5. Results

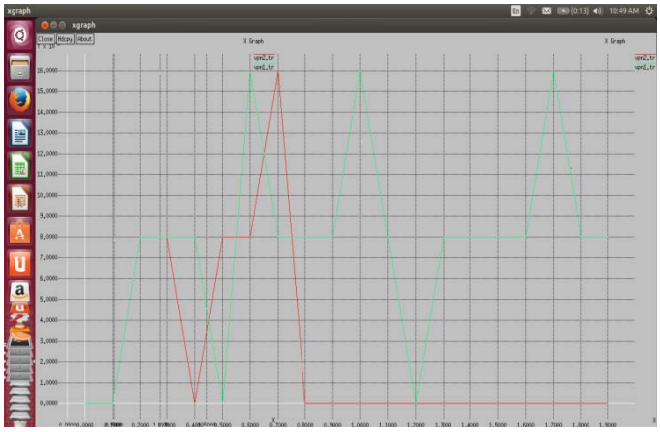

Figure 2: Represent Signal Communication Strength

In Fig. 2: represents signal communication strength here red line is showing strength during attack and green line show after detection the\of attack the lifetime is increased. Here x-axis denotes the time and y-axis denotes iteration of data for the detection of attack. It shows the prevention of the attack on the system. When attack on network (red lines) then original signal strength (green lines) interrupted by attacker's signal strength that make network slow for a while as well as signal also fluctuate because red lines share bandwidth of network though after prevention the green lines strength remain as usual as before attack.

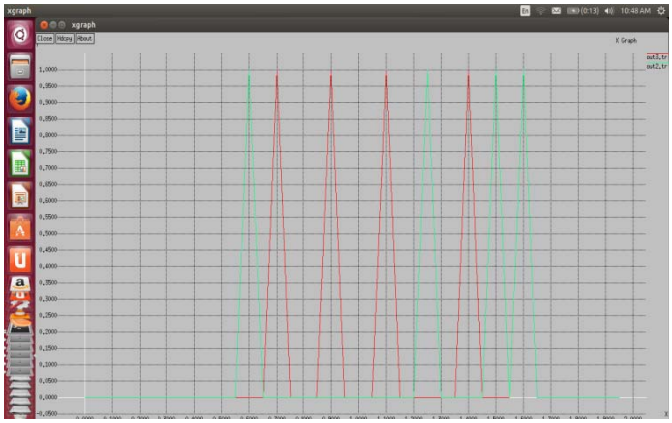

Figure 3: Represent System Distortion

In Fig. 3: the red line is for attack and green line is for detection these two lines show the peak values for the system. In this x-axis shows the time and the y-axis define the distortion occurred in the network and less will be the distortion more reliability is there. When system start up after some time red lines of attack distort the system with its peak value but after prevention the red lines disappear from figure and original system frequency (green lines) retain peak value after neglecting red lines of attack.

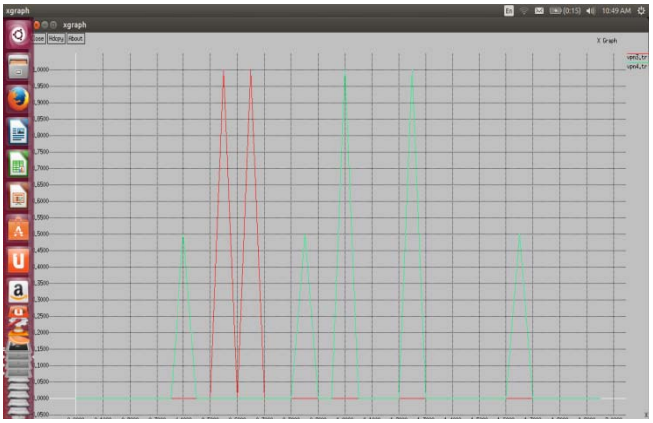

Figure 4: Represent Actual System During and After Attack

In Fig. 4: the red line represent system during attack and green line represent system after attack. Here x-axis shows the time and y-axis shows the performance of the system. In given figure, when system under attack its performance goes down as red lines show where green lines at zero level it original performance at minimum value but after prevention performance of system become reliable because attack performance now at zero level that depicts prevention is done.

6. Conclusion & Future Work

VPN network traffic is controlled by using security algorithm Blowfish and MD5. Blowfish provides a good encryption rate in software and no effective crypt analyzing it has been found till date. Blowfish has a 64 bit block size and variable key length from 32 up to 448 bits and MD5 is message digest having version 5 which is used for encryption procedure. It provide more security to the system. This is implemented by using simulator NS2 and in results various scenarios are discussed and figures are shown during attack, after detection and prevention of attack. These figures conclude that the system become efficient by applying security algorithms.

In future we can make network more reliable with the help of backup node, having address of all nodes available in the network. Whenever a node compromised or detected as a bot then node will be deleted from network. On the place of deleted node, back up node will placed to make network available for communication with interconnect nodes of deleted node.

References

[1] MeisamEslahi, RosliSalleh, Nor BadrulAnuar, "**Bots and Botnets: An Overview of Characteristics, Detection and Challenges**" IEEE International Conference on Control System, Computing and Engineering, pp. 349-354, 23-25 Nov 2012.

[2] Nam-Yih Lee, Hung-Jen Chaing, "**The Research of Botnet Detection And Prevention**" Computer Symposium (ICS), IEEE, pp. 119-124, 16-18 Dec 2010.

[3] M. La Polla, F. Martinelli, and D. Sgandurra, "A **Survey on Security for Mobile Devices**," IEEE Communications Surveys & Tutorials, 2012, doi:10.1109/SURV.2012.013012.00028.

[4] L. Chao, J. Wei, and Z. Xin, "**Botnet: Survey and Case Study**," in Proceedings of the Fourth International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 1184-1187.
[5] ByungHa Choi, Sung-kyo Choi, Kyungsan Cho, "**Detection of Mobile Botnet Using VPN**" Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 142-146, 3-5 July 2013.
[6] N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, "**Botnets: Lifecycle and Taxonomy**," in Proceedings of the Conference on Network and Information Systems Security (SAR-SSI), pp. 1-8, 2011.
[7] M. Chandramohan and H. Tan, "**Detection of Mobile Malware in the Wild**", *Computer*, vol. 45, pp. 65-71, 2012.
[8] Juniper, "**Malicious Mobile Threats Report**" 2010/2011, 2011.
[9] GuiningGeng, Guoai Xu, Miao Zhang, YanhuiGuo, Guang Yang, and Cui Wei, "**The Design of SMS Based Heterogeneous Mobile Botnet**," Journal of Computers, Vol 7,Nno. 1, 235-243, Jan 2012.
[10] Y. Chen, V. Paxson, and R. H. Katz. (2010). "**What's New About Cloud Computing Security?**"[PDF]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf
[11] E. Yuce, "**A Literature Survey About Recent Botnet Trends**," GÉANT Network, ULAKBIM,Turkey, Rep. JRA2 T4, 2012.
[12] M. Feily, A. Shahrestani and S. Ramadass, "**A Survey of Botnet and Botnet detection**," Procs of Third International Conference on Emerging Security Information, Systems and Technologies, pp. 268 - 273 Jun. 2009.
[13] F. Giroire, J. Chandrashekar, Nina Taft, Eve Schooler, and Dina Papagiannaki, "**Exploiting Temporal Persistence to Detect Covert Botnet Channels**," Procs. of the 12th International Symposium on Recent Advances in Intrusion Detection, RAID '09, No. 20, pp. 326-345, 2009.
[14] Byungha Choi, and Kyungsan Cho, "**Detection of Insider Attacks to the Web Server**," Jounal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 3, No. 4, pp. 35-45, 2012.
[15] L. Xie, X. Zhang, J.-P. Seifert, and S. Zhu, "**pBMDS: A Behaviorbased Malware Detection System for Cellphone Devices**," Procs. of the 3rd ACM conference on Wireless Network Security, WiSec Oct. 2010.
[16] A. Bose, X. Hu, K. G. Shin, and T. Park, "**Behavioral Detection of Malware on Mobile Handsets**," in Procs. ofMobiSys, pp. 225 - 238 Jun. 2008.
[17] K. Grewal, and R. Dangi , "**Comparative Analysis of QoS VPN Provisioning Algorithm on Traditional IP based VPN and MPLS VPN using NS-2**," International Journal of Computer Applications, Vol. 48, No.1, pp.43-46, June 2012.