INFORMATION ON DOTORAL DISSERTATION

Title of the thesis: **A solution for fast detecting Hot-IPs in network and Its applications**

Speciality: **Information System**

Code: **62.48.01.04**

Name of the candidate: HUYNH NGUYEN CHINH

Name of the research supervisors:

Supervisor 1: Assoc. Prof. NGUYEN DINH THUC

Supervisor 2. PhD. TAN HANH

Academic institute: Posts and Telecommunications Institute of Technology

THE SCIENTIFIC CONTRIBUTIONS

1. Propose a solution for fast detecting Hot-IPs in network based on Non-Adaptive group testing and some techniques to improve the efficiences. In which, parallel processing technique is used to compute the result vectors in testing groups; using distributed architecture for multi-area networks to early alert from an area to others; and selecting the parameters depending on implemented locations to reduce costs. Basic theory of the proposed solution is codes concatenations used to construct strongly explicit disjunct matrices. Therefore, these matrices do not need to store directly.
2. Propose two new algorithms to detect Hot-IPs online based on the non-adaptive group testing algorithm. In the two new algorithms, groups over threshold will not need to update, list of Hot-IP candicates is identified and initiated with counters. Updating for Hot-IP candicates in this list is executed instead of all counters in the groups of disjunct matrices.
3. Modeling four applications: (1) detecting items may be Internet worms, (2) detecting items may be attackers or victims in denial-of-service attacks, (3) detecting items may be abnormal operation devices, and (4) monitoring Hot-IPs and system resources to manage and limit the operation of Hot-IPs in networks.

APPLICATIONS IN PRACTICE AND OPENED ISSUES FOR FURTHER STUDIES

Applications in practice

Nowadays, forms of network attacks are very popular, especially DoS/DDoS attacks, constructing solutions to detect and limit these attacks are very important. The thesis has proposed the solution to detect items appearing with very high frequency in networks, called Hot-IP, applying on detecting or preventing network attacks such as denial-of-service attacks or propagating Internet worms…Therefore, the thesis can be applied in practice.

Opened issues for further study:

The thesis has presented a completely solution for detecting Hot-IPs in networks and its applications in the field of network security. Beside on applying the solution on real networks, especially implementing in hardwares, further study is analyzing some factors in data streams to recognize and classify threats accurately in networks.

Supervisors **Ph.D. candidate**

NGUYEN DINH THUC TAN HANH HUYNH NGUYEN CHINH