‘On Trustworthy Multicasting in Computer Networks using Softcomputing Tools’

ABSTRACT

Vijay Kumar Nangia
Department of Electrical Engineering,
Faculty of Engineering & Technology,
Jamia Millia Islamia,
New Delhi-110025

ABSTRACT

The Internet has seen tremendous growth in the recent years. Image and text, the traditional data types, no longer dominate the World Wide Web. The emerging applications based on video and audio, demand much higher bandwidth and more stringent latency requirements. Large-scale applications like content delivery and on-line interactive worlds pose serious scalability problems for the Internet. To improve performance of the Internet, the Internet Protocol (IP) Unicast or client-server model has been augmented with Multicast, providing one-to-many and many-to-many delivery mechanisms.

Multicasting has been in existence for more than two decades. Multicasting can be implemented at different layers of the protocol stack. IP multicasting at the network layer has been the research area of major attention from the beginning, It increases bandwidth efficiency, because packets destined to multiple receivers travel only once on common parts of the network. It also reduces server load, as a transmitter sends out packets only once for any number of receivers.

The attention of the most researchers, over the years, has been focused on improving the address allocations, routing protocols, and widespread deployments. With the accelerated expansion of the Internet, however, the scalability in IP multicast has been a matter of concern. Many researchers have considered forwarding state scalability as the most important issue facing IP multicast deployment. The costs of forwarding state come in terms of used up memory at the routers, and processing time and effort of periodic control messages to maintain such state. These costs increase with the number of concurrently active multicast groups in the Internet. Due to such issues and major difficulties in its deployment, the implementation of IP multicasting could never really take off.

The standard Transmission Control Protocol (TCP), where IP multicasting functions, was designed for one-to-one communication and there was tight linking between source and receiver. TCP is thus inherently not appropriate for large-scale applications with many receivers. Amongst the multicasting techniques at alternative layers, potentially the most feasible and favoured technique has been multicasting at the Application Layer, even with its drawbacks like relatively poorer efficiency and security concerns.

While much research effort has been focused towards finding more and more efficient and practical multicasting techniques, with the exponential growth of the Internet in the recent years, an area that is of increasing concern and needing immediate attention, is about the authenticity of its content and the users. Nowadays, cyber-terrorism is a potential threat to organisations and countries that have become more dependent on cyber-space. Securing cyber space is a challenging task. It requires innovative solutions to deal with cyber-terrorism in all its forms and manifestations. One of the manifestations of cyber-terrorism is unauthorised intrusion into the computer systems of an organisation. This unauthorised access has the objective of extracting, modifying or damaging sensitive information. Detecting this threat and responding accordingly require researcher's immediate attention so as to provide proactive solutions.

The threat of cyber attacks and malware is very real and grave. Under the circumstances, it is very important that the access to Internet sites is regulated and user's identity is also protected at the same time. Our research effort has been towards these singular aims i.e.

(a) Establishment of a parameter of trustworthiness in multicasting

(b) To conceal and protect the identity of the users of the computer networks

In our research work, an attempt has been made to establish a parameter of trustworthiness of the users of Internet. The parameter is based on the related attributes for trust, which are fuzzy naturally. A trust value is calculated using the suggested fuzzy equations. The permission given to a user to access is regulated depending upon the trustworthiness ascribed to it as per the computed trust value.

To conceal and protect the identity of the user, is the other important aspect of research that has been vigorously pursued and studied. Following the existing technique of user anonymity in the unicast networks, a new protocol has been proposed by us for the relatively more complex multicast communication. We have called it 'Screened Multicast Protocol' (SMP). An existing and very efficient application layer multicasting protocol Narada, has been used as an example to implement the SMP and has been evaluated for performance for success at concealment of user's identity under different network conditions.