International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-3, Issue-5, May 2017
ISSN: 2395-3470
www.ijseas.com

Demonstrating Cognitive Packet Network Resilience to Worm Attacks

Akhilesh Pandey

MIET College Meerut CS Department Mahamaya Technical University (UP,INDIA)

er.akhil12@gmail.com

Abstract— We discuss a packet network architecture called a cognitive packet network (CPN), in which intelligent capabilities for routing and flow control are moved towards the packets, rather than being concentrated in the nodes and protocols. Our architecture contains "smart" and "dumb" packets, as well as acknowledgement packets. Smart CPN packets route themselves, and learn to avoid congestion and losses from their own observations about the network and from the experience of other packets. They use a reinforcement learning algorithm to route themselves based on a goal function which has been assigned to them for each connection. Dumb CPN packets of a specific quality of service (QoS) class use routes which have been selected by the smart packets (SPs) of that class. Acknowledgement (ACK) packets are generated by the destination when an SP arrives there; the ACK heads back to the source of the SP along the inverse route and is used to update mailboxes in CPN routers, as well as to provide source routing information for dumb packets. We first summarize the basic concepts behind CPN, and present simulations illustrating their performance for different QoS goals, and analytical results for best and worst case performance. We then describe a test-bed network we have designed and implemented in order to demonstrate these ideas. We provide measurement data on the test-bed to illustrate the capacity of the network to adapt to changes in traffic load and to failures of links. Finally, we use measurements to evaluate the impact of the ratio of smart to dumb packets on the end-to-end delay experienced by all of the packets.

.

- ***Keywords***— **Design and performance;**
- **Cognitive packet networks**
- **Smart and dumb packets**

Introduction

PACKET SWITCHING NETWORK WHERE PACKETS ROUTE THEMSELVES

PACKETS ARE ASSIGNED GOALS BEFORE ENTERING THE NETWORK

PACKETS LEARN TO ACHIEVE THEIR GOALS

LEARNING IS PERFORMED BY SHARING INFORMATION BETWEEN PACKETS

PACKETS SHARING SAME GOALS CAN BE GROUPED INTO CLASSES

PACKETS DO NOT RELY ON NODES FOR ROUTING

CPN is designed on behalf of A.I (Artificial Intelligency) by learning of special small packet network that is called smart packets (SP) which probe or analyze the network and make a better path of packet routing. Where SP which are used for discovery, CPN also uses source routed dumb packet "(DP)" to carry the payload (information), and acknowledgement packet to come back information Which has been discovered by Smart packet .That data take back by ACK is used in nodes to train neural networks by using a Reinforcement Learning (RL) algorithm which have a relatively short memory to generate routing decision. The goal of SPs is to see the networking condition and find out the best route, on behalf of quality of goal , for every source-destination pair in networking system . On every hop's SPs are routed on behalf of last packet experience with same source and same task(destination). "goal" is used instead of "Quality of service features" to emphasizes the fact where there are no Quality of service needed and that Cognitive network gives a best effective service .The function of the SP are based on a learning algorithms

In case of to explore all possibles route, at some hop, each

Smart packet makes a random routing decision, with a small probability
(generally 5%). To prevent overburdening the system with unsuccessful request or packet which are in effect lost, all packet have a life-time constraint based on the number of nodes they have explored.
Many algorithm has been used in Cognitive packet networking as learning
and decision technique in order for Smart packet to find best routes from source to destination on behalf of the goals. As long as the decision process is concerned, Random Neural Networks (RNNs) are widely used. This is a biologically
inspired model which is characterized by the existence of positive (excitation) and negative (inhibition) signals in the form of spikes of unit amplitude that circulate between the neurons and alter the potential's of the neurons. Each neuron can be connect to another neuron and each connection is characterized by an excitatory or inhibitory weight .The state of a neuron point , which is represent the possibility that the neuron is excited, and satisfies a system of nonlinear equations with a one such solution. So, in a Cognitive packet networking, at each node a special RNN that have various neurons as the possible outlet link, represents the decision to select a given output link for a Smart packets. The coming of Smart packet awake the execution of Random neural network and the routing decision is the output link according to the most excited neurons.
The reinforcement learning algorithm that was designed into CPN is Reinforcement
Learning (RL); this resulted from prior studies of the routing of autonomous mobile agents in a dangerous landscape . RL is used to change synaptic weights in order to reward or punish a neuron according to the level of goal satisfaction measured on the corresponding output. Therefore the decisional weights of a RNN are increased or decreased based on the observed success or failure of subsequent SPs to achieve the goal. Thus RL will tend to prefer better routing schemes, more reliable access paths and better Quality of services .

The Cognitive packet network has been shown to be effective for a various type of user
uses , including bandwidth & congenstion control power-based routing control in wireless networking and admission control in care of security views , the authors of investigated the application of defense method on the resilience
of the Cognitive packet network against Denial of service attacks.
They introduced a generic framework of DoS protection based on the dropping of probable illegitimate traffic, and presented a mathematical model with which one can measure the impact that both attack and defense have on the performance of a network. Their CPN-based distributed DoS defence technique exploits the
ability of the CPN to trace traffic going both downstream
and upstream, owing to SPs and ACK packets. When a node detects an attack, it uses the ACKs to ask all intermediate
nodes upstream to drop the packets of the attack flow. Every node is allowed to chose the highest bandwidth which it will get from any flow that ends at the hop and the highest bandwidth that it allocates to a flow that traverses the node. These parameters may vary dynamically as a result of other conditions, and they can also be selected based on the identity and the Quality of services needs of the flows. When
a hop gets an Smart packet or Dump packet from a flow that it has not previously
encountered it sends a Flow acknowledgement packet bring back to the source along the reverse path and informs the source of its bandwidth allocation. The node checks the flows which is traverse it and drops packets of any flow that exceeds the allocation;
it can also awake upstream nodes that packet of this flow must be dropped.
Other possible actions include diverting the flow with in a "honeypot" or to a special network.

This generic defense was further improved by using prioritization and rate-limiting instead of simple dropping The same authors has also designed a Denial of services detection method which makes use of on-line statistics collected by the Cognitive packet network protocol's monitoring system and fused them with a Random neural network More analyticallyThis scheme uses input characterstics to immdediately behave and the longer term statistical propertie of the network traffic. IN case of offline information gathering , It gets the probability density function maximum likehood ratios for the input features. When the real time decision are needed it measures the input values find out the the likelihood ratios corresponding to those values and combine that likelihood values using an Random neural network.

The overall architecture give the output in a form of a numerical value which is a
measure of having an on going attack in the network, that is consequently used in the prioritization and rate limiting method

REFERENCES

[1] Z. Chen, L. Gao, and K. Kwiat. Modeling the Spread of Active Worms. In Proceedings of the IEEE INFOCOM 2003, volume 3, pages 1890–1900, San Francisco, CA, USA, Apr. 2003.
[2] S. Dobson, S. Denazis, A. Fern´andez, D. Ga¨ıti, E. Gelenbe, F. Massacci, P. Nixon, F. Saffre, N. Schmidt, and F. Zambonelli. A survey of autonomic communications. ACM Trans. Adapt. Autonomous Systems (TAAS), 1(2):223–259, 2006.
[3] E. Gelenbe. Random Neural Networks with Negative and Positive Signals and Product Form Solution. Neural computation, 1(4):502–510, 1989.
[4] E. Gelenbe. Cognitive Packet Network. US Patent, 6804201 B1, Oct. 2004.
[5] E. Gelenbe. Steps towards self-aware networks. Communications of the ACM, 52(7):66–75, July 2009.
[6] E. Gelenbe, M. Gellman, R. Lent, P. Liu, and P. Su. Autonomous Smart Routing for Network QoS. In Proceedings of the First International Conference on Autonomic Computing (ICAC), pages 232–239, New York, NY, USA, May 2004.
[7] E. Gelenbe, M. Gellman, and G. Loukas. An Autonomic Approach to Denial of Service Defence. In Proceedings of First International IEEE WoWMoM Workshop on Autonomic Communications and Computing (ACC'05), pages 537–541, Taormina, Italy, June 2005.
[8] E. Gelenbe and R. Lent. Power-aware ad hoc cognitive packet networks. Ad Hoc Networks Journal, 2(3):205–216, July 2004.
[9] E. Gelenbe, R. Lent, A. Montuori, and Z. Xu. Towards Networks with Cognitive Packets. In Proceedings of the 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (IEEE MASCOTS), pages 3–12, San Francisco, CA, USA, Aug. 2000. Opening Invited Paper.
[10] E. Gelenbe, R. Lent, A. Montuori, and Z. Xu. Cognitive Packet Networks: QoS and Performance. In Proceedings of the 10th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS'02), pages 3–9, Fort Worth, Texas, USA, Oct. 2002. Opening Keynote Paper. 1http://www.switch.ch/network/
[11] E. Gelenbe, R. Lent, and Z. Xu. Design and Performance of Cognitive Packet Networks. Performance Evaluation, 46(2-3):155–176, Oct. 2001.
[12] E. Gelenbe and G. Loukas. A Self-Aware Approach to Denial of Service Defence. Computer Networks, 51(5):1299–1314, Apr. 2007.
[13] E. Gelenbe and A. Nunez. Traffic Engineering with Cognitive Packet Networks. Simulation Series, 35(4):514–518, Apr. 2003.
[14] E. Gelenbe, G. Sakellari, and M. D' Arienzo. Admission of QoS Aware Users in a Smart Network. ACM Transactions on Autonomous and Adaptive Systems, 3(1):4:1–4:28, Mar. 2008.
[15] E. Gelenbe, E. Seref, and Z. Xu. Simulation with Learning Agents. Proceedings of the IEEE, 89(2):148–157, Feb. 2001.
[16] M. Gellman and P. Liu. Random Neural Networks for the Adaptive Control of Packet Networks. In Proceedings of the 16th International Conference on Artificial Neural Networks (ICANN 2006), pages 313–320, Athens, Greece, Sep. 2006.
[17] G. Loukas and G. Oke. Likelihood Ratios and Recurrent Random Neural Networks in Detection of Denial of Service Attacks. In Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2007), pages 16–18, San Diego, California, USA, July 2007.
[18] G. Oke and G. Loukas. A Denial of Service Detector based on Maximum Likelihood Detection and the Random Neural Network. The Computer Journal, 50(6):717–727, Sep. 2007.
[19] G. Oke and G. Loukas. Distributed Defence Against Denial of Service Attacks: A Practical View. In Proceedings of 1st BCS International Academic Conference, Visions of Computer Science, pages 153–162, London, UK, Sep. 2008.
[20] G. Oke, G. Loukas, and E. Gelenbe. Detecting Denial of Service Attacks with Bayesian Classifiers and the Random Neural Network. In Proceedings of the IEEE International Fuzzy Systems Conference (FUZZ-IEEE 2007), pages 1964–1969, London,UK, July 2007.
[21] G. Sakellari. The Cognitive Packet Network: A Survey. The Computer Journal: Special Issue on Random Neural Networks, doi:10.1093/comjnl/bxp053, June 2009.
[22] P. Su and M. Gellman. Using adaptive routing to achieve Quality of Service. Pe