International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Special Issue 3, October 2020 ||

Lightweight Signature Based Capability Management in Named Data Networking

Asst. Prof . Jensy Varghese, Asst. Prof. Yasir Moidutty

Assistant Professor, Department of Computer Science Engineering, Royal College of Engineering and Technology Thrissur, Kerala India

Assistant Professor, Department of Electronics and Communication Engineering, Royal College of Engineering and Technology, Thrissur, Kerala India

ABSTRACT: Named Data Networking (NDN) [1] is a content-based network architecture that delivers packets referenced by location in dependent content names, as opposed to packet addresses as in traditional IP networks. NDN interconnects users and content providers (CPs) through a set of content routers [2]. It also supports in-network caching, such that content may be available at a CP or cached in the routers. NDN is an entirely new architecture, but one whose design principles are derived from the successes of today's Internet, reflecting our understanding of the strengths and limitations of the current Internet architecture, and one that can be rolled out through incremental deployment over the current operational Internet [3]. Today's Internet's hourglass architecture centers on a universal network layer, which implements the minimal functionality necessary for global interconnectivity. This thin waist enabled the Internet's explosive growth by allowing both lower and upper layer technologies to innovate independently without unnecessary constraints [4]. NDN architecture retains the same hourglass shape, but transforms the thin waist to focus on data directly rather than its location [5]. More specifically, NDN changes the semantic of network communication from delivering a packet to a given destination address to retrieving data identified by a given name..

KEYWORDS: spammer, machine learning, support vector machine,random forest

I. INTRODUCTION

Named Data Networking (NDN) [1] is a content-based network architecture that delivers packets referenced by location in dependent content names, as opposed to packet addresses as in traditional IP networks. NDN interconnects users and content providers (CPs) through a set of content routers [2]. It also supports in-network caching, such that content may be available at a CP or cached in the routers. NDN is an entirely new architecture, but one whose design principles are derived from the successes of today's Internet, reflecting our understanding of the strengths and limitations of the current Internet architecture, and one that can be rolled out through incremental deployment over the current operational Internet [3]. Today's Internet's hourglass architecture centers on a universal network layer, which implements the minimal functionality necessary for global interconnectivity. This thin waist enabled the Internet's explosive growth by allowing both lower and upper layer technologies to innovate independently without unnecessary constraints [4]. NDN architecture retains the same hourglass shape, but transforms the thin waist to focus on data directly rather than its location [5]. More specifically, NDN changes the semantic of network communication from delivering a packet to a given destination address to retrieving data identified by a given name..

Security [6] must be built into the architecture. Security measures in the current Internet architecture are an afterthought which does not meet the demands of today's diverse environment. NDN provides a fundamental security building block right at the thin waist by signing all named data. NDN retains and expands this principle by securing data end-to-end. Network traffic [7] must be self-regulating. Flow-balanced data delivery is essential to the stability of large systems. Unlike IP's open-loop packet delivery, NDN designs a flow-balance feedback loop into the thin waist. The architecture should facilitate user choice and competition wherever possible. Although not considered in the original Internet design, global deployment has taught us that "architecture is not neutral." NDN makes a conscious effort to empower end users and facilitate competition. Communication in NDN is driven by the receiving ends, i.e., the data consumers, through the exchange of two types of packets: Interest and Data [8]. Both types of packets carry a name that identifies a piece of data that can be transmitted in one Data packet. To receive data, a consumer puts the name of desired data into an Interest packet and sends to the network. Routers use this name to forward the Interest toward the data producer(s) [9]. Once the Interest reaches a node N that has the requested data, node N will return a Data packet that contains both the name and the content, together with a signature by the producer's key which binds the two. This Data packet follows in reverse the path taken by the Interest to get back to the requesting consumer [10].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Special Issue 3, October 2020 ||

Security can no longer be tied to a content location or to a particular host. Therefore, a content oriented security model is adopted. According to NDN, robust security model requires the following security services are [11]-[13],

1. Validity: there is no change in the data or in the correspondence between the name and its content (authenticity).
2. Provenance: data are published by an appropriate publisher in measure to produce these contents.
3. Relevance: data represents the answer to a question posed by the receiver.
4. Access control: the access to data is limited to authorized entities.
5. Confidentiality: data are readable only by authorized entities.

Naming plays a critical role in security [14]. Indeed, to ensure security services, certain requirements must be satisfied. For data integrity, the name should establish a binding between the name and the publisher's public key [15]. To ensure data authenticity, the name should establish a binding with the content. This is ensured, in NDN, by the digital signature linking the name to its content. To verify the provenance, three potential bindings should be ensured are a binding between the publisher real-world identity and the name, a binding between real-world identity and the publisher public key and a binding between the publisher public key and the name [16]. Bindings are transitive, providing any two of them implies the third one. Finally, to ensure pertinence, the name should be human-readable and meaningful. An intelligent content discovery system to fully utilize the cache resources (DENA) [17] is used to encompass the deep exponential network-based cache announcement, cache energy-based cache replacement. Stochastic adaptive forwarding (SAF) [18] imitates water-pipe system, intelligently guiding and distributing interests through network crossings circumventing link failures and bottlenecks. Just as real pipe systems, SAF uses overpressure valves enabling congested nodes to lower pressure autonomously. Named-data network utility maximization (NDNUM) [19] used to maximize the data receiving rate related network utility minus power consumption while consider NDN's communication characteristics that are different from IP. Bloom filter aided hash table (BFAST) [20] is designed based on a basic hash table, it employs a counting Bloom filter to balance the load among hash table slots, so that the number of items in each non-empty slot is close to1,leading to low searching time in each lot.

II. RELATED WORK

Yan et al. [21] have proposed a hybrid content naming and ad dressing scheme with the content management architecture for high scalability and security. It utilizes the domain name system (DNS) to limit the signaling cost in the NDN operation, including the content retrieval and provider mobility. The content naming and addressing scheme utilizes the DNS and its extension protocols for higher scalability and security of content publishing and retrieving in NDN. The scheme used to build a comprehensive security chain for the content publishing and retrieving.

Rehman et al. [22] have proposed a location-aware on-demand multipath caching and forwarding (LOMCF) for NDN-based MANETs. It is assumed that all the participating nodes can access their current location information at any time using any external service such as the global positioning system (GPS). LOMCF protocol considers the node's current location in its packet forwarding mechanism. The packets follow multiple routes. Consequently, high reliability in packet transmission is achieved especially in dynamic MANET's environment. LOMCF protocol by utilizing the distance-based caching policy, the contents are stored near to the consumer nodes which further reduce the content retrieval time for the future requests. LOMCF protocol takes the remaining energy of the node into account that improves the node as well as network performance.

Rehman et al. [23] have proposed on-demand energy-based forwarding strategy (OEFS), which takes the node's residual energy into account before sending packets. OEFS considers the residual energies of the nodes in its communication process. Its energy-based forwarding mechanism enhances node lifetimes as well as network performance. When nodes are in Danger States, they focus more on the delivery of Data packets to satisfy the pending requests of their neighbor nodes. To mitigate packet collisions, it reduces the Interest and Data packet flooding in the networks.

Kim et al. [24] have investigated the problem of content poisoning attack in NDN and presented an effective solution to this problem. In terms of mathematical analyses and simulation studies, this scheme saves a large amount of computational resources by avoiding meaningless verification for by-passing content and by favoring 'already verified content'. Nevertheless, malicious effects from poisoned content in the CS are perfectly prevented. The potential drawbacks of the proposed scheme such as the increased access latency and verification attack. Hence, when content

arrives at the router, it consumes the pending entry if both the content name and faces are successfully matched. It is worth noting that checking the incoming face of content is necessary only at the edge router that is directly connected to the end-hosts.

Wang et al. [25] have proposed named-data link state routing protocol (NLSR) for intra-domain routing in NDN. It is an application level protocol similar to many IP routing protocols, but NLSR uses NDN's Interest/Data packets to disseminate routing updates, directly benefiting from NDN's built-in data authenticity. The NLSR design, which was first developed in 2013 and deployed on the NDN test bed in August 2014, has undergone significant changes. Following an application-driven design approach, NLSR's development helped drive the development of the trust/security functionality of NDN libraries as well as a number of features in NFD and ChronoSync.

Torres et al. [26] have a controller based routing scheme (CRoS) that runs on top of NDN and, thus, preserves all NDN features using the same interest and data packets. CRoS adds router actions and avoids control message overhead by coding signaling information on content names. The scheme enables data mobility and avoids the replications of routing information from controller to routers because they request the routes on-demand. CRoS requires low router memory size because it stores only the routes for simultaneously consumed prefixes. The scheme automates router provisioning and efficiently installs a new route, on all routers, in a path with a single route request to controller.

Ndikumana et al. [27] have proposed an incentive mechanism, where the internet service providers (ISP) generate revenue from caching by selling cached contents to its customers. Then, price-based cache replacement policy (PBCR) is used as cache replacement policy for paid content, where PBCR triggers the content needs to be replaced when the cache storage is full. An incentive mechanism used to improves the ISP's profits via the use of auction theory. The ISP earns profits from caching by alleviating the volume of transit traffic and selling cached contents to its customers, where the contents are from multiple CPs. An incentive mechanism encourages the ISP and CPs to be truthful when participating in the designed auction, through the Vickrey-ClarkeGroves (VCG) approach.

Yao et al. [28] have discussed the problem of content request forwarding in the context of NDN is naturally formulated as a semi-Markov decision problem (SMDP). Since the exact SMDP solution is intractable, a variant of reinforcement learning (RL) method integrated with function approximation by neural networks is developed to find the optimal solution for SMDP abstract. A broad set of experimental comparisons was carried out to verify the effectiveness of the resulting forwarding strategy. The results show that the RL method provides an efficient solution to our SMDP-based forwarding model and approach can further enhance network performance in comparison to existing forwarding strategies by reducing rejection ratio, network load, as well as delivery time.

III. PROBLEM METHODOLOGY

Li et al. [29] have capability-based security enforcement architecture (CSEA), a capability-based security enforcement architecture that enables data authenticity in NDN in a distributed manner. CSEA leverages capabilities to specify the access rights of forwarded packets. It allows NDN routers to verify the authenticity of forwarded packets, and throttles flooding-based DoS attacks from unsolicited packets. Further develop a lightweight one-time signature scheme for CSEA to ensure the timeliness of packets and support efficient verification. The prototype CSEA on the open-source CCNx platform, and evaluate CSEA via test bed and Planet lab experiments.

As far as security is concerned, IP networks and CDNs behave much the same way. Alternatively, the named data network (NDN) approach offers a way to distribute data more securely and efficiently. NDN, data traveling through the network is digitally signed by the sender. Security has always been an afterthought in IP networks, whereas it is built into the NDN model. The most crucial security aspect of the NDN is that every data packet is cryptographically signed by the producer's key. Each data packet contains a signature over the name and the message or payload. It also contains information about the key used to verify the signature. NDN design requires mandatory digital signatures for all data packets, which can leverage to verify the integrity and authenticity of the data packets by routers and end users. The lightweight one-time signature scheme used to ensure timeliness of packets in CSEA [29]. From these, security issues have not been fully addressed by existing NDN architecture. The open issues fall mainly within two categories is privacy and trust.

Contributions.

For this reason, a lightweight signature based capability management (LSCM) is proposed to further enhance security in NDN. It requires signing every data packet, enabling consumers to verify each incoming Data's signature, hence ensuring data authenticity and integrity. In LSCM, we propose a cryptographic hash function based on sponge functions, which generate hash codes of arbitrary length. Applications define trust degree is required to determine whether a given packet or identity is trustworthy or not. The trust degree of data packets is compute by an optimal decision making (ODM) algorithm, which shows the packet's trustworthiness before cryptographic signature verification. Moreover, we focus on three specific attacks are content poisoning, DoS and content leakage. In order to study the performance of the proposed LSCM technique, several simulations have been performed in the NS2 environment. The simulation results show that the performance of proposed LSCM technique is very efficient in terms of high secure and low overhead compare to CSEA technique.

REFERENCES

[1]D. Corujo, R. Aguiar, I. Vidal and J. Garcia-Reinoso, "A named data networking flexible framework for management communications", IEEE Communications Magazine, vol. 50, no. 12, pp. 36-43, 2012.
[2]W. Quan, C. Xu, J. Guan, H. Zhang and L. Grieco, "Scalable Name Lookup with Adaptive Prefix Bloom Filter for Named Data Networking", IEEE Communications Letters, vol. 18, no. 1, pp. 102-105, 2014.
[3]"NETWRAP: An NDN Based Real-TimeWireless Recharging Framework for Wireless Sensor Networks", IEEE Transactions on Mobile Computing, vol. 13, no. 6, pp. 1283-1297, 2014.
[4]Rao Ying, Luo Hongbin, Gao Deyun, Zhou Huachun and Zhang Hongke, "LBMA: A novel Locator Based Mobility support Approach in Named Data Networking", China Communications, vol. 11, no. 4, pp. 111-120, 2014.
[5]K. Kaur and S. Kad, "A Study of Vehicular Information Network Architecture based Named Data Networking (NDN)", International Journal of Computer Applications, vol. 140, no. 6, pp. 34-39, 2016.
[6]"Securing building management systems using named data networking", IEEE Network, vol. 28, no. 3, pp. 50-56, 2014.
[7]M. Lhogeshvaree, "LIVE: Lightweight Integrity Verification for Named Data Networking", International Journal Of Engineering And Computer Science, 2016.
[8]R. Xie, Y. Wen, X. Jia and H. Xie, "Supporting Seamless Virtual Machine Migration via Named Data Networking in Cloud Data Center", IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 12, pp. 3485-3497, 2015.
[9]J. Luo, C. Wu, Y. Jiang and J. Tong, "Name Label Switching Paradigm for Named Data Networking", IEEE Communications Letters, vol. 19, no. 3, pp. 335-338, 2015.
[10]X. Lin, J. Liu and S. Gritzalis, "Security and privacy in emerging information technologies", Security and Communication Networks, vol. 5, no. 1, pp. 1-2, 2011.
[11]S. Bouk, S. Ahmed, M. Yaqub, D. Kim and M. Gerla, "DPEL: Dynamic PIT Entry Lifetime in Vehicular Named Data Networks", IEEE Communications Letters, vol. 20, no. 2, pp. 336-339, 2016.
[12]K. Ohsugi, J. Takemasa, Y. Koizumi, T. Hasegawa and I. Psaras, "Power Consumption Model of NDN-Based Multicore Software Router Based on Detailed Protocol Analysis", IEEE Journal on Selected Areas in Communications, vol. 34, no. 5, pp. 1631-1644, 2016.
[13]Q. Chen, R. Xie, F. Yu, J. Liu, T. Huang and Y. Liu, "Transport Control Strategies in Named Data Networking: A Survey", IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2052-2083, 2016.
[14]H. Guo, X. Wang, K. Chang and Y. Tian, "Exploiting Path Diversity for Thwarting Pollution Attacks in Named Data Networking", IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2077-2090, 2016.
[15]B. Rainer, D. Posch and H. Hellwagner, "Investigating the Performance of Pull-Based Dynamic Adaptive Streaming in NDN", IEEE Journal on Selected Areas in Communications, vol. 34, no. 8, pp. 2130-2140, 2016.
[16]J. Pan, S. Paul and R. Jain, "A survey of the research on future internet architectures", IEEE Communications Magazine, vol. 49, no. 7, pp. 26-36, 2011.
[17]H. Zhang, R. Xie, S. Zhu, T. Huang and Y. Liu, "DENA: An Intelligent Content Discovery System Used in Named Data Networking", IEEE Access, vol. 4, pp. 9093-9107, 2016.
[18]D. Posch, B. Rainer and H. Hellwagner, "SAF: Stochastic Adaptive Forwarding in Named Data Networking", IEEE/ACM Transactions on Networking, vol. 25, no. 2, pp. 1089-1102, 2017.
[19]C. Li, R. Xie, T. Huang and Y. Liu, "Jointly Optimal Congestion Control, Forwarding Strategy and Power Control for Named-Data Multihop Wireless Network", IEEE Access, vol. 5, pp. 1013-1026, 2017.
[20]H. Dai, J. Lu, Y. Wang, T. Pan and B. Liu, "BFAST: High-Speed and Memory-Efficient Approach for

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Special Issue 3, October 2020 ||

NDN Forwarding Engine", IEEE/ACM Transactions on Networking, vol. 25, no. 2, pp. 1235-1248, 2017.
[21]Z. Yan, J. Lee, X. Lee and Y. Park, "Utilizing the Domain Name System for Scalable and Secure Named Data Networking", Wireless Personal Communications, vol. 84, no. 3, pp. 2135-2149, 2015.
[22]R. Rehman and B. Kim, "LOMCF: Forwarding and Caching in Named Data Networking Based MANETs", IEEE Transactions on Vehicular Technology, vol. 66, no. 10, pp. 9350-9364, 2017.
[23]R. Rehman, S. Ahmed and B. Kim, "OEFS: On-Demand Energy-Based Forwarding Strategy for Named Data Wireless Ad Hoc Networks", IEEE Access, vol. 5, pp. 6075-6086, 2017.
[24]D. Kim, J. Bi, A. Vasilakos and I. Yeom, "Security of Cached Content in NDN", IEEE Transactions on Information Forensics and Security, vol. 12, no. 12, pp. 2933-2944, 2017.
[25]L. Wang, V. Lehman, A. Mahmudul Hoque, B. Zhang, Y. Yu and L. Zhang, "A Secure Link State Routing Protocol for NDN", IEEE Access, vol. 6, pp. 10470-10482, 2018.
[26]J. Torres, I. Alvarenga, R. Boutaba and O. Duarte, "An autonomous and efficient controller-based routing scheme for networking Named-Data mobility", Computer Communications, vol. 103, pp. 94-103, 2017.
[27]A. Ndikumana, N. Tran, T. Ho, D. Niyato, Z. Han and C. Hong, "Joint Incentive Mechanism for Paid Content Caching and Price Based Cache Replacement Policy in Named Data Networking", IEEE Access, vol. 6, pp. 33702-33717, 2018.
[28]J. Yao, B. Yin and X. Tan, "A SMDP-based forwarding scheme in named data networking", Neurocomputing, vol. 306, pp. 213-225, 2018.
[29]Q. Li, P. Lee, P. Zhang, P. Su, L. He and K. Ren, "Capability-Based Security Enforcement in Named Data Networking", IEEE/ACM Transactions on Networking, vol. 25, no. 5, pp. 2719-2730, 2017.