Unit 11

Jonathan Callaghan

Team debate – individual response

Team 1: It is our belief that the future of the Internet is based on content centric networking (CCN &/or NDN or COAST).

Team 2: It is our belief that the future of the Internet is based on peer-to-peer overlay-based networking (BitTorrent, TOR, Freenet, KAD).

Team 3: It is our belief that the future of the Internet is based on the MobilityFirst architecture.

Team 4: It is our belief that the future of the Internet is based on the adoption of IPv6 and the rollout of the associated security measures (DNSSEC, HTTP/3, IPsec, etc.)

Each team **will** make their opening arguments in **support** of their position.

Each **member** should **post at least one argument** for their position.

Team 3: It is our belief that the future of the Internet is based on the MobilityFirst architecture.

Response:

MobilityFirst's key goal is trustyworthiness, with a scalable name service design and Globally Unique Identifier to enhance security. MobilityFirst aims to improve the current internets architecture by allowing resumption of downloads when a device moves and strengthen the mobile and wireless networks.

For security, NetFence is support against DoS attacks by use of networls than end systems.

This adopts caching to achieve high performance on data delivery and with IoT it can lower control overhead with a fair performance and packets success rate. Separation of names and network address for high mobility. (Su et al., 2015) MobilityFirst can easily construct end-to-end communications. (Raychaudhuri et al., 2012)

Counter-response for Team 1's statement (CCN/NDN/COAST):

NDN:

Whilst NDN can eliminate some existing DDoS attack there is scope for new NDN-specific attacks such as interest flooding and content/cache poisoning (Ghali et al., 2014).

There are also privacy concerns as signing data packets supports integrity however trust issues arise and greater research is needed in this area. Key revocation and management are open issues regarding this. Threat actors could infer sensitive information about a user by monitoring its requests.

Data confidentiality is a concern also throuhg caching as data packets cached at routers are available to anyone that reuires for them. User privacy at routers could also be intruded at responses at routers.

NDN does not validate Interest packets and potential DoS attacks are difficult to detect without information about data consumers.

COAST:

COAST has active and passive crawling however a more efficitient discovery mechanism needs to be designed.

Similar to NDN, COAST can have specific DoS attacks.

Host-Oblivious Network Security has a low probability of success in establishing the session key between data consumer and producer.

Too much processing at network nodes, lack of access control and high update overhead. Similar to NDN. Confidentiality as issue and they cannot construct end to end communications. (Ding et al., 2016)

Ding, W., Yan, Z. & Deng, R. H. (2016). A Survey on Future Internet Security Architectures. *IEEE Access,* 4, 4374-4393.

Ghali, C., Tsudik, G. & Uzun, E. Needle in a haystack: Mitigating content poisoning in named-data networking. Proceedings of NDSS workshop on security of emerging networking technologies (SENT), 2014.

Raychaudhuri, D., Nagaraja, K. & Venkataramani, A. (2012). MobilityFirst. *ACM SIGMOBILE Mobile Computing and Communications Review,* 16, (3): 2-13.

Su, K., Bronzino, F., Ramakrishnan, K. K. & Raychaudhuri, D. (2015). *MFTP: A Clean-Slate Transport Protocol for the Information Centric Mobilityfirst Network*. *Proceedings of the 2nd ACM Conference on Information-Centric Networking.* San Francisco, California, USA: Association for Computing Machinery.