IP Network Recovery Based on Security Managements

Mahboobeh Zangiabady
Department of computer science $ Engg
JNTUH
Hyderabad, India
Me_zangiabady@yahoo.com

Abstract— Computer networks are complex systems, often routing hundreds, thousands, or even millions of data packets every second. Therefore, in order for networks to handle large amounts of data, it is important that the data routes efficiently. So, the need for security management and protecting data become evident in networks. IP network recovery defines Clusters, or multiple computers that work together. IP network recovery designs security policy in network to reduce packet failure, minimize error in networks, and prevent from congestion. The scope of this paper is to introduce structure for Data protection and Retention. It improves energy efficiency in networks by using recovery load distribution algorithm.

Keywords: energy efficiency; security; congestion; IP network recovery.

I. INTRODUCTION

Network is a complex issue that is historically only practiced by those who are trained in the domain. However, as more people are connected to the network, the number of people who should know the basics of energy efficiency in a networked world is also increasing. Energy efficiency is the goal of efforts to reduce the amount of energy required to provide products and services. This method is used to receive a packet of routing information and send it through a network device to another device on a different network. If your network does not have a router, allowing routing of data between your network and other networks would not exist [6]. It is important to find appropriate strategies for improving energy efficiency before the background of rapidly increasing traffic volumes [5].

A router for routing a packet should be aware of the following information: First, router finds destination address, second, it identifies Neighboring routers that are using the possibility of obtaining information on remote networks are provided. Third, router fined Existing routes to all remote networks. Fourth, router fined the best path to a remote network [7].

One of the main potentials required for routing in a network is to communicate with other networks. If there is no possibility of routing protocols, computers will not be able to exchange data [6].

Routers are always attacks by hacker or software. Router may discard packets, so this problem is causing the loss of packets [7][8]. And receiver cannot reach packets. So, packet should resend for several times. The constrained resources of sensor nodes make it very unlikely to employ strong security mechanisms on a sensor platform; the networks are usually deployed in hostile environments such as military battlefields. Therefore, routing protocols for networks face many difficulties, such as energy constraints invite DoS attacks [8], memory and bandwidth constraints prevent using sophisticated routing protocols, compromised nodes may inject malicious messages or drop data traffic, and so on. MRC is connectionless that send packet over networks [11]. First IP network recovery find additional route to destination and the recovered traffic is routed in a backup configuration from the point of failure to the egress node [4]. This shifting of traffic from the original path to a backup path affects the load distribution in the network, and might lead to congestion [2]. Occasionally the load added on a link can be significant. Enhanced IP network recovery find isolated node [3].

II. OVERVIEW OF INR PROTOCOL

A. *step one*

First, Spatial structure refers to an integrated information environment in wide range area that in this case is PLR and delay is a technique to solve packets failure problems. So, Packet loss rate calculates the average loss of IP packets over the network server is defined.

Second, delay is the average time it takes for destination to receive packet. This parameter is calculated based on the average of the sampling period.

First, One of the most important and challenging problems in the sensor network is energy and lifetime of network nodes [5]. To increase the life of nodes at data transfer between source and destination nodes can be used in different ways. One of these methods is loads distribution [1] among network nodes. Second, specify the buffer size and solve the traffic problem and congestions. Third, resolve the ambiguity around the lost packets. Once the ambiguity from congestion is removed, subsequent packet losses can be attributed to malicious actions. Fourth, calculate the number of Routers that have been attacked. Fifth, the packet includes a timestamp. Timestamp consist of an optional generation time. So with time stamp router can understand the stream of data. So it is simple to understand which packets are come from attackers. Sixth, Separation of isolated router from non-isolated routers by IP addresses [3]. Seventh, generate backup from data .with this solution we can compare packets that receive by destination with original packets. Then we calculate the number of packets lost.

B. Step2

After first step INR distributes the processing and traffic evenly across a network, making sure no single device is overwhelmed. Web servers, as in the example above, often use load balancing to evenly split the traffic load among several different servers. This allows them to use the available bandwidth more effectively, and therefore provides faster access to the websites they host. The goal of network security, network protection against these attacks, so the targets can be presented in four categories: Fixed a data privacy, Maintain integrity, Maintaining data availability, and Risk Analysis [9].Network security is a process in which a network can be secured against a variety of internal and external threats [2]. The following steps are recommended for safety and have been approved: The first thing helps the network technician able to detect possible faults related to how network worked before packet has lost. It is easier to identify the cause of errors.

- Link Test
- Research on segments activity analysis
- Use of DHCP
- Ping in local and remote for test link.
- Identify the part that should be protected
- To make decisions about where they need to be protected from the departments concerned.
- Make decisions about threats.
- Re-review process and strengthen its ongoing weakness

Besides the obvious benefits of increasing energy efficiency of network elements by leveraging technology progress, load-adaptive network operation is a very promising option. The risk analysis of network security policies must be defined in such a way that risks of damage to a minimum. General overview of security policies and do not pay details. Details can be changed within a short time, but the overall securities of a network that constitute its Policies remain constant [9]. Implementation of security policy before each router is mandatory “Fig. 1”.

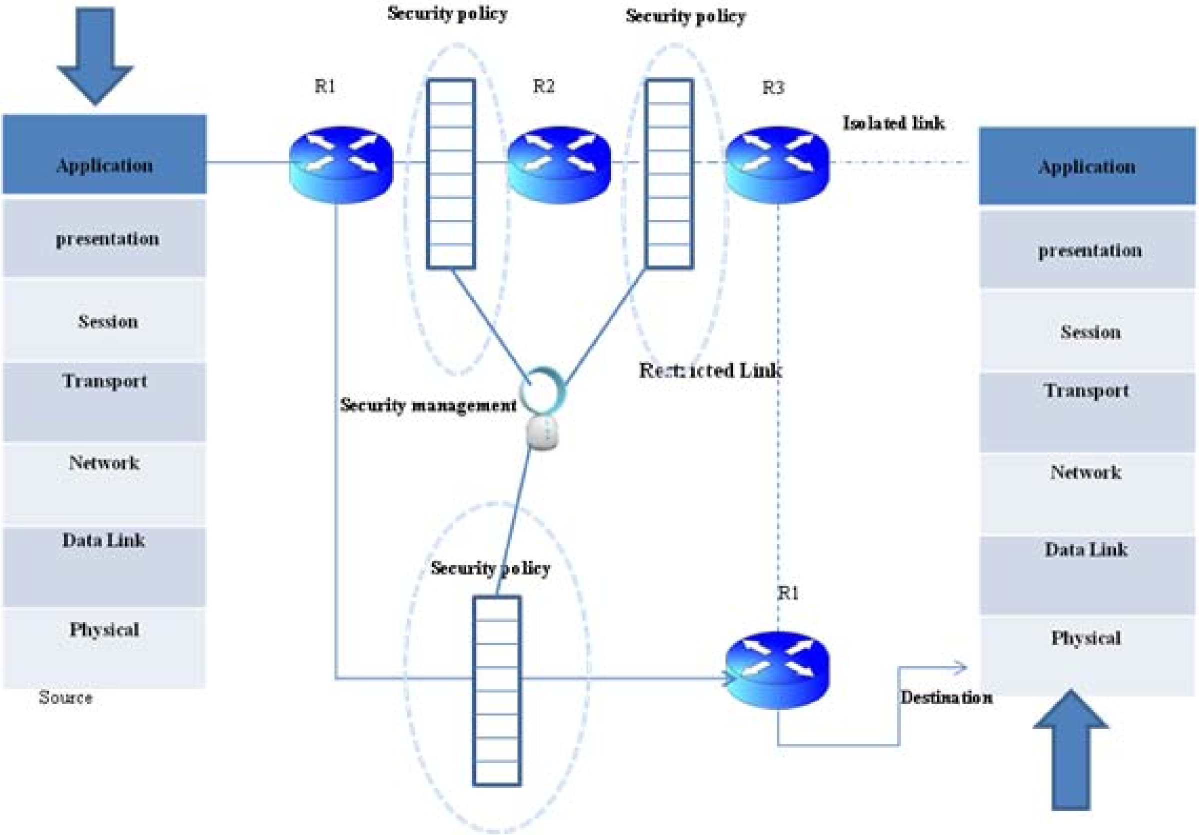
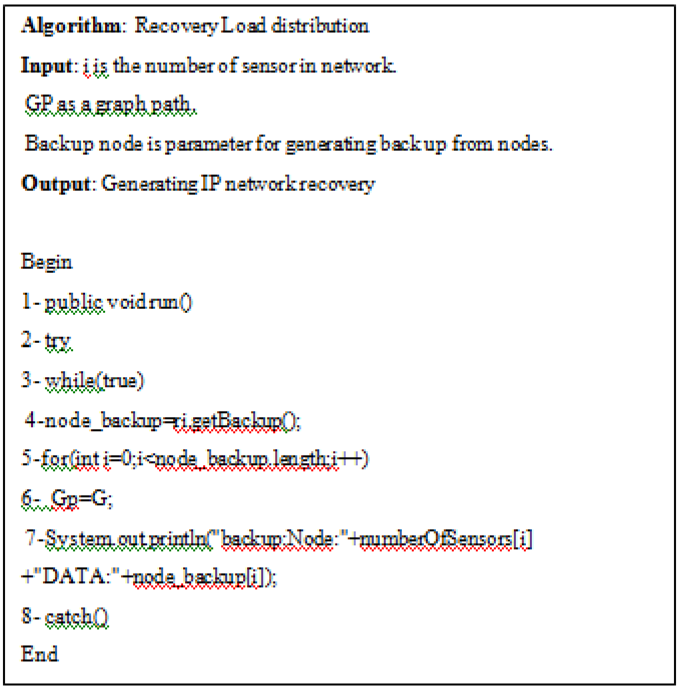


Figure1 .Design security policy before routers

III. GENERATING RECOVERY LOAD DISTRIBUTION ALGORITHM:

Whether load distribution is done on a local network or a large Web server, it requires hardware or software that divides incoming traffic among the available servers. Networks that receive high amounts of traffic may even have one or more servers dedicated to balancing the load among the other servers and devices in the network [1]. These servers are often called (not surprisingly) load balancers”table I”.

TABLE I. GENERATING RECOVERY LOAD DISTRIBUTION ALGORITHM



```
Algorithm: Recovery Load distribution
Input: i is the number of sensor in network.
 GP as a graph path.
 Backup node is parameter for generating back up from nodes.
Output: Generating IP network recovery

Begin
public void run()
try
while(true)
node_backup=ri.getBackup();
for(int i=0;i<node_backup.length;i++)
 Gp=G;
System.out.println("backup:Node:"+numberOfSensors[i]
+"DATA:"+node_backup[i]);
catch()
End
```

IV. EXPERIMENTAL RESULTS

A. Simulation parameters

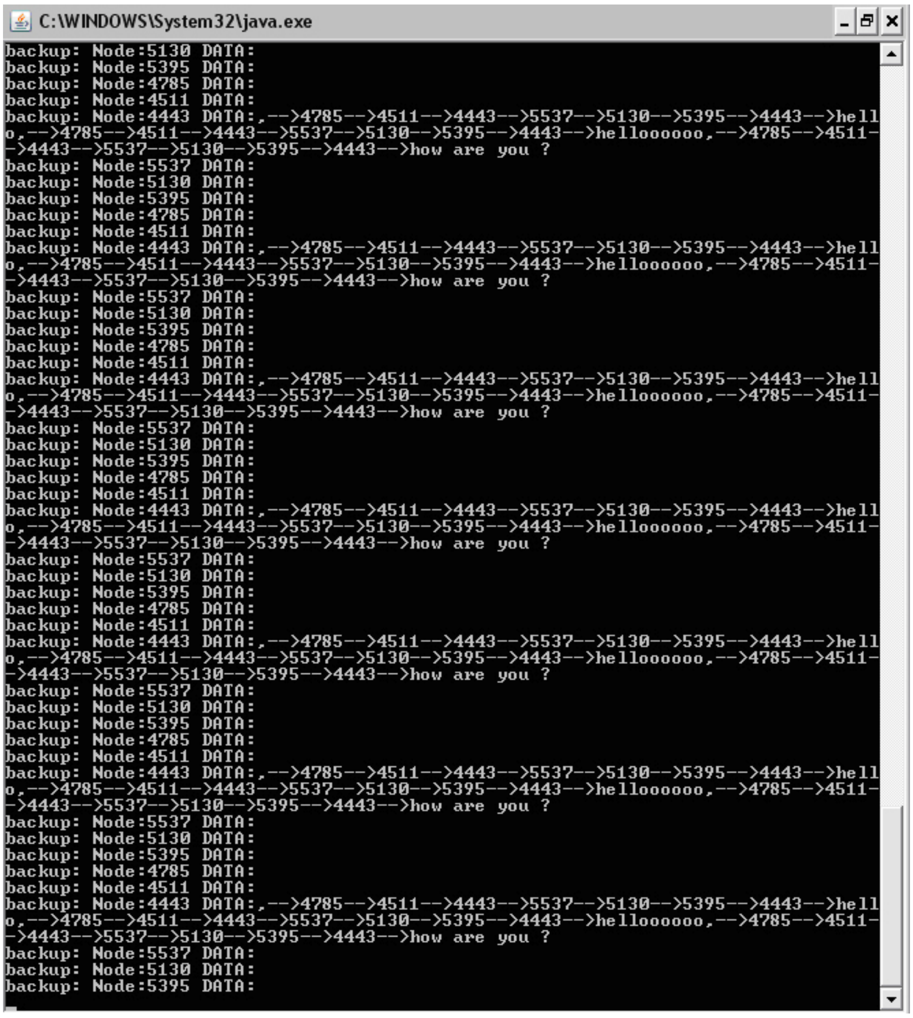
Compare with EINR, INR design security policy for packets which before routers. Hence it guarantees information security in networks. Second parameter is energy efficiency improvement in networks “TABLE II”. Protocol tries to detect errors and prevent from congestion.

TABLE II . INR EXPERIMENTAL RESULTS

	delay	**Improve energy efficiency**	**security policy**	**congestion**	**errors**
INR	minimum	Yes	Yes	minimum	minimum

B. Simulation results

IP network recovery tests for more than 100 nodes by using java” Fig. 2”. Unlike other methods used with normal IP rerouting, this method does not compromise on the routing performance in the failure free case.



```
backup: Node:5130 DATA:
backup: Node:5395 DATA:
backup: Node:4785 DATA:
backup: Node:4511 DATA:
backup: Node:4443 DATA:,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hell
o,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hellooooo,-->4785-->4511-
->4443-->5537-->5130-->5395-->4443-->how are you ?
backup: Node:5537 DATA:
backup: Node:5130 DATA:
backup: Node:5395 DATA:
backup: Node:4785 DATA:
backup: Node:4511 DATA:
backup: Node:4443 DATA:,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hell
o,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hellooooo,-->4785-->4511-
->4443-->5537-->5130-->5395-->4443-->how are you ?
backup: Node:5537 DATA:
backup: Node:5130 DATA:
backup: Node:5395 DATA:
backup: Node:4785 DATA:
backup: Node:4511 DATA:
backup: Node:4443 DATA:,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hell
o,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hellooooo,-->4785-->4511-
->4443-->5537-->5130-->5395-->4443-->how are you ?
backup: Node:5537 DATA:
backup: Node:5130 DATA:
backup: Node:5395 DATA:
backup: Node:4785 DATA:
backup: Node:4511 DATA:
backup: Node:4443 DATA:,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hell
o,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hellooooo,-->4785-->4511-
->4443-->5537-->5130-->5395-->4443-->how are you ?
backup: Node:5537 DATA:
backup: Node:5130 DATA:
backup: Node:5395 DATA:
backup: Node:4785 DATA:
backup: Node:4511 DATA:
backup: Node:4443 DATA:,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hell
o,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hellooooo,-->4785-->4511-
->4443-->5537-->5130-->5395-->4443-->how are you ?
backup: Node:5537 DATA:
backup: Node:5130 DATA:
backup: Node:5395 DATA:
backup: Node:4785 DATA:
backup: Node:4511 DATA:
backup: Node:4443 DATA:,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hell
o,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hellooooo,-->4785-->4511-
->4443-->5537-->5130-->5395-->4443-->how are you ?
backup: Node:5537 DATA:
backup: Node:5130 DATA:
backup: Node:5395 DATA:
backup: Node:4785 DATA:
backup: Node:4511 DATA:
backup: Node:4443 DATA:,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hell
o,-->4785-->4511-->4443-->5537-->5130-->5395-->4443-->hellooooo,-->4785-->4511-
->4443-->5537-->5130-->5395-->4443-->how are you ?
backup: Node:5537 DATA:
backup: Node:5130 DATA:
backup: Node:5395 DATA:
_
```

Figure2 : Simulation results

V. PERFORMANCE COMPARISON WITH OTHER RELATED WORKS

In this section, I compare 4 protocols. MRC is strictly connectionless and it is base on hop by hop forwarding [11]. FINR or fast IP network recovery is local mechanism that route packet through backup configuration [4] .but it does not guarantee security policy. EINR improve speed by separation of isolated nodes from non isolated nodes .EINR does not improve energy efficiency [3] “Fig. 3”.

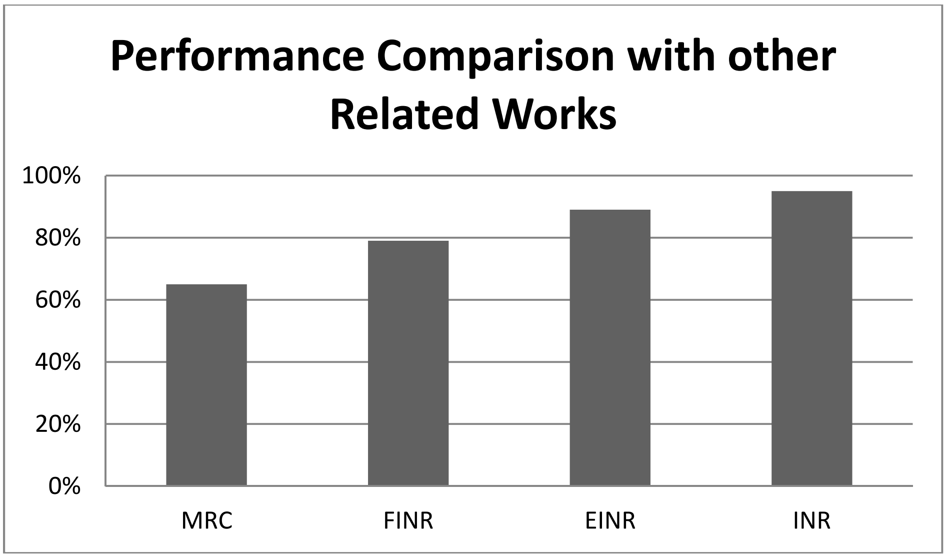


Figure 3 . Comparison with other related works

VI. CONLUSION

Network behavior analysis (NBA) is an intrusion-detection technique that uses the patterns in network-traffic structures and properties to identify possible attacks and technical problems with minimal impact on user data .privacy With use of security policy, packet receive by destination and it prevents from packet failure .INR minimize error and congestion in network. So, this mechanism used to optimize energy in networks.

REFERENCES

[1] Mingui Zhang, Bin Liu, and Beichuan Zhang,” Load-balanced ip fast failure recovery,” IPOM '08 Proceedings of the 8th IEEE international workshop on IP Operations and Management,2008,pp.5-10

[2] Mariana Hentea,” Intelligent system for information securitymanagement: architecture and design issues,” Informing Science & Information Technology, Vol. 4, 2007,pp. 30-37

[3] Mahboobeh Zangiabady, Mohammad Sadegh Mirzaei,” Enhanced ip network recovery: novel method tocope with isolated node,” International Conference on Computing, Communications and Applications-ICCCSA / Hyderabad, 2012,pp.2,3

[4] Mahboobeh Zangiabady, Mohammad Sadegh Mirzaei,”Novel method for fast ip network recovery, “IEEE Student Conference on Electrical, Electronics and Computer Science, MANIT Bhopal, March 2012,pp. 4

[5] Rod Mahdavi, PE, LEED AP William Tschudi, PE,” Wireless sensor network for improving the energy efficiency of data centers,” The General Services Administration ,march 2012,pp. 25-34

[6] Alper T. M_zrak, Stefan Savage, Keith Marzullo,” Detecting malicious packet losses,” IEEE Transactions on parallel and distributed systems, vol. 20, no. 2, february 2009 191,pp.193-195

[7] Raj Kumar Rajendran, Dan Rubenstein,” A theory for networks with misconfigured routers,” Columbia University Technical Report, New York, NY, May 2004,pp. 2-4

[8] Hemanth S, G Sudhakar,Chaitanya K,” Dynamic recognition of malicious routers,” international journal of modern engineering Research (IJMER), Vol.1, pp. 4-10

[9] http://www.securitymanagement.com/

[10] LOAD BALANCING : http://www.IBM.com/

[11] Amund Kvalbein, Audun Fosselie Hansen, Tarik Ci, Stein Gjessing, OlavLysne, “Multiple routing configurations for fast IP network recovery,” IEEE/ACM Transactions on Networking, April 2009, Volume: 17, pp.473-475