Named Data Networking (NDN), Internet Architecture Design and Security Attacks

G. Arulkumaran, N. R. Rajalakshmi

Abstract: ***In Internet over established communication medium a packet in a network transmit data where users and data server with specific IP addresses interacted each other. Recent years, this peer to peer data communication also called as client – server data communication. Modern applications like YouTube, Social Networks and Bit Torrent have revolutionized the idea of user generated contents. The end users care only for precise data items irrespective of their sources. So, the importance is based on precise data called as named data rather than using IP addresses to recognize servers hosting a meticulous content. Likewise, necessity of IP addresses is a demanding issue persistent the Internet community. Due to content-centric networking platform, in which data has less importance, and proposed new terminology called Named Data Networking. NDN allows end users to float a new data request without any awareness about the end user host. Compare to Internet services NDN can handle security issues and user mobility, more efficiently. In this paper, we surveyed different network issues and security attacks in Named Data Networks and its counter measures and also we identified a set of current challenges in NDN for budding researchers in due course.***

Index Terms--- Named Data Networking, IP address, Security attacks, NDN Security

I. INTRODUCTION

Data communication was deliberated more than three decade to establish point-to-point communication between two end hosts which bring back data from servers. TCP/IP protocol allowed users to transfer audio, video, text and images over the Internet. In recent years, Internet changes in terms of the nature of applications, usage patterns and user requirements have significantly anxious. Recently evolving content-centric applications like, YouTube, Amazon, social networking, Netflix and e-commerce etc., allow users to share audio, video, texts. The internet traffic is slow due to Videos sharing. Today, irrespective of the location most of the application information conveyance model is worried about what information is required. Additionally, support for versatility and security isn't in-worked in Internet, however offered as various fixes or extra includes which may bomb now and again. The previously mentioned reasons encouraged scientists to locate an effective elective design to the Internet, which will inalienably bolster content-driven correspondence. Among a few supported ventures for structuring content-based future Internet standards, Named Data Networking (NDN) came up as the promising competitor which legitimately manages application produced variable-length, area free names to scan and force substance for a mentioning client, independent of their facilitating element. The essential plan standards of NDN depend on the Internet. NDN can legitimately utilize significant IP administrations like, Domain Name Service (DNS) and between space steering strategies. IP steering conventions like, BGP and OSPF can be adjusted to NDN with little alterations. Nonetheless, NDN offers certain upgraded highlights as clarified underneath. It utilizes information parcels with substance names rather than source and goal addresses. The utilization of novel substance names for correspondence enables switches to monitor bundles' states, which supports various capacities not at all like the IP switches. The information parcels are independent and free from where they are recovered and where they can be sent. These highlights permit in-arrange reserving of substance for satisfying future solicitations and innately bolster shopper versatility. In NDN, all information bundles are marked by its maker and checked by the customer, in contrast to IP. NDN switches support multi-way sending, i.e., they can advance a client solicitation to various interfaces simultaneously.

II. NDN CLASSIFICATION

The architectural design and functional characteristics of NDN as shown in figure below, NDN features broadly classified into system architecture, system services, and applications.System architecture – Describe the association of various segments and their connection inside the framework alongside its few working standards. Framework Services - It worries about the primary practical attributes of NDN, which incorporates steering, storing, sending, security and portability. Since, NDN underpins in-organize storing of client mentioned content while conveying the equivalent.

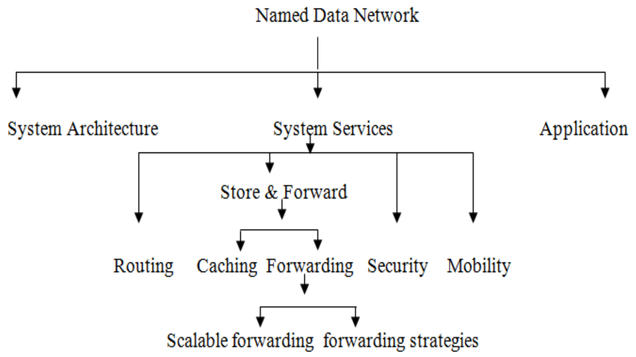

Fig 2.1 Characteristics of Named Data Network

Revised Manuscript Received on September 22, 2019.

G. Arulkumaran, Assistant Professor, Vel Tech Rangarajan Dr.Sagunthala R&D institute of Science And Technology, Chennai. erarulkumaran@gmail.com
N. R. Rajalakshmi, Associate Professor, Vel Tech Rangarajan Dr.Sagunthala R&D institute of Science And Technology, Chennai. rajirajasekaran@gmail.com

Retrieval Number: K125809811S19/2019©BEIESP
DOI: 10.35940/ijitee.K1258.09811S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Store and forward can further be sub-isolated into saving and sending. Security is the best in-amassed feature of the NDN building which gives secure correspondence through named data. While, flexibility deals with the treatment of all issues related to the customer and provider compactness. Applications – shows the valuable points of interest of the well-arranged NDN plan, in reality, through different standard similarly as novel applications.

III. NDN SECURITY ATTACKS

In the data centric network security attacks is one of the main areas to focus to establish the communication. The basic challenges in NDN security are trust management, privacy protection and cost-effective security operations. The security attacks in NDN layers are,

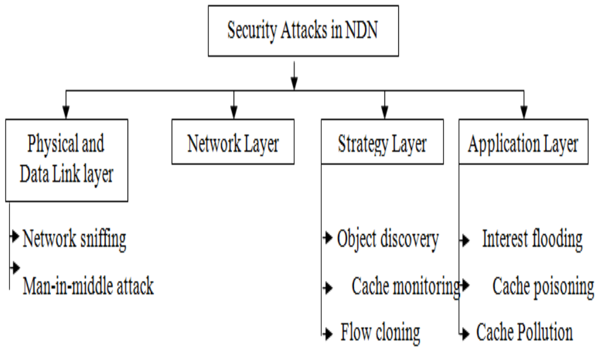

Fig 3.1 Named Data Network Security Attacks

3.1 Physical and Data Link Layer

Named data network design encryption mechanism is similar to the TCP / IP architecture. There are two major attacks in physical and data link layer.

i) Network sniffing – In named data network when the communication established, the application may capture the content and name without encryption transferring called as network sniffing. There three types of sniffers are external sniffer, internal sniffer and wireless sniffer.

ii) Man-in-middle attack – In named data network between two communication an attacker may secretly change the content is called man in middle attack. As a countermeasure for these attacks, NDN design supports an encryption mechanism similar to the TCP/IP architecture.

3.2 Network Layer

Prefix hijack is the main attack in network layer, this is also known as black hole prefix hijack attack, in that a malicious autonomous system advertises itself as invalid prefixes to other nodes. This corrupts the routing information and other existing autonomous system and starts forwarding information requests to this malicious autonomous system. This attack is less effective in NDN. With respect to name interface forwarding strategies at the router level will keep information about the performance of each interface status. It can be prevent from prefix hijack using securing named data mechanism in NDN because each router update and have a public key name provided by the network operator. All updated routers information will be signed by the interface key for supporting the authentication to the update named information.

3.3 Strategy Layer

In strategy layer the possible main attack is due to naming the contents. Someone can track the content easily in between the communicating parties. When congestion happen, then due to retransmission of packets network get overhead. Even after encrypt the data in the encrypted routers, it is easy to discover other information like, content name, node size, previous node, next node etc., this concept is known as cache snooping. There are three cache snooping attacks

i) Object discovery attack – Discover objects in between the routers. To prevent this attack limit the number of name prefix matching using some exclusion filter.

ii) Cache monitoring attack – Monitoring the existing router data. To prevent this attack generate one time name of the content name as unpredictable.

iii) Flow cloning attack – Recognize the complete data flow in between the router. To prevent this attack challenger predict the name of the request content through object discovery.

Another possible attack in strategy layer is scanning attack that scans port of the router. In port scanning, a malicious node sent message to each and every port in between the communication router and wait for a response and get the data's like, port alive, port entry node, exit node. The use of port is specific in NDN; it supports different names for different services in all possible names. Therefore while designing need little attention on input packet due to scanning attack.

3.4 Application Layer

The most common attacks in application layer are Denial of Service (DoS), Distributed Denial of Service (DDoS) attack and Domain Name System (DNS) attack. DoS attack means with the assistance of web association just a single PC framework flood a server. DDoS assault means circulated with the assistance of numerous PC frameworks. DNS assault distinguished names in the application layer and aggressor re-course the approaching traffic to a predefined server. DNS assault is beyond the realm of imagination in NDN doesn't make any impact whenever got substance is legitimate. NDN in-manufactured security highlights which oppose the NDN from specific assaults, for example, reflection assaults, data transfer capacity exhaustion, store harming, and dark opening prefix capture.

In reflection assault, due its symmetric correspondence enemy utilizes another host IP to make assault which is unimaginable in NDN. In data transmission consumption, with solicitations for officially existing substance enemy floods the injured individual's hub. This assault is constrained in NDN through middle of the road switch solicitation will arrive at the stores. Stored duplicates fulfill from the get-go in the interests for a similar substance. The store contamination and reserve harming are two fundamental DoS assault that focus on the substance. The three new NDN-explicit DoS assaults are in particular, store harming and reserve contamination and enthusiasm flooding with a lot of countermeasures.

i) Interest Flooding Based on the kind of substance demand, enthusiasm flooding assaults can be additionally delegated static, dynamic and non-existent.NDN is flexible to both static and phony assault, Static assault having like transfer speed exhaustion. In phony assault issue unsatisfiable information parcels to focused servers. Until it arrives at the focused on server NDN naturally lightens the intrigue total at the switch.

ii) Cache harming An aggressor can over-burden the store through the invalid signature or wrong private key Destination bundles. A customer may effortlessly confirm the mark and distinguish reserve harming. This element presents two principle challenges, for example, signature confirmation overhead and trust the board. The creators have likewise centered for solid authoritative of Input parcels with its comparing goal bundles and proposed countermeasure dependent on heuristics, between switch correspondence and client criticism.

iii) Cache Pollution Two countermeasures, credulous and particular have been proposed against reserve based security assaults. Gullible countermeasure further can be classified as distinguishing an assault and anticipating an assault. Difficulties in identifying the reserve contamination assaults are that aggressors may change their conduct and switches have less preparing capacity. To keep information from the assailant, the bounce check highlight could be debilitated and some postponement can be included for bringing the stored information to give a feeling that reserve is shared by numerous clients. Specific countermeasures demonstrate that substance accessible in the system can be named delicate and non-touchy. Specific countermeasure is additionally delegated particular storing based on substance ubiquity and particular burrowing for touchy substance. Content ubiquity may rely upon the setting where it is utilized and the area.

3.5 DDoS Attack

They have proposed four countermeasures to be specific, token container with per interface reasonableness, clever assault moderation, fulfillment based Interest acknowledgment and fulfillment based pushback.

First approach adjusts the token container of bundle exchanged system and ensures that next jump will get a reasonable blend of Input parcels. Second approach utilizes the measurements of Interest fulfillment proportions to settle on choices for sending approaching Input parcels. Third approach utilizes the Interest fulfillment proportion dependent on direct likelihood to acknowledge or dismiss the approaching Input parcel. In fourth approach, every switch reports its Interest limit for every approaching interface to their downstream switch. Assessment demonstrated that the fourth approach beats the rest. Be that as it may, the plan can't recognize Input bundles having phony names. In enthusiasm flooding, a specific name prefix is focused on and ordinarily demands are sent for same name prefix from foe side. This doesn't just deplete PIT yet additionally, squanders FIB assets. In communicate based Interest flooding, enemy chooses a non-existent name prefix for information bundles and floods it. A two-stage identification plan has been proposed to follow the ordinary name prefixes utilized in Interest flooding. The two stages are harsh recognition stage and precise distinguishing proof stage.

3.6 Session Attack

Because of information driven nature of NDN, many existing Internet-based applications, for example, ACT, live gushing, and vehicle to vehicle correspondence, on the Internet can be executed without looking after sessions. NDN these assaults are less powerful as security is applied at information level rather than channel. Checking Attack - Scanning every single imaginable name in NDN is troublesome

IV. RESULT AND CONCLUSION

As NDN is a sprouting territory of research, it offers abundance of open research difficulties for ebb and flow just as future maturing analysts. NDN engineering should bolster intelligible, all around remarkable and secure and area autonomous names. In this manner, the serious issue is to build up a naming component that can fulfill every one of these prerequisites. Presently existing naming approaches, similar to level, various leveled, and characteristic worth, bolsters a portion of the necessities. Level names give uniqueness, and prompt no overhead for finding the longest prefix coordinating. Level names can act naturally affirming and can be effectively dealt with profoundly versatile structure, as DHTs. Be that as it may, level names don't bolster name accumulation.

REFERENCES

1. Divya Saxena, et., al (2016) "Named Data Networking: A Survey" Article in Computer Science Review, DOI: 10.1016/j.cosrev.2016.01.001. All substance following this page was transferred by Divya Saxena on 02 April 2018.

2. L. Zhang, et., al (2010) "Named Data Networking (NDN) Project", Available: http://nameddata.net/venture/yearly progress-outlines/.

3. D. Estrin, et., al (2012) "Named Data Networking (NDN) Project" Available: http://nameddata.net/venture/yearly progress-rundowns/.

4. Jacobson, et., every one of the (2009) "Systems administration named content " In Proceedings of the fifth International gathering on Emerging systems administration examinations and advancements (CoNEXT).

5. Ahlgren, et., al (2012) "A review of data driven systems administration," IEEE CommunicationsMagazine, 50(7), pp. 26-36.

6. Z.A. Jaffri, et., al (2013), "Named Data Networking (NDN), New Approach to Future Internet Architecture Design: A Survey," In International Journal of Informatics and Communication Technology (IJ-ICT), 2(3), pp. 155-165.

7. Y. Li, et., al (2014) "Quicken NDN name query utilizing FPGA: Challenges and a versatile methodology," In Proceedings of the 24th IEEE International Conference on Field Programmable Logic and Applications (FPL), pp. 1-4.

8. Afanasyev, et., al (2015) "SNAMP: Secure Namespace Mapping to Scale NDN Forwarding," In Proceedings of the 18thIEEE Global Internet Symposium.

9. P. Gasti, et., al (2013) "DoS and DDoS in named information organizing," In Proceeding of the 22nd IEEE International Conference on Computer Communications and Networks (ICCCN), pp. 1-7.

10. Karami, et., al (2015) "A mixture multiobjective rbf-pso strategy for moderating dos assaults in named information organizing," Neurocomputing, pp. 1262-1282.

11. Z. Zhu et., al (2012) "XMPP over Named Data Networking: Design," 2012, pp. 1–8.

12. K. Lei, et., al (2014) "Adaptable control board for media gushing in NDN," In Proceedings of the first ACM International Conference on Information Centric Networking, pp. 207-208.