

On A New Global Catastrophic ICT Model

Dipashree M. Bhalerao¹, M. Tahir Riaz², Michael Jensen³ Ole Brun Madsen⁴ and Ramjee Prasad⁵

Sinhgad Technical Education Society, Department of Electronics and telecommunication, Pune, India¹, CTIF, Department of Electronic Systems, Aalborg University, Aalborg, Denmark²⁻⁵
E-mail: {¹dmb, ²tahir, ³mj, ⁴obm, ⁵prasad}@es.aau.dk

Abstract--- Many parts of India are prone to natural disasters, particularly caused by earthquakes and floods because of its geographical location. The Catastrophic areas can be rural, remote or urban anywhere in the world. It has been understood that earthquakes directly do not cause causalities but instead by side effects of weak or faulty constructed buildings and infrastructure etc. As there can be destruction in all kinds of infrastructure, it is difficult to keep communication in such areas. Communication in such areas is one of the highest priorities to solve various problems faced. A large group of the world's population suffers from affordable ICT solutions and the presence of sufficient ICT infrastructure. The main goal of this paper is to create a framework to define catastrophic areas from an ICT point of view. QOS features like packet loss rate, delay, throughput and delivery ratio for 50 nodes have been experimented. The graphs are taken before calamities and after introduction of calamities. This comparison tells the network parameter patterns in catastrophic area. This in turn helps, to define the catastrophic area. The paper has also tried to show the catastrophic area connectivity coverage before and after calamities. This definition of catastrophic area from ICT point of view has no one tried before. Network parameters behavioural graphs are also important. This paper presents only behavioural part.

Keywords ICT Infrastructure, rural area, poor area, catastrophic area, Internet of Things

I. INTRODUCTION

This work is a follow-up on the discussions at on the needs for a new global ICT infrastructure [1] reference architecture for rural poor and catastrophic area (RPC). Almost every year, the world is stricken by numerous catastrophic natural disasters, such as earthquake, hurricane, typhoon, tsunami, etc. When a catastrophic natural disaster strikes, an organized and effective rescue operation is essential to rescue those victims who are trapped under collapsed buildings or landslides, and also to relief massive survivals who lose their life support [2]. However, communication systems are usually paralyzed by many causes. The loss of communication systems made rescue and relief operations extremely difficult costing many lives unnecessarily. The causes of communication system failure can be any one out of the base-stations crashed, trunks broken, backup power generators failed, cooling systems for critical equipments failed, cell phones/Machines ran out of battery, chargers not available and communication network traffic jams and similar others. Threatened by so many sources of potential failures, it needs a reliable communication system to survive. When a disaster

strikes suddenly, there is not enough time allowed to deploy a new full-functional alternative solution.

We can conclude that the communication system often fails due to natural catastrophe or other problems in communication infrastructure. This failure can be in different percentages according to intensity of natural calamity. Hybrid network scenario has been developed with 50 nodes using NS2 simulator. Damage in different percentages of 50 and 90 are introduced in the network. For all cases natural and damaged, QOS parameters are recorded and plotted. The nature of graph will help in defining the catastrophic area

The main aim of the paper is to develop the framework of behavioral pattern for defining catastrophic area from ICT point of view. Here no remedial actions are suggested, as focus is only on catastrophic area network behavior. First we try to define normal term catastrophe and then we try to plot and model it from the ICT point of view. Catastrophic failures are events that cause entire clusters of infrastructure to become unavailable such as network partitioning, router failures, natural disasters, or even terrorist attacks. ICT catastrophic area is an area where availability of communication is degraded or not available due to a catastrophic event like cyclones, earthquake etc. Catastrophic failures are failures that completely block all communication from the current server cluster to the client.

When information between communication networks is damaged because of natural catastrophe or due to any other mishap to communication infrastructure, we say that there is ICT failure.

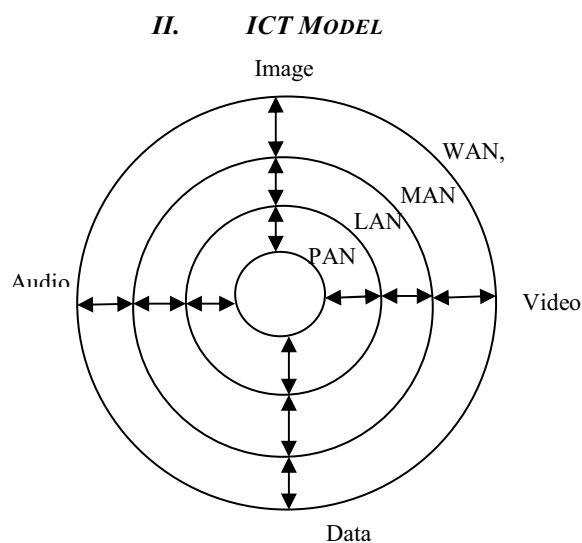


Figure 2. A generic representation of ICT model.

The Information and communication technology can be easily understood if we separate information and communication from each other, and if we try to understand each separately and then correlate them. Information is nothing but data with intelligence or data with meaning. For example 0 means off or false and 1 means on or true. This data when added intelligence to it is useful information. This can be in the form of data, image, audio or video form. Communication means exchange of information from one thing to another thing for the required work. These things can be one or many. Also they can be at one place only or at different geographical locations. For communicating with these things we may use PAN, LAN, VAN, MAN or WAN. Communication can be within individual network or within intra network. When two or more different networks are connected we say it is an internetwork. Internet is such a structured and organized system which makes use of the above given communication networks for exchanging wealth of information between them. This organized information is easily communicated to user.

CATASTROPHIC ICT MODEL

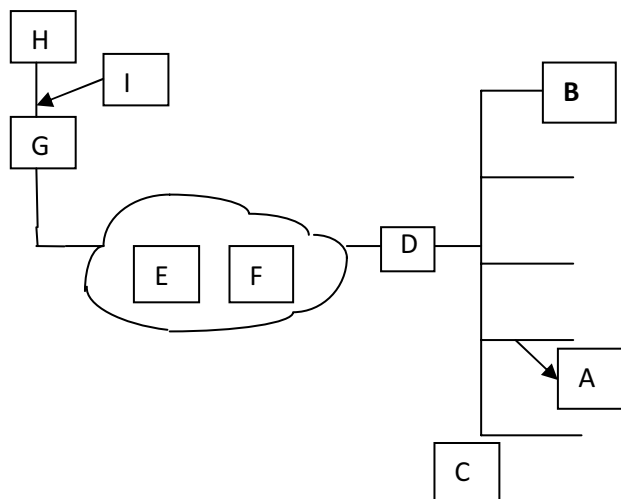


Figure 2. sever - client channel failure model

These networks can be connected in any combination, for example, between PAN and WAN or WAN AND WAN. In any network, data will be transmitted from server to client. In this chain what are the possible places of failure are shown in above failure model. As damage occurs out of above failures any failure is possible. In Figure 1, we illustrate where failures can occur along a communication channel [3, 4] and put them into two categories: *server-side* and *client-side*. Different blocks in communication between server and client can be shown as follows. These are failure points. Failure can be in the range 1-100 %.

Server side

Failures are: (A) Process, (B) Machine, (C) Cluster, (D) Switch, (E) NAP, (F) router with/without route, alternate route.

Client side

Failures are: (G) Router, (H) Machine, and (I) Process.

Between two routers the connection can be point to point link with modem at each end; between routers to machine it can be wired or wireless link. Number of base-stations can be there in the Internet cloud. Instead of a switch there can be other devices like hub, bridge etc. This setup will be according to the types of networks.

Table I : Network Components

Sr. no	Type of Network	Link type	DTE/DCE
1	WAN	Wired + wireless	Switch, modem, NAP, computer, Cell, ISP
2	MAN	Wired + wireless	Hub, router
3	LAN	Wired + wireless	Hub, router
4	PAN	Wireless	Sensor nodes

Now we have ICT model and communication channel with us. We know the effect of catastrophe on this channel.

We assume that there is sufficient field strength and QOS in network communication, when normal conditions are there. Taking into account all things, we try to develop catastrophic ICT Model as follows.

Catastrophic ICT model combines the ICT model and sever - client channel failure model.

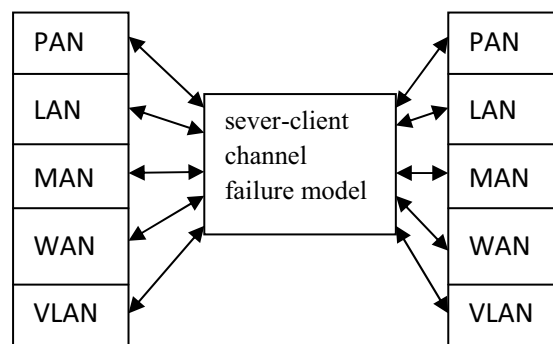


Figure 3. Catastrophic ICT Model

III. SIMULATION IN NS2

We create a scenario of Hybrid model considering the same type is used in practice. It is a combination of wireless and wired network. We put 50 wireless nodes. The node has two ray ground models and uses MAC-802.11 standard. The area for model is set as 100*3480 in meters. Total period of execution is 110ms. Antenna is Omni directional and drop tail

type of queue. All these things can be changed and readings can be taken for other models, Queues etc.

This script defines a simple topology of 50 nodes, and single agent, a UDP agent with a CBR traffic generator. The simulation runs for 110ms. The output is two trace files, out.tr and out.nam.

Scenario is divided into 10 domains. 4 wireless and six wired. Three wireless domains have 15 nodes , and fourth domain has 6. Remaining domains consists of total 16 wired lines. These lines are connected to a base station , which is nothing but a wireless node. There are total 12 base stations which are scattered in 4 wireless domains.

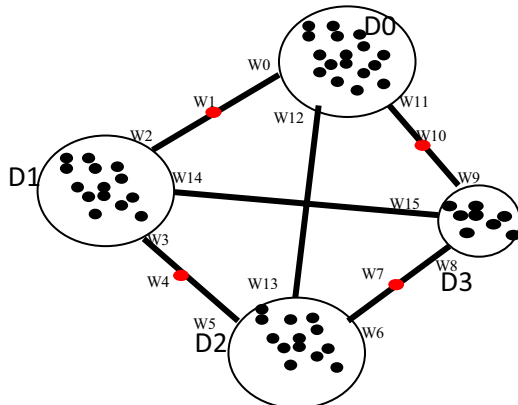


Figure 4. Developed Hybrid model topology

To study the catastrophic effect , following steps have been taken.

1. Conectivity is provided between wireless-wireless, wired-wired, wireless-wired and wired-wireless points. Different points from all domains have been taken.Damage has been introduced by deactivating links and nodes.
2. Domain 1 and 2 are damaged for 40-50 %.
3. Domain 1,2 and 3 are damaged for 90-92 %.
4. The graphs are plotted for Normal connectivity pattern and with 50 % and 90% damaged pattern.

IV. RESULTS AND GRAPHS

Throughput, packet delivery ratio, End to End delay results are shown below.

Table II: Interval VS Throughput

Interval	Throughput-n	Throughput-50	Throughput-90
1	16.66666667	8.333333333	0
2	16.82389937	8.757961783	0
3	16.8618267	8.80952381	0
4	16.875	8.805031447	0
5	17.1875	8.62745098	0
6	16.51376147	8.962264151	0
7	17.39130435	8.743169399	0
8	17.5	8.805031447	0
9	16.43835616	8.965517241	0
10	16.66666667	8.333333333	0

Table III: Interval VS Packet delivery ratio

INT	PK-Del-ratio-n	PK-Del-ratio-50	PK-Del-ratio-90
1	16.6667	8.33333	0
2	16.8239	8.75796	0
3	16.8618	8.80952	0
4	16.875	8.80503	0
5	17.1875	8.62745	0
6	16.5138	8.96226	0
7	17.3913	8.74317	0
8	17.5	8.80503	0
9	16.4384	8.96552	0
10	16.6667	8.33333	0

Table IV: Interval VS Average end to end delay

INT	e-e-avg-del-n	e-e-avg-del-50	e-e-avg-del-92
1	10736.1	4347.99	880.642
2	11185.6	4619.88	889.567
3	11091.5	4281.52	834.037
4	10639.1	4112.26	778.514
5	10158	4062.72	500.664
6	10379.9	3853.07	667.478
7	10268	3086.46	813.412
8	9567.34	3903.77	214.929
9	9608.7	3920.24	250.751
10	9856.78	2970.99	273.546

Records are taken for packets generated, packets received, dropped and lost packets. Average end to end delay, packet delivery ratio and throughput are calculated from above mentioned records. All above mentioned and calculated results are plotted below. Above results are plotted below. Also other plots are us

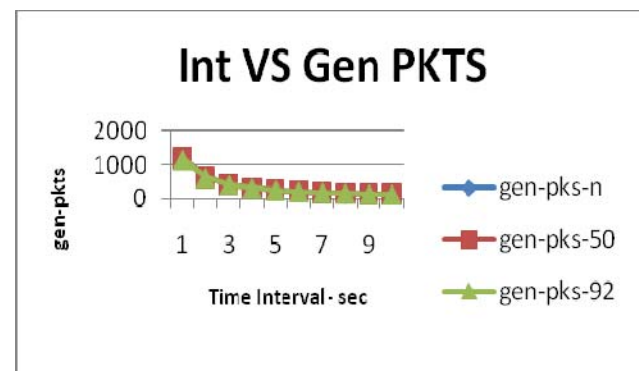


Figure 5. Time interval Vs packets generated

From the above graph (Fig.5) we can say that packet generation is approximately same in all the three cases. This is because the nodes and wired links are made down, but the generation is still there. The time interval suggests the effect of catastrophe on damage.

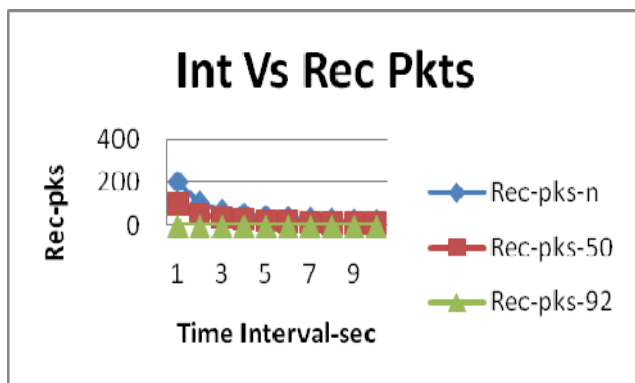


Figure 6. Time interval Vs received packets

Second graph (Figure.6) shows that the received packets are reduced as damage is increased. For 90 % damage no packets are received. Because of damage number of packets received will start reducing.

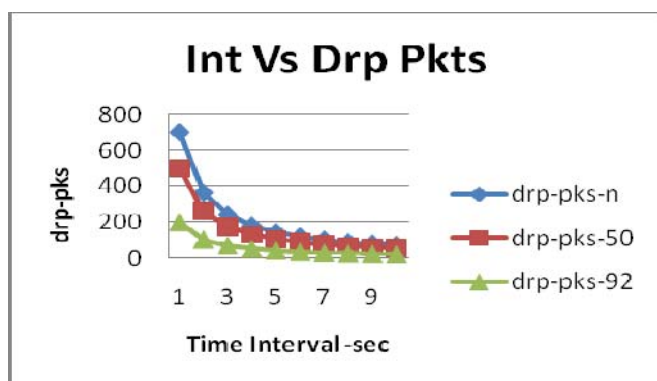


Figure7. Time interval Vs dropped packets

Third graph (Figure-7) shows the dropped packets pattern. Here dropped packets are maximum in 90% of damage. Drop rate increases as damage is increased. It indicated that if there is no infrastructure to transmit packets at the destination node, they will be dropped in the proportion of damage.

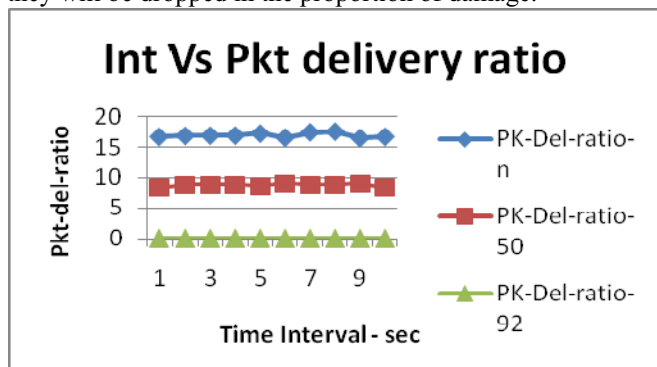


Figure 8. Time interval Vs packet delivery ratio

Fourth graph (Fig-8) is between the time interval Vs the packet delivery ratio. From the graph we conclude that the delivery ratio tends to zero with a considerable damage.

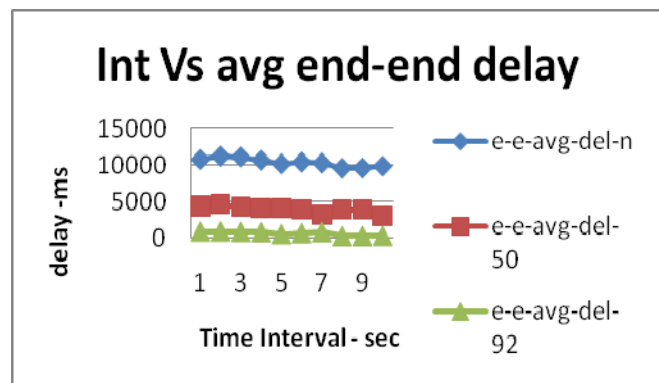


Figure 9. Time interval Vs avg. end to end delay

Fifth graph (Fig-9) is between the time interval Vs the average end to end delay. This is in msec. Graph nature tells us that it reduces drastically to fractions of u- sec. Reduction increases with damage. Because of intermediate damages and congestion end to end delay that is latency is going to increase

From the graph (Figure-10) we can say that packet loss ratio also increases as the damage is increased. Packets can be lost because of congestion. Congestion is bound to be there when damages are there. Over the period of time network shall be passing packets slowly though network which is working.

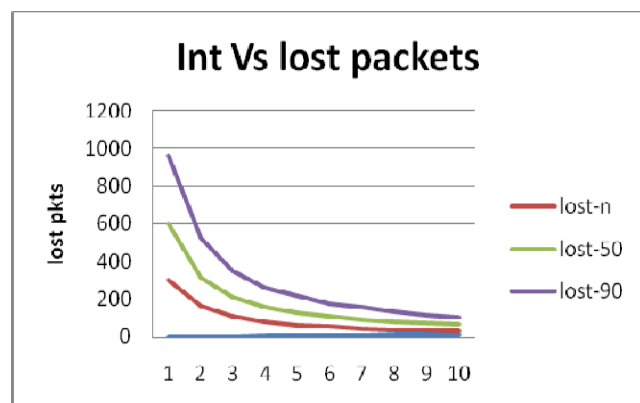


Figure 10. Time interval Vs packet loss rate

From the throughput graph ((Fig-11) we can observe the throughput decrease drastically, with the damage. IT is a ratio of received packets by generated packets. Generated packets are equals to received plus dropped packets. The graph proves the relation with damage.

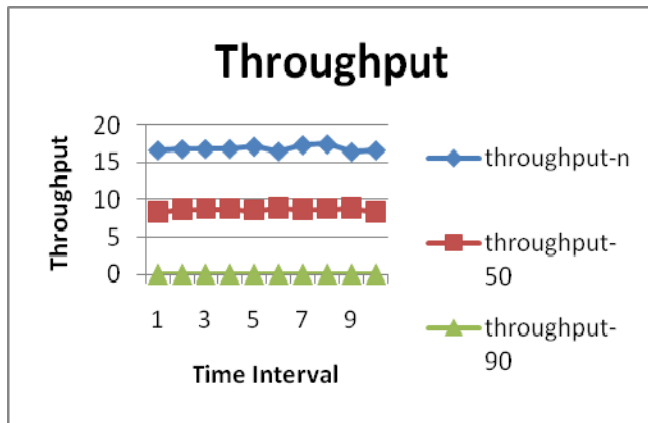


Figure 11. Time interval Vs throughput

V. CONCLUSIONS

It is observed that according to different topologies plotted above, QOS parameters changes the graph, but the overall graph nature remains same. From the above graphs we conclude that whenever received packets are zero and packet delivery rate is zero, then there is a severe catastrophic condition. Here we need to compare these results with normal results. When end to end delay, throughput, generated packets decreases drastically, damage increases. Packet loss rate increases as damage increase.

Catastrophic condition can be due to natural calamity or damage in infrastructure because of other problem.

VI. FUTURE WORK

Plotting of behavioral pattern is not sufficient for a complete definition of catastrophic area. Mathematical model and algorithm can be developed for accurate definition of catastrophic area.

REFERENCES

- [1] The 11th Strategic Workshop SW'09 in Rebild, Denmark 2009, "on Wireless Innovation for InterDynamic TecHnology."
- [2] M. Luo and C. Yang. "Constructing zero-loss web services." In IEEE Infocom 2001, Anchorage, Alaska, April 2001.
- [3] Michael Haungs, Raju Pandey, Earl Barr, "Handling Catastrophic Failures in Scalable Internet Applications," saint, pp.188, 2004 Symposium on Applications and the Internet (SAINT'04), 2004
- [4] L. Alvisi, T.C. Bressoud, A. El-Khashab, K. Marzullo, and D. Zagorodnov. Wrapping server-side TCP to mask connection failures. In the Proceedings of IEEE, INFOCOM 2001, pages 329–338, Anchorage, AK, USA, April 2001.