CS540 - Paper Review Report # 18

Hailu Belay Kahsay - 20155624

Title: Networking Named Content

Author: Van Jacobson, Diana K. Smetters, James D. Thornton, Michael F. Plass, Nicholas H. Briggs, Rebecca L. Braynard

When computer networks were created in 1960s/70s, they aim to solve the resource sharing , between communicating devices, problem. That is, the construction philosophy and design of today's global computer network focuses on the use of addresses and the transmission control protocol (TCP) to exchange data and share resources among host machines.

Arguing that users care about having content accessible via the Internet and not the locations of the host machines, and to solve availability, security and location-dependency problems, the authors suggest content-centric networking (CCN), a better communication architecture built on named data, for content-based packet transmission.

CCN consists of two types of packets namely:Interest and Data. A customer asks for content by broadcasting its interest packet over all available connectivity. Any node that receives the request and has data that fulfills the query can reply with a data packet. CCN uses content names to connect interest and data packets, which enables multiple nodes to share broadcasts of identical content over a transmission medium. CCN looks up the name of each arriving packet at a node and performs the appropriate action.

In the paper it is explained that, the core CCN packet forwarding engine has three main data structures: [1] Forwarding Information Base: to forward Interest packets toward potential source(s) of matching Data; [2] Content Store: a buffer memory of the arriving data packets exploits the probability of data sharing, which reduces downstream delay and the demand for upstream bandwidth; and [3] Pending Interest Table: keeps track of Interests forwarded upstream toward content source(s) so that returned Data can be sent downstream to its requester(s). CCN maintains local communication and a flow balance of packets at each hop. CCN transport is designed to operate on top of unreliable packet delivery services, including the highly dynamic connectivity of mobile and ubiquitous computing. To provide reliable, resilient delivery, CCN Interests that are not satisfied in some reasonable period of time must be retransmitted (by receiver's strategy layer).

The authors discuss the implementation of and performance results from a prototype CCN network stack and demonstrated its usefulness for both content distribution and point-to-point network protocols. Its data transfer efficiency was analogous to that of TCP. It remained constantly effective in distributing multiple copies of a large data file over a network. VoIP on top of the prototype system showed no packet lost due to link connection failures.

The CCN paradigm represents a remarkable call for a shift away from the traditional TCP/IP. CCN is different from the traditional IP in its optimal strategic choice among alternative multiple connections in the dynamic Internet environment. The authors design a content-based security system to replace the IP network stack. The system offers the protection of and trust in the content for retrieval over the Internet. In the model, private content can be encrypted and all content is digitally signed. Moreover, all routing and policy information can be authenticated to help combat network attacks such as spoofing, flooding, and tampering. With today's ever-increasing activities over social Websites, the content distribution effectiveness of CCN is valuable.

Discussion points:

- Though CCN uses content-based security (digital signatures and encryption) but it still is vulnerable to denial of service attack.
  - Hiding legitimate content
  - Flooding Interest packets
- Computational requirement of CCN nodes?
- Stakeholders willingness to accept CCN over existing TCP/IP architecture?

CS540 - Paper Review Report # 18

Hailu Belay Kahsay - 20155624

Title: VANET via Named Data Networking

Author: Giulio Grassi, Davide Pesavento, Giovanni Pau, Rama Vuyyuru, Ryuji Wakikawa, Lixia Zhang

VANET is the technique that uses moving vehicles, that are equipped with a variety of wireless communication interfaces such as 3G/LTE, WiMAX, WiFi, IEEE 1901 (Power Line Communication), and 802.11p (DSRC/WAVE), as wireless nodes in a mobile network. Using any and all of these interfaces a car should be able to communicate with either infrastructure servers or other vehicles as needed by applications. Whenever more than one interface is available, the vehicle should be able to pick and choose the best one or use multiple in parallel. And each wireless node takes a role as an end-user and wireless router to create a wide range communication.

Even though numerous vehicles are connected to Internet today, due to the fact that they are mainly connected via cellular networks only and Vehicle-to-Vehicle (V2V) communication usage is limited to one-hop communication, VANETs is not popular. To address these problems the authors proposed Vehicular Named Data Networking, by inheriting the basic principle of the NDN to VANET.

The authors argue that V-NDN, by naming data rather than hosts and decoupling communication from specific interfaces and IP addresses, can bring substantial benefits to vehicular communication: it enables vehicles to utilize any available interfaces and fetch data from any of the available nodes, it removes the isolation between applications and network transport, allowing forwarding nodes to handle data based on application needs.

In the paper, NDN model basics: NDN naming, its main entities with their functionalities and how NDN operates; and the modifications needed to the baseline NDN operations to accommodate VANET specific features, such as Opportunistic caching strategy (for rapid data dissemination), spreading content to wider area (via mules, moving cars while carrying data) and routing issues(interest packet forwarding), are discussed. Naming data also enable mules to cache it, making V-NDN resilient to connectivity disruptions that characterize vehicular networks: even when the communication between consumer and producer is interrupted, mules can bring the required data to the consumer over time. Design and Implementation of V-NDN prototype under Ubuntu Linux 12.04 LTS also is included in the paper.

Discussion points:

- Privacy and Trust management issues?
- Killer Application?
- Strategies for scalable namespace design?
    - Application's data, communication, and storage models with the routing and security implications of names in NDN
- Development and integration of high-performance cryptographic algorithms?
- social impacts of NDN: data retention policy and content regulation?