In this article " Security Concerns in MMO Games - Analysis of a Potent Application Layer DDoS Threat " the authors have discussed possible defense mechanisms and flaws for the online attack such as exploiting in-game dependencies between 7 players. The results indicate the need for an adequate DDoS detection system that would 404 consider cooperative player efforts instead of solely relying on inspecting individual actions 405 per player. The review and results need to be improved for acceptance in this journal. The article is based on a review paper and all the suggested results should be analyzed more carefully. There is nothing new about this article in my opinion and all suggestion methods should be improved.

Authors:

The article suggests a possibility of exploiting client dependencies within the server application, which can result in denial of service. We conducted two experiments in a lab to prove our hypothesis. In the first scenario, attackers target the server. In the second scenario, a DDoS attack's target is a client who does not have to possess a public IP address, meaning such vulnerability can affect devices in NAT (Network Address Translation). Moreover, the novelty of this article lies in using graph theory to describe interrelationships between the players by mapping their API calls to a graph to display the affected parties, amplification factors, or other information which is not visible by just observing bandwidth per a connected client. The results show that the performed attacks align with our logical graph's model and that, so far, there is no adequate defense framework. The review and results have been improved accordingly.

We have done our best to correct the grammatical mistakes in the paper. We have relied on the Grammarly service for these corrections.