Named Data Networking

Abstract— **Named Data Networking (NDN) is a proposed Internet architecture that shifts the network communication model from delivering packets to IP addresses to collecting data packets by names. As a result of the architectural change, host functions and initial configurations are altered. We offer an overview of the essential functions of a host in an NDN network, as well as the actions required to configure an NDN host, in this paper. We also contrast the functioning and setup of an NDN and an IP host to demonstrate the variations that come from the different architectural designs.**

I. INTRODUCTION

Named Data Networking (NDN) is a new future Internet Architecture that has no dependency on IP. NDN architecturehas an hourglass shape with an NDN layer as the narrow waist. It can send datagrams and follows the end-to-end prin- ciple which can assert the information pushed into one end of the Internet can come out the other end without modification. Although IP and NDN seem to have commonalities there are major differences between them. The IP address can define "where" the location is and all the devices find, send, and exchange information with other connected devices using this protocol. However, Named Data Networking (NDN) can embed name into the routing instead of using IP and Domain Name System (DNS). Today all the naming is done through DNS. DNS translates a name into an IP address and routing is done based on IP addresses. So instead of using IP, we're looking at NDN which deals with a different perspective of networking the world of computing devices. With NDN, we are managing the routing and security natively with names while getting rid of the IP addresses. NDN names data instead of data locations. NDN consumers fetch data instead of senders pushing packets to destinations. NDN is especially suitable for emerging applications environments that include mobile edge computing, Internet of Things (IoT), and Low Latency Applications such as interactive Augmented Reality/Virtual Reality.

II. MOTIVATION AND NEED

As the Internet became the world's storefront, almost all the services are available online. We made it easy for anyoneto discover, consume, and create content, exabytes of new content is being produced and distributed yearly. Because of this, IP despite being designed for the conversations between communicating endpoints. The increasing user demands or seamless communication on the move brings about new challenges that stress the current Internet, originally designed to support communication between fixed end-points. On the other side, NDN directly retrieves the objects by name in a secure, reliable, and efficient way. The prime objective is to secure information from the users to the data and not just from the host or client-server communication, which transport layer security (TLS) normally does. Unlike TLS, which carries users to the host or container, NDN takesus to the next level and secures data from the user to the actual data. TLS only encrypts the channel and doesnot encrypt from the user through the application to the data. The main advantage of NDN is that it can be layered over anything, including IP itself. Our motivation is the architectural mismatch of today's Internet architecture and its usage. Specifically today we build, support, and use Internet applications and services on top of an extremely capable architecture not designed to support them. But, whatif we had an architecture designed to support them? For example, NDN can tell if all the data on the web page one is viewing was produced and signed by one's bank. Whereas, IP cannot do this. As all applications can benefit from running over NDN networks. NDN names data instead of locations, removing a major obstacle in supporting mobility in TCP/IP networks. NDN enables in-network storage because data can stand alone, enabling scalable and robust data dissemination.

III. PROBLEM DEFINITION

Securing contents themselves in NDN is more important than protecting the infrastructure of the network. In NDN, content security is a challenge since there exist several security concerns of NDN content including naming-related attacks, caching-related attacks, routing-related attacks, and other attacks. NDN is a promising protocol that can help to reduce congestion at the Internet scale by putting contentat the center of communications instead of hosts, and by providing each node with a caching capability. NDN can also natively authenticate transmitted content with a mechanism similar to website certificates that allow clients to assess the original provider. But this security feature comes at a high cost, as it relies heavily on asymmetric cryptography which affects server performance when NDN Data is generated. If a testbed has 14 server cores that can only generate 400 Mbps of new NDN Data with default packet settings, we have to propose and evaluate practical solutions to improve the performance of server-side NDN Data generation thatcan lead to significant gains.

IV. RESEARCH TASK

Most research papers have focused on NDN caching performance evaluation but none of them considered the per- formance of NDN Data packets generation while this is also of prime importance for the mentioned applications. We can give the first comprehensive evaluation of NDN throughput at the server-side while measuring the CPU consumption

under different scenarios using NDNperf, which is an open-source tool for NDN performance evaluation we made. NDN server-side performance evaluation and sizing purposes, to have an idea of the throughput a server can achieve when it has to generate and transmit NDN Data packets. NDN is capable of providing at least comparable content distribution functionality as another content distribution method, it is important to improve the system performance. In particular, the capability to show that one of our simple changes in the source code could almost double the forwarding node throughput. One option is to use multiple parallel paths only when needed. Another approach is to proactively split traffic along multiple paths so that a router can get feedback on data-plane performance from all the multiple paths, and if a failure occurs, it may affect only a small portion of the traffic. The two approaches are not exclusive of each other, and we investigate both. The new communication model of NDN must contain not only transmission but also storage, which requires a new fundamental theory of communication. In all of these areas, investigation of new evaluation methodologies to gauge the correctness and effectiveness of the NDN design is crucial. We can also plan to explore practical applications of group signature schemes for signature privacy, where any member of a group can sign on behalf of the group, and anyone can verify a group signature, but the identity of the signer remains private and no connection can be made between multiple group signatures. We need to ex- plore obtaining at least some of the appealing features of group signatures at acceptable (i.e., lower) costs. (This might require deconstructing group signature schemes to come up with derivatives offering somewhat weaker privacy properties but at lower cost). Group signatures can also be used in combination with ephemeral keys, where "expensive" group signatures are used to delegate trust to ephemeral keys used to sign content.

V. IMPLEMENTATION DETAILS

The purpose of this project is to build a performance model for our analysis. We need to consider a network topology that has a consumer i.e traffic generator client, a forwarder (NDN-DPDK), and a producer i.e traffic generator server, arranged in a linear pattern. We want to work for a periodic report of performances such as end-to-end throughput, latency, and processing time. Working on Fresh NDN Data generation or NDN Data delivery from caches to make the content directly addressable. Also, the implemented codebase should be able to use all available signatures implemented in the NDN library, with the chosen size of the key, and the transmission size of Data packets is also very important. With NDN, we can manage routing and security using names instead of IP addresses. It has its routing protocol. Link state routing is one of the routing protocols it uses. It's open-source software that you may download as an instance to operate on a virtual server, an iOS device, or an Android device. At the same time, having IP with NDN is still possible.

VI. PERSPECTIVES

The ability to build a lot of the next-gen applications is better supported with this Named Data Networking architecture. For the situations where we need to implement reverse multicasting a video in your device that you want it to go to one lakh people at once. Then the only way is to opt for a forwarding channel such as YouTube or Twitter. Whereas with NDN we can directly transmit through the interest model. When the node receives an interest packet, it initially searches for the name of the requested content in its Content Store, and this is how we can utilize the interest packet. Also with NDN, we can have data in a lot of different locations and we don't have to tie the application or instance to a specific IP address. NDN is capable of making data itself identifiable, independent from its containers or channels and this requires the data to be secured directly.

REFERENCES

1. V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs, and R. Braynard, "Networking Named Content," in Proc. of CoNEXT, 2009.
2. L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, kc claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named Data Networking,"ACM Computer Communication Review, July 2014.
3. Khoussi,S.,Nouri,A.,Shi,J.,Filliben,J.,Benmohamed,L.,Battou,A.,Bensalem , S.: Performance evaluation of a NDN forwarder using statistical model checking. CoRR abs/1905.01607 (2019), http://arxiv.org/abs/1905.01607
4. Jacobson,V.,Smetters,D.K.,Thornton,J.D.,Plass,M.F.,Briggs,N.H.,Braynard, R.L.: Networking Named Content (2009), https://named-data.net/wp-content/ uploads/Jacob.pdf
5. Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, and L. Zhang, "An overview of security support in Named Data Networking," NDN, Technical Report NDN-0057, Apr. 2018.
6. M. Zhang, V. Lehman, and L. Wang, "Scalable Name-based Data Syn- chronization for Named Data Networking," in Proc. of IEEE INFOCOM, 2017.
7. G.LiuandA.Afanasyev,"NDN-FCH(findclosesthub),"https://github.com/named-data/ndn-fch, 2018.
8. NDN Project Team, "Local hub prefix discovery," https://named-data.net/doc/NFD/current/local-prefix-discovery.html, 2018.
9. Y. Li, A. Afanasyev, J. Shi, H. Zhang, Z. Zhang, T. Li, E. Lu, B. Zhang, L. Wang, and L. Zhang,"NDNautomatic prefix propagation," NDN, Technical Report NDN-0045, March 2018.
10. NDN Project Team, "Readvertise end-host routes into NLSR," https: //redmine.named-data.net/issues/3818, 2017.
11. Z. Zhang, Y. Yu, A. Afanasyev, and L. Zhang, "NDN certificate management protocol (NDNCERT), NDN, Technical Report NDN-0050, Apr. 2017.
12. "Internet Protocol," J. Postel, Ed., September 1981. .
13. Mediouni, B.L., Nouri, A., Bozga, M., Dellabani, M., Legay, A., Bensalem, S.: SBIP 2.0: Statistical model checking stochastic real-time systems. In: Automated Technology for Verification and Analysis - 16th International Symposium, ATVA 2018, Los Angeles, CA, USA, October 7-10, 2018, Proceedings. pp. 536–542 (2018)
14. Named data networking project. Tech. rep., USA (Oct 2010), http:// named-data. net/techreport/TR001ndn-proj.pdf
15. Nouri, A.: Rigorous System-level Modeling and Performance Evaluation for Em- bedded System Design. Ph.D. thesis, Grenoble Alpes University, France (2015)
16. Nouri, A., Bensalem, S., Bozga, M., Delahaye, B., Jegourel, C., Legay,A.: Statis- tical model checking QoS properties of systems with SBIP. Int. J. Softw. Tools Technol. Transf. (STTT) 17(2), 171–185 (April 2015)
17. L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. Thornton, D. Smetters, B. Zhang ,G. Tsudik , kc claffy, D. Krioukov, D. Massey, C. Papadopoulos, T. Abdelzaher, L. Wang, P. Crowley, E.Yeh. Named Data Networking (NDN) Project. Technical Report NDN-0001, October 2010.