World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:07, 2015

Secure Network Coding against Content Pollution Attacks in Named Data Network

Authors : Tao Feng, Xiaomei Ma, Xian Guo, Jing Wang

Abstract : Named Data Network (NDN) is one of the future Internet architecture, all nodes (i.e., hosts, routers) are allowed to have a local cache, used to satisfy incoming requests for content. However, depending on caching allows an adversary to perform attacks that are very effective and relatively easy to implement, such as content pollution attack. In this paper, we use a method of secure network coding based on homomorphic signature system to solve this problem. Firstly ,we use a dynamic public key technique, our scheme for each generation authentication without updating the initial secret key used. Secondly, employing the homomorphism of hash function, intermediate node and destination node verify the signature of the received message. In addition, when the network topology of NDN is simple and fixed, the code coefficients in our scheme are generated in a pseudorandom number generator in each node, so the distribution of the coefficients is also avoided. In short, our scheme not only can efficiently prevent against Intra/Inter-GPAs, but also can against the content poisoning attack in NDN.

Keywords : named data networking, content polloution attack, network coding signature, internet architecture
Conference Title : ICICS 2015 : International Conference on Information and Computer Security
Conference Location : Singapore, Singapore
Conference Dates : July 04-05, 2015