Design and prototyping of a Software-defined network architecture to detect and prevent real-time botnet attacks (SDNA)

Project Outcome:

In the project, it was envisioned to develop distributed botnet detection and defense system for ISPs, having modules running at customer homes as well as the ISP core, for real time bot detection and fine grained flow blocking. The vision is completely achieved in a pilot deployment. On the non-technical front, the project team established contacts with national & international researchers and industry.

The project also empowered and developed field expertise in undergraduate and post graduate students, which was achieved through rigorous training. The developed system is at a point where it can realistically be further matured for actual deployment, and have filed a patent for the novel technology. All of this has happened on schedule and on budget, without any significant overruns.

The following objectives have been successfully achieved after the completion of the funded project;

- Design a novel software-defined ISP network architecture that will assist in real-time botnet detection
- Quantify the existence and proportion of IRC, HTTP and p2p, based botnets in Pakistan.
- Develop a distributed botnet detection algorithm that can exploit the nature of our proposed SDN architecture and work at line rate to prevent botnet attacks at their source
- Develop a ground-truth on the data-set collected in collaboration with top security researchers at the University of California at Berkeley (UCB)
- Evaluate the proposed architecture and iterate on a prototype solution
- Patent the technology developed in this project.
- Develop a prototype of SDN architecture for Nayatel and deploy it in a pilot project.
- Once the robustness and efficacy of the prototype is validated, the industrial partner will mature the technology and develop a comprehensive solution that can be offered to customers.