ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 6, June 2020

Cyber Risk Analysis of Combined Data Attacks against Power System State Estimation

S.Abirami[1], Lynus Sarah[2], E.Padma Sundari[3], Dr.R.Ravi[4]

[1, 2,3](Department of IT, UG Scholar, Francis Xavier Engineering College, Tirunelveli, India)

[4](Professor, Department of IT, Francis Xavier Engineering College, Tirunelveli, India)

Abstract: Data is an extremely valuable resource, hence it has become a key target of cyber criminals all over the world. Therefore it has become mandatory to ensure protection from and perform analysis of data attack. In this paper, we conduct the risk analysis of combined data attacks against power system state estimation. To perform risk analysis we have made use of two languages – python and R and one algorithm – Greedy algorithm. In this paper, the nodes of a network are analysed to find all the attacked nodes in the network. The data set containing the information about the attacked node is fed at input in R studio. R language is essential for providing and in-depth graphical representation of the attack node based on the types of attack performed and the types of protocols used in the process. Finally, the risk of combined attacks to reliable system operation is evaluated using the results from vulnerability assessment and attack impact analysis. The findings in this paper are validated and supported by a detailed case study.

Keywords: **combined data attacks, risk analysis, power system state estimation**

I. Introduction

A. *THE PROBLEM (Slow coordination)*

The reconvergence times in traditional routing systems after failures are known be high. In a nutshell, in these traditional routing systems, whenever a link or node fails, routing tables are recomputed by executing the (distributed) routing protocol again. These recomputations result in relatively long outages after failures, leading to high packet loss rates. While recent advances in routers have reduced reconvergence times, they are still too high for critical services which are sensitive to periods of traffic loss that are orders of magnitude shorter than this.

B. *THE SOLUTION (No coordination)*

Modern computer networks hence include pre-computed backup routes and rules for fast failover, allowing for very fast failure detection and rerouting. These local in band re-routing mechanisms are often meant as a first line of defense, and the resulting fast but simple rerouting is just a temporary solution, before the control plane rigorously optimizes the flow allocation for the new network topology. A most well-known example is Fast Reroute in MPLS where, upon a link failure, packets are sent along a precomputed alternate path without waiting for the global recomputation of routes. Another example, particularly relevant in data centers, are failover schemes based on ECMP: when a link is detected to be unavailable (e.g., using LLDP neighbour discovery), flows are load-balanced (i.e., re-hashed) among the remaining shortest paths.

These mechanisms avoid the complexities involved in distributed coordination among switches or routers, but are completely local approaches: the reaction of a router only depends on the status of its incident links, and a router does not inform other routers about failures. In this case, the disruption time can be limited to the small time taken to detect the adjacent failure and invoke the backup routes.

C. *THE CHALLENGE (Multiple failures)*

The challenge of designing resilient local fast rerouting mechanisms is that these mechanisms need to reply on local knowledge only : in contrast to dynamic routing tables which may change in response to link failures (e.g., using link reversals), failover routing tables are usually statically preconfigured. However, rerouting traffic along efficient paths based on local decisions only is challenging in the presence of multiple failures: a real and frequently studied threat, also in data centers, e.g., due to shared risk link groups (see also RFC 8001), attacks, network virtualization, cascading overload, or simply node failures which affect all incident links.

II. EXISTING SYSTEM

In the existing system, without relay the data will send from a client and a receiver. If some traffic arises the data will be lost. There is no intermediate between a client and a receiver. No acknowledgement of the data sent. The path will not check the closest path of the nearest node. If the server is busy in the network there is no other service for the retransmission and the data will be lost permanently. There is no trust worthy server. In the network path, there is lot of fluctuation, un-availability and delay of the process. You may lose some features or experience some in compatibilities between a client and a receiver due to the mobility and reliability. Without intermediate we cannot transfer the data through the network. The user will be concern after sending the packets. There is no confirmation about the delivery of the packets and also no acting server.

III.PROPOSED SYSTEM

The objective is to deliver frames faster by using multi-rate capability, which does not necessary enhance the communication reliability in interference- rich environment. On the other hand, cooperative communication at the PHY layer attracts a lot of researches attention because it directly enhances the link reliability. Cooperative communication exploits diversity offered by multiple users, known as multiuser or cooperative diversity. It dramatically improves bit error rate (BER), resulting in a more reliable transmission and a higher throughput. It is important to note that the primary motivation of the cooperative diversity in this paper is to improve the link reliability over wireless fading channels.

The proposed CD-MAC operates on a single channel and uses a single partner (rely). Meanwhile, the relay do not store a copy of clients data, it only deliver the data from sender to receiver. A key element of the CD-MAC is the selection of partner; each node moniters its neighbours and dynamically determines a single partner as the one that exhibits the best link quality. In the original CD-MAC algorithm, a sender and its partner cooperatively transmit a frame whenever a sender experiences a transmission failure. However a transmission, failure due to collisions/ interference should be treated differently from that due to channel error. If it is due to the later, it helps because the communication becomes more reburst in the presence of channel error. While most of studies concentrate on evaluating BER and outage probability via cooperative diversity, This paper evaluates system-levels performances such as packet delivery capability.

IV.SYSTEM REQUIREMRNTS

A. *Software Requirements*

- Operating System: Windows 10
- Front end : R studio, IDLE python
- Back end : No DB
- Coding language : R,python

B. *Hardware Requirements*

- System : Pentium IV 2.4 GHz.
- Hard disk : 60 GB
- RAM : 1GB
- Keyboard : Logitech 110 keys
- Mouse : Logitech Mouse

V. MODULES DESCRIPTION

Sender module is the initiate module for the data transfer between the nodes in network communication. A sender node is the data source node which will transmit that data into the valid destination.

Fig.1 python screen

Receiver is the destination node where the sender data have to reach. Receiver nodes are generally aware of its neighbour node to get the data from sender. After it received the data exactly receiver node should send acknowledgement to the sender to intimate that the data was received.

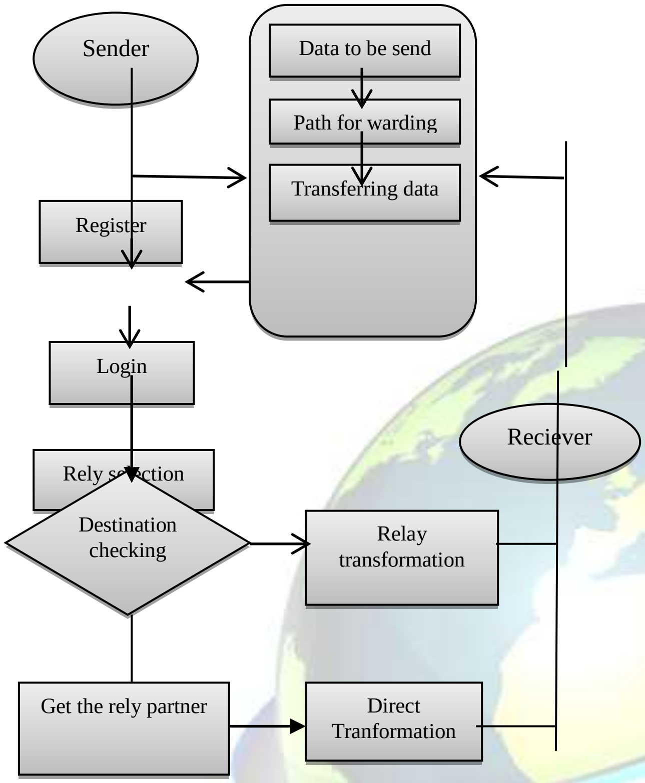

Fig.2 System Architecture

Partner selection module is main process, here the node will chooses a neighbour node which is actually better in performance to transmit data to destination. It will use the performance between the sharing data among nodes and its corresponding neighbours. RTS/CTS are not the mandatory in this CD-MAC so there is no need of much concentrate here. These request are improves the additional performance about the network communication.

Once sender chooses the relay partner, performance depends data transfer will be maintain in the network. These performance are mainly depend on data sharing, most nearer, data availability. If the relay performance are poor than the sender node then that transmission depends that next nearest neighbour.

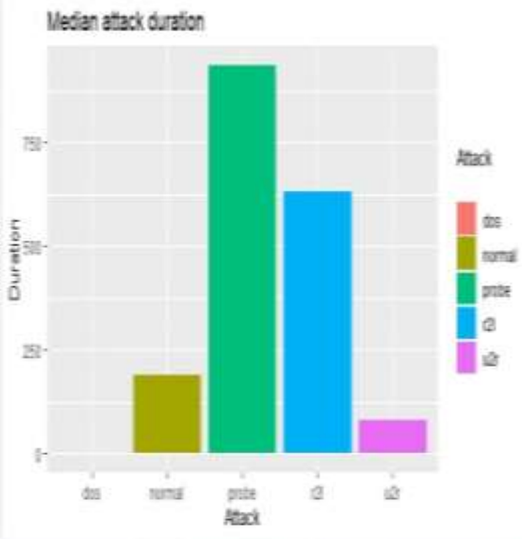

Fig.3 Median attack duration

This module is the final module, which explains the overall data transfers, node problems, relay details and the data sharing with the admin part. If the sender and receiver nodes use the CTS/RTS then that details are reported to the admin respectively.

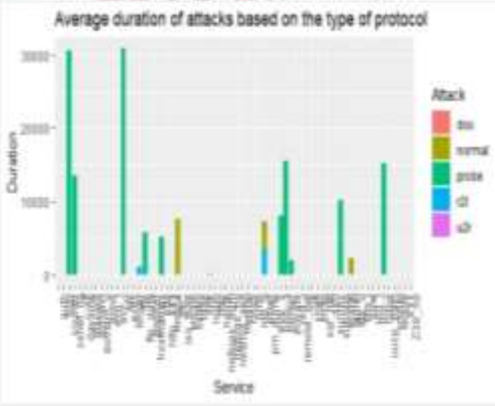

Fig.4 Average duration of attacks based on the type of protocol

VI. Conclusion

In order to guarantee connectivity, this paper leveraged an intriguing connection between local failover mechanisms and combinatorial block designs. In particular, we developed a deterministic failover scheme defining an almost optimal trade-off between resilience and network load: the resulting bounds are off by a constant factor of the optimal bound. Our work hence settles an open question: while mechanisms such as Fast Reroute have been in place for many years, the fundamental trade off regarding their level of resiliency and resource overheads such as load were long not well understood.

An attractive property of our approach is that the required number of failover rules is low: the number of rules only depends linearly on the number of failed links incident to the switch, and not on the number of possible combination of possible combination of possible link failures.

REFERENCES

[1]. M. Al-Fares, A. Loukissas, and A. Vahdat, “A scalable, commodity data center network architecture,” ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 4, pp. 63–74, 2008.

[2]. A. K. Atlas and A. Zinin, “Basic specification for IP fast-reroute: Loop-free alternates,” IETF, Fremont, CA, USA, Tech. Rep. RFC 5286, 2008.

[3]. M. Borokhovich, L. Schiff, and S. Schmid, “Provable data plane connectivity with local fast failover: Introducing openflow graph algorithms,” in Proc. ACM SIGCOMM HotSDN, 2014, pp. 121–126.

[4]. M. Borokhovich and S. Schmid, “How (not) to shoot in your foot with SDN local fast failover: A load-connectivity tradeoff,” in Proc. 17th Conf. Princ. Distrib. Syst. (OPODIS), 2013, pp. 68–82.

[5]. M. Canini, P. Kuznetsov, D. Levin, and S. Schmid, “A distributed and robust SDN control plane for transactional network updates,” in Proc. IEEE INFOCOM, Apr./May 2015, pp. 190–198.

[6]. M. Chiesa et al., “The quest for resilient (static) forwarding tables,” in Proc. IEEE INFOCOM, Apr. 2016, pp. 1–9.

[7]. S. Dolev, R. Segala, and A. A. Shvartsman, “Dynamic load balancing with group communication,” in Proc. SIROCCO, 1999, pp. 111–125.

[8]. T. Elhourani et al., “IP fast rerouting for multi-link failures,” in Proc. IEEE INFOCOM, Apr./May 2014, pp. 2148–2156.

[9]. T. Elhourani et al., “IP fast rerouting for multi-link failures,” in Proc. IEEE INFOCOM, Apr./May 2014, pp. 2148–2156.

[10]. G. Enyedi, G. Retvasri, and T. Cinkler, “A novel loop-free ip fast reroute algorithm,” in Proc. Meeting Eur. Netw. Univ. Companies Inf. Commun. Eng. (EUNICE). Cham, Switzerland: Springer, 2007.

[11]. E. Gafni and D. Bertsekas, “Distributed algorithms for generating loop free routes in networks with frequently changing topology,” IEEE Trans. Commun., vol. COM-29, no. 1, pp. 11–18, Jan. 1981.

[12]. P. Gill, N. Jain, and N. Nagappan, “Understanding network failures in data centers: Measurement, analysis, and implications,” ACM SIGCOMM Comput. Commun. Rev., vol. 41, no. 4, pp. 350–361, Aug. 2011.

[13]. P. Hande, M. Chiang, R. Calderbank, and S. Rangan, “Network pricing and rate allocation with content provider participation,” in Proc. IEEE INFOCOM, Apr. 2009, pp. 990–998.