World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:12, No:03, 2018

# Secure Optimized Ingress Filtering in Future Internet Communication

**Authors :** Bander Alzahrani, Mohammed Alreshoodi

**Abstract :** Information-centric networking (ICN) using architectures such as the Publish-Subscribe Internet Technology (PURSUIT) has been proposed as a new networking model that aims at replacing the current used end-centric networking model of the Internet. This emerged model focuses on what is being exchanged rather than which network entities are exchanging information, which gives the control plane functions such as routing and host location the ability to be specified according to the content items. The forwarding plane of the PURSUIT ICN architecture uses a simple and light mechanism based on Bloom filter technologies to forward the packets. Although this forwarding scheme solve many problems of the today’s Internet such as the growth of the routing table and the scalability issues, it is vulnerable to brute force attacks which are starting point to distributed- denial-of-service (DDoS) attacks. In this work, we design and analyze a novel source-routing and information delivery technique that keeps the simplicity of using Bloom filter-based forwarding while being able to deter different attacks such as denial of service attacks at the ingress of the network. To achieve this, special forwarding nodes called Edge-FW are directly attached to end user nodes and used to perform a security test for malicious injected random packets at the ingress of the path to prevent any possible attack brute force attacks at early stage. In this technique, a core entity of the PURSUIT ICN architecture called topology manager, that is responsible for finding shortest path and creating a forwarding identifiers (FId), uses a cryptographically secure hash function to create a 64-bit hash, h, over the formed FId for authentication purpose to be included in the packet. Our proposal restricts the attacker from injecting packets carrying random FIds with a high amount of filling factor ρ, by optimizing and reducing the maximum allowed filling factor ρm in the network. We optimize the FId to the minimum possible filling factor where ρ ≤ ρm, while it supports longer delivery trees, so the network scalability is not affected by the chosen ρm. With this scheme, the filling factor of any legitimate FId never exceeds the ρm while the filling factor of illegitimate FIds cannot exceed the chosen small value of ρm. Therefore, injecting a packet containing an FId with a large value of filling factor, to achieve higher attack probability, is not possible anymore. The preliminary analysis of this proposal indicates that with the designed scheme, the forwarding function can detect and prevent malicious activities such DDoS attacks at early stage and with very high probability.

**Keywords :** forwarding identifier, filling factor, information centric network, topology manager

**Conference Title :** ICCNS 2018 : International Conference on Cryptography and Network Security

**Conference Location :** Miami, United States

**Conference Dates :** March 12-13, 2018

Open Science Index, Computer and Systems Engineering Vol:12, No:03, 2018 publications.waset.org/abstracts/76680.pdf