOR MRC

MRC configurations are defined by the network topology which is the same in all configurations, and the associated link weights, which differ among configurations. We formally represent the network topology as a graph G=(N,A), with a set of nodes N and a set of unidirectional links (arcs) .1 In order to guarantee single-fault tolerance, the topology graph G must be bi-connected. A configuration is defined by this topology graph and the associated link weight function. Multipath routing enables a network's traffic to be split among two or more possibly disjoint paths in order to reduce latency, improve throughput, and balance traffic loads. Yet, once the control plane establishes multiple routes, a policy is needed for efficiently splitting traffic among the selected paths. In this paper, we introduce opportunistic multipath scheduling technique for exploiting short term variations in path quality to minimize delay, while simultaneously ensuring that the splitting rules dictated by the routing protocol are satisfied. In particular, measured path conditions on time.

TABLE I
NOTATION

G=(N,A)	Graph comprising nodes N and directed links (arcs) A
C_i	The graph with links weights as in configuration i
S_i	The set of isolated nodes in configuration C_i
B_i	The backbone in configuration C_i
A(u)	The set of links from node u
(u,v)	The directed link from node u to node v
P_i (u,v)	A given shortest path between nodes u and v in C_i
N(p)	The nodes on path p
A(p)	The links on path p
W_i (u,v)	The weight of link (u,v) in configuration C_i
W_i (p)	The total weight of the links in path p in configuration C_i
Wr	The weight of a restricted link
n	The number of configurations to generate (algorithm input)

Description:

Algorithm 1 loops through all nodes in the topology, and tries to isolate them one at a time. A link is isolated in the same iteration as one of its attached nodes. The algorithm1 terminates when either all nodes and links in the network are isolated in exactly one configuration, or a node that cannot be isolated is encountered. We now specify the algorithm in detail, using the notation shown in Table I.

Algorithm1: Generating Backup Configurations For MRC

```
for i Є {1….n}do
    Ci←(G,wo)
    Si←ø
    Bi←Ci
end
Qn←N
Qa← ø
i←1
while Qn≠ ø do
      u←first(Qn)
      j←i
     repeat
          if connected(Bi\({u},A(u))) then
               Ctmp←isolate(Ci,u)
               if Ctmp≠null then
                    Ci←Ctmp
                    Si←Si U {u}
                    Bi←Bi\({u},A(u))
         i←(I mod n)+1
    until u Є Si or i=j
    if u≠Si then
         Give up and abort
end
```

a) Main loop:

Initially, n backup configurations are created as copies of the normal configuration. A queue of nodes (Qn) and a queue of links (Qa) are initiated. The node queue contains all nodes in an arbitrary sequence. The link queue is initially empty, but all links in the network will have to pass through it. Method first returns the first item in the queue, removing it from the queue.

When a node u is attempted isolated in a backup configuration Ci, it is first tested that doing so will not disconnect Bi according to definition .The connected method at line 13 decides this by testing that each of 's neighbors can reach each other without passing through , an isolated node, or an isolated link in configuration Ci .

If the connectivity test is positive, function isolate is called, which attempts to find a valid assignment of isolated and restricted links for node u as detailed below. If successful isolate, returns the modified configuration and the changes are committed .Otherwise no changes are made in Ci.

If u was successfully isolated, we move on to the next node. Otherwise, we keep trying to isolate u in every configuration, until all n configurations are tried. If u could not be isolated in any configuration, a complete set of valid configurations with cardinality n could not be built using our algorithm. The algorithm will then terminate with an unsuccessful result.

So all above discussion states that our propose method guarantees recovery in all single failure scenarios, MRC is based on keeping additional routing information in the routers, and allows packet forwarding to continue on an alternative output link immediately after the detection of a failure.

IV. OUTPUT OF PROPOSED SYSTEM

The Message transfer relates with that the sender node wants to send a message to the destination node Sender node first selects the Destination node. Sender types the data or browses the .txt file and uploads the url. Checks the corresponding node and corresponding path is available. After the path is selected also find out that node or link is failure and status of the destination node through is true. If anyone of the node or link is failed means sender use the preconfigured backup path. The receiver node receives the message completely and then it send the acknowledgement to the sender node also near by nodes through the router nodes where it is received the message.

V. OVERVIEW OF INTRUSION DETECTION SYSTEM (IDS)

An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use Intrusion detection and prevention systems for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. Intrusion detection and prevention systems have become a necessary addition to the security infrastructure of nearly every organization.

A. Research in Intrusion Detection System (IDS)

A field of research in intrusion detection has focused on the ability of the IDS to detect intrusion attempts, using statistical and algorithm based approaches, and discern between what is merely anomalous (unknown to the system) and not a risk, and what is potentially harmful to the system and should be prevented. Tools available on the market have incorporated these statistical and algorithm-based models in the design of their detection modules, but have largely left response up to the operator, giving the user the ability to script responses. Since precious time is used in detecting an attack, these systems will need to adopt some autonomous response capability, using not only risk and response categorization but also a response escalation algorithm, similar to biological and immune response systems.

B. Implementation of Intrusion Detection System (IDS)

In general, IDS can be implemented in the various locations, as shown in this simplified figure.1.The figure shows that:-

- IDS 1 can detect attacks against the firewall.
- IDS2 detects traffic which has penetrated the firewall.
- IDS 3 represent implementation of one or more IDS at various nodes throughout the network, and can detect attacks by insiders.

IDS should be implemented in conjunction with, rather than in replacement of, a firewall, notification systems, and other intrusion countermeasures. All the organization should have a well defined security policy before implementing IDS, which will help configure the IDS detection parameters and determine an appropriate response. For example, the organization should have a policy clearly defining what constitutes an authorized user, what access rules are, and what the consequences for unauthorized access.

One of the main tasks of IDS is to help distinguish between malevolent and innocent intrusions. Nowadays, computer systems have become more vulnerable to intrusions than ever. Intrusion Detection is a security technology that allows not only the detection of attacks, but also attempts to provide notification of new attacks unforeseen by other components. Intrusion detection is an important component of a security system, and it complements other security technologies. IDS requires full packet inspection in order to identify attack attempts.

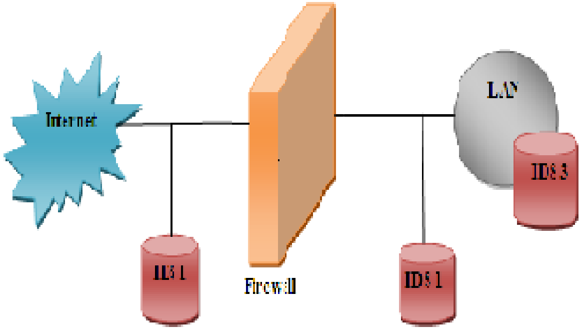

Fig.1 Implementation of Intrusion Detection System (IDS)

VI. ADVANTEGES OF PEER TO PEER REPUTATION MANAGEMENT.

- 100% message transfer.
- Link and Node failures of IP networks.
- The slow convergence of routing protocols after a network failure becomes a growing problem
- Packet loss or packet delay due to congestion.
- Time consumed to send the data is increased due to resending of lost data.
- The failure of particular link is identified.

VII. CONCLUSIONS

Summing up, the work, we have presented Multiple Routing Configurations as an approach to achieve fast recovery fro a link or node failure. MRC is based on providing the routers with additional routing configurations, allowing them to forward packets along routes that avoid a failed component. MRC guarantees recovery from any single node or link failure in an arbitrary bi-connected network. By calculating backup configurations in advance, and operating based on locally available information only, MRC can act promptly after failure discovery. The concept of (IDS) Intrusion detection has indeed come a long way, becoming a necessary means of monitoring, detecting, and responding to security threats. IDS technology has gone through countless iterations and numerous owners. Nonetheless, the use of intrusion detection as a means of deterring misuse has ultimately become commonplace. Moreover, IDS has become essential.

ACKNOWLEDGMENT

We wish to express our sincere gratitude to H.O.D of Computer Science Department of G.H.Raisoni College of Engineering and Technology for women's for providing us an opportunity to do paper work on "Peer To Peer Reputation Management " in "International Journal Of Computer Science Engineering And Technology". We sincerely thank to our paper guide Mrs. Pratibha Mishra, Department of Computer Science and Engineering, for guidance and encouragement in carrying out this paper work, for their kind co-operation to the completion of our paper work. Last but not least we wish to avail of this opportunity, express a sense of gratitude and love to our friends and beloved parents for their manual support, strength, help and for everything.

REFERENCES

[1] Mchugh, J. et al. "Intrusion Detection: Implementation and Operational Issues," Software Engineering Institute Computer Emergency Response Team White Paper, January 2001.

[2] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed internet routing convergence," IEEE/ACM Trans. Networking, vol. 9, no. 3, pp. 293–306,Jun.2001.

[3] Proctor, Paul, The Practical Intrusion Detection Handbook, Prentice Hall, 2001.

[4] slideshare.net/.../ieee-2011-software-projects(US) .

[5] L. Xiong and L. Liu, "PeerTrust: SupportingReputation

[6] Based Trust in Peer-to-Peer Communities," IEEE Trans.

[7] Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.

[8] Jonne Zutt, Arjan J.C. van Gemund, Mathijs M. de Weerdt, and Cees Witteveen (2010). Dealing with Uncertainty in Operational Transport Planning. In R.R. Negenborn and Z. Lukszo and H. Hellendoorn (Eds.) Intelligent Infrastructures, Ch. 14, pp. 355-382. Springer.

[9] Matthew Caesar and Jennifer Rexford. BGP routing policies in ISP networks. IEEE Network Magazine, special issue on Interdomain Routing, Nov/Dec 2005.

[10] Neil Spring, Ratul Mahajan, and Thomas Anderson. Quantifying the Causes of Path Inflation. Proc. SIGCOMM 2003.

[11] Ratul Mahajan, David Wetherall, and Thomas Anderson. Negotiation-Based Routing Between Neighboring ISPs. Proc. NSDI 2005.

[12] Ratul Mahajan, David Wetherall, and Thomas Anderson. Mutually Controlled Routing with Independent ISPs. Proc. NSDI 2007.

[13] Denning, Dorothy E., "An Intrusion Detection Model," Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131

[14] Lunt, Teresa F., "IDES: An Intelligent System for Detecting Intruders," Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22–23, 1990, pages 110–121.

[15] Lunt, Teresa F., "Detecting Intruders in Computer Systems," 1993 Conference on Auditing and Computer Technology, SRI International

[16] Sebring, Michael M., and Whitehurst, R. Alan., "Expert Systems in Intrusion Detection: A Case Study," The 11th National Computer Security Conference, October, 1988

[17] Smaha, Stephen E., "Haystack: An Intrusion Detection System," The Fourth Aerospace Computer Security Applications Conference, Orlando, FL, December, 1988

[18] Vaccaro, H.S., and Liepins, G.E., "Detection of Anomalous Computer Session Activity," The 1989 IEEE Symposium on Security and Privacy, May, 1989

[19] Teng, Henry S., Chen, Kaihu, and Lu, Stephen C-Y, "Adaptive Real-time Anomaly Detection Using Inductively Generated Sequential Patterns," 1990 IEEE Symposium on Security and Privacy

[20] Heberlein, L. Todd, Dias, Gihan V., Levitt, Karl N., Mukherjee, Biswanath, Wood, Jeff, and Wolber, David, "A Network Security Monitor," 1990 Symposium on Research in Security and Privacy, Oakland, CA, pages 296–304