



Computer Engineering Group

Associate Professor Yie-Tarng Chen

Ph.D., Purdue University, U.S.A.

Field of study: Multimedia Networks, High-Speed Backbone Router, and Security in Sensor Networks

Key words: Packet Classification, Sensor Networks

URL: <http://homepage.ntust.edu.tw/YTCHEN/>

Email: ytchen@et.ntust.edu.tw

Phone: 886-2-27376420(voice), 886-2-27376424(Fax)

1. The Subject and Aims of Research

Our researches focus on new technologies to support next-generation networks such as multimedia networks, high-speed backbone router design and security issues in sensor networks.

2. Related Recent Research Topics

A Flexible Service Model for Advance Reservation.

Resource reservation is considered to a promising approach to provide quality of service (QoS) for real-time connections. The reservation can be divided with respect to time when actual resource allocation occurs (1) immediate reservation (2) advance reservation. In advance reservations, optimization of system resources is still an untouched research issue. We propose a flexible reservation model and a request scheduling to tackle this issue. The flexible reservation model introduces a flexible interval for the starting time of the book-ahead request. Therefore, the flexible intervals of book-ahead requests can be represented as a multistage digraph and then the optimal scheduling can be found on the shortest path of the digraph. The results of simulations show significant improvement in terms of the accept ratio for advance requests. One of contributions of this work is to propose an initial look for the optimization of advance reservation systems.

A Novel Signature-based Packet Classification

We develop a novel signature-based packet classification that can achieve gigabit speed at limited memory consumption. The innovative aspect of signature-based scheme is to extract the rule into an equivalent signature, a unique variable-length bit string with shorter width. Therefore, only a small fraction of a rule is inspected in search, resulting in considerable saving in lookup time as well as providing an effective solution for high dimensional rule. Moreover, the signature-based packet classification can perform well at high dimensions. We show that the performance of the signature-based scheme can reach 11 million packets per second even in the worst case, when implemented by 3.96-M 10-ns SRAM for 10000 rule four-dimensional classifier.

An Efficient Packet Classification Algorithm for Network Processors

We propose a novel packet classification algorithm for network processor. A priori knowledge of rules is employed to construct the two-level index tables, the major structure of the packet classification engine. First, a large set of rules is separated into several clusters and rules in different clusters can be searched in parallel. Then, each rule is encoded as a shorter bit string with one-bit trie with bits selection. Finally, all encoded rules are compressed into two-level index tables. In the proposed architecture, packet classification can be completed with two-memory access in index table and one rule comparison under a small memory requirement. We show that the

performance of the proposed algorithm can achieve 8 million packets per second even in the worst-case, when implemented by 549 KB 10-ns SRAM for 20000 four-dimensional rules.

Resilient Key Pre-distribution Scheme for Wireless Sensor Networks

Key management is a challenge issue in Distributed Sensor Networks (DSN) due to ad hoc nature and resource limitations. Many existing encryption schemes such as public-key cryptography are not suitable for resource-limited sensor networks. Recently, the probabilistic key pre-distribution scheme provides an option to address this issue. However, key recovery has not been supported. Based on our observation, probabilistic key pre-distribution scheme cannot operate normally even when 5% of sensors are compromised. We propose a novel snake key pre-distribution scheme with key recovery capability. First, we spread a huge key pool on a two-dimensional key table. Each key in the key table preserves relative information for key encrypting keys (KEKs). When a key is compromised, we can use a suitable KEK in the key table to encrypt a new-generated key message. Furthermore, we take advantage of deployment locality in key pre-distribution to further increase local connectivity ratio. Sensors located in the close region select keys from a subset of the key table.

Selected Publications and Projects

Publications:

1. Yie-Tarng Chen and Kai-Hui Lee "A Flexible Service Model for Advance Reservation." Computer Networks (SCI), Vol. 37, pp.251-262, 2001
2. Yie-Tarng Chen and Shin-Shian Lee "An Efficient Packet Classification Algorithm for Network Processors" IEEE ICC 2003, Anchorage, Alaska, USA on May 11-15, 2003

Projects

1. NSC94-2213-E-011-059 "The Study of Key Pre-distribution Scheme for Distributed Sensor Networks"
- NSC93-2213-E-011-073 "Explore Rule Segmentation in Parallel Packet Classification Algorithm"