



## TECHNOLOGY

# Method for Performance-aware Security of Unicast Communications in Hybrid Satellite Networks

## OVERVIEW

Satellite links suffer from longer propagation delays compared to terrestrial links. Most Internet traffic uses the Transmission Control Protocol (TCP), which is highly susceptible to the delay-bandwidth product and exhibits very poor performance in satellite channels as satellite channels have very high bandwidth. Commercial satellite networks employ HTTP proxy servers, at the central hub and each client location, to improve the speed of response to web browsing requests for Internet traffic. When a remote client makes a request for a webpage, the web server responds with the requested base HTML page. The hub HTTP proxy server performs pre-fetching and forwards the pre-fetched information to the client proxy with the end result that only a single GET request from the user browser traverses the satellite link.

Secure Socket Layer (SSL), a protocol that is widely used in secure web browsing, disables the performance optimization obtained by pre-fetching by the hub proxy server. This is because a HTML webpage encrypted into SSL records is readable only by the client and the web server who have the decryption keys. The keys are not available to the hub HTTP proxy, and therefore the hub HTTP proxy cannot read the HTML webpage and hence, cannot perform pre-fetching. A conventional method tries to overcome this problem by breaking up the end-to-end single SSL connection between client and server into multiple SSL connections. A major drawback of this scheme is that it requires a high level of trust in the intermediate nodes, which might be unacceptable when absolute end-to-end security is desired.

Researchers in the Electrical & Computer Engineering Department at the University of Maryland have developed a novel technique that allows SSL to work in conjunction with TCP and HTTP proxy servers in hybrid satellite networks, so that the unicast communications is secured without sacrificing the performance optimization algorithms.

Advantages: In comparison to traditional SSL, our scheme has:

- Much lower handshake time between the hub HTTP proxy server and the remote client
- Much lower application response time for multiple secure browsing sessions with multiple servers

Applications:

- Secure HTTP unicast communications services

Lead Inventors:

Prof. John Baras, Dr. Ayan Roy-Chowdhury

Stage of Development:

Patent pending

## CONTACT INFO

UM Ventures

0134 Lee Building

7809 Regents Drive

College Park, MD 20742

Email: [umdtechtransfer@umd.edu](mailto:umdtechtransfer@umd.edu)

Phone: (301) 405-3947 | Fax: (301) 314-9502

## **Additional Information**

### **INSTITUTION**

University of Maryland, College Park

### **PATENT STATUS**

Patent(s) pending

### **LICENSE STATUS**

Available for exclusive or non-exclusive license

### **CATEGORIES**

- Microelectronics
- Aerospace
- Information Technology

### **EXTERNAL RESOURCES**

- [US Patent 8,671,273](#)

IS-2008-134