A Role of Routing, Transport and Security mechanisms in Information Centric Network

Mahesh R Patil, Agilandeeswari L

Abstract* : *Legacy networks which were discovered in 1970's suited better for olden day's communication model where the network is host centric, but nowadays expectations from communication networks is changing and it is shifting from host centric to data centric. To suit recent expectations there is need of revolution in communication networks; Information Centric Network (ICN) is a new kind of network architecture evolving for future internet. This article introduces ICN and its prominent features and reviews the work done post architectural approaches in the areas of routing, transport and security specifically.

Index Terms*: *Information centric network Legacy network NDN

I. INTRODUCTION

Information Centric Network (ICN) is a kind of network structure which is data centric rather than host centric, i.e. in this type of network more importance is given to the content being carried on network rather than from where the content is extracted. In legacy networks content is delivered from origin servers, but here in ICN it's not necessary that content to be delivered from origin servers, it can be delivered from anywhere in the network because this content is location independent. Introduction of in-network caching feature in ICN enables the routers to store content in their content store, when a request arrives for a particular content, router checks whether the content is available in its store, if it is available then router responds to that request by sending content back to the requester.

A. Operations of ICN

Operation of ICN is different from legacy networks, in ICN there are two different kind of packets i.e. interest packet and data packet, at first user issues request for a content by sending interest packet to all available connectivity, this interest packet contains name of the content as prefix. Any in-network node which has that data in its content store consumes that interest and responds with a data packet back to requester if name in interest and name of content matches. Multiple in-network nodes having same data can also send this data to requester through multiple faces available, it's not mandatory that only one node should forward data. If the content is not available with any of the in-network nodes then interest packet is forwarded towards the content producer or origin server by placing content name in pending interest table (PIT) of its own and when server responds with data packet then in-network nodes will cache the data and serves the requester with data packet. Sometimes there may be request for such a content which does not exist yet and even producer or origin doesn't have that content, in this case content is generated on the fly and sent back to requester which is called as dynamic content generation.

In figure 1 we can see that object B is a certain YouTube media content available at YouTube server but it is also stored in an untrusted host in the network. Now user Bob wants to access the media content B but Bob is connected via an untrusted connection to reach the node containing media content. No matter whether it is untrusted host or untrusted connection but the media content can be trusted due to public key infrastructure (later explained) and this content is delivered from in-network cache and not from origin server because in-network router holds the copy of that media object. This copy is distributed in an asynchronous fashion to all the users requesting the same copy until content is available in cache. This content will be replaced if there is request for another content.

Note that this article summarizes the work done post architectural approaches in the areas of routing, transport and security for ICN. This article dose not concentrates on architectures alone, for architectures please refer [1] and [2]. This article discuses about different ICN routing and transport protocols and their comparisons which evolved after the architectures were developed, providing a rough overview of all these approaches along with their description, advantages, disadvantages and research challenges. Terms like content, data, information and object in this article are used interchangeably.

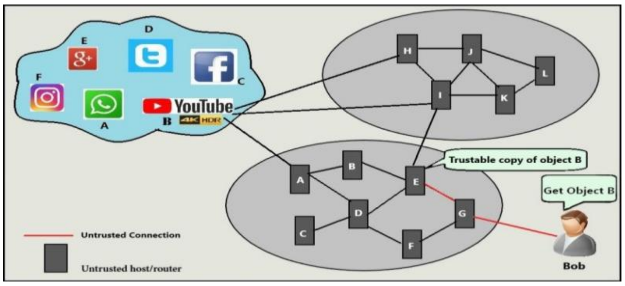

Fig 1: ICN Operation

Revised Manuscript Received on July 05, 2019.

Mahesh R Patil, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India.
Agilandeeswari L, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India.

B. Problems with Legacy Networks

Legacy networks were designed according to the requirements of 1970’s communication model; where there was a need to connect two different geographically located systems using a network to access files and services. During that time telephone networks were effective and successful global communication system and TCP/IP offered a unique solution for communication between two end points. Later as time passed Internet started to expand and more and more devices got capability to interact with each other in the network like mobile phones, laptops, Desktop PC’s, tablets etc. Now with the introduction of Internet of Things it is expected that any object in the physical world can get capability to interact in the network using IP. Nowadays internet traffic is growing to a greater extent and rapidly it is shifting from host centric to content centric. Many of the users just need content to be delivered and it is not expected from where it will be delivered e.g. YouTube video. Moreover Cisco has forecasted that 82% of the internet traffic in 2020 will be video. So legacy networks are not efficient to meet changing demands and there is need of ICN to solve growing internet traffic. Let’s consider 10 users watching live telecast of cricket match on mobile phone over same Wi-Fi network and connected to same access point using Legacy network. In this scenario 10 different streams will be created and same content will be running over these 10 streams and these streams will acquire entire bandwidth ultimately making internet connection slower for all users because TCP will be busy in retrieving the same content from the same origin server all the time. Suppose if ICN is introduced in this scenario then only one stream will be there between nearest router and origin server, and nearest router will cache the contents and will deliver to all the users in asynchronous fashion ultimately reducing internet traffic and delivering better quality of service.

This article reviews the work done in the areas of network layer, transport layer, and security in ICN after different architectures evolved for ICN, though this article may not contain latest updates related to these areas but it covers most of the work done past architectural approaches. Particularly these areas are chosen for review because they are interrelated and many of the problems in ICN which needs to be addressed has strong bonding with them, let’s consider Request aggregation research challenge where the number of requests must be aggregated in a single request. This challenge needs support from transport layer for managing request retransmissions, sub-flowlets (partial data can be delivered by any in-network node) and other aspects, as well as it needs support from network layer to deliver the content to all the aggregated requesters. For access control and authorization of aggregated requesters needs security implications. There are more research challenges described in this article which needs support of these three areas.

This paper is organized in seven different sections, where section II describes the features of ICN, which is helpful to understand why ICN is better compared to legacy networks and gives clear idea what ICN provides us and its advantages over legacy networks. Section 3 summarizes different architectural approaches of ICN. Section 4, 5 and 6 elaborates the work done on routing, transport and security in ICN. Finally, conclusions were drawn in Section 7.

II. Features of ICN

A. Named Data

Each and every content in information centric network is associated with a name, these names are unique identifiers for associated content based on location independency. To address a content these names are used instead of IP addresses. All the network operations are mapped to named data and not location [3].

B. Improved Transport

ICN has a connectionless receiver driven pull based transport model compared to legacy sender based TCP/IP model. In ICN a content is retrieved from multiple unknown sources without initiating a connection [3].

C. In-Network Caching

Pure ICN nodes like routers will be having cache memory to store contents in their cache. Any ICN node with this cache has the facility to store the content travelling through that path. This will help to provide the same content to other requesters instead of forwarding request further. When a request arrives, in-network node will first check its own content store for the requested content, if the content is present then it will respond with the content. If content is not available then it will forward request by placing content name in pending interest table. So by using cache it’s not necessary to retrieve the content all the time from origin servers, content request satisfaction can be done by in-path caching [3].

D. Asynchronous Multicast

ICN node can deliver the content to the multiple requesters simultaneously in asynchronous fashion using in-network caching, where only one request is forwarded towards the uplink.

E. Consumer Mobility

Legacy TCP/IP networks are meant for static wired connections whereas for wireless connectivity a special kind of TCP is deployed. ICN natively has connectionless transport protocol where it is initially tuned for consumer mobility.

F. Native Multi-homing

ICN takes the advantage of all the available interfaces to retrieve the content. For e.g. a requester can use multiple interfaces like Wi-Fi, Bluetooth or LTE at the same time and content is delivered using multipath ICN through different interfaces. It’s almost similar to multipath TCP but there is some difference. Even multipath TCP uses multiple interface to retrieve content but it is end to end connection oriented, where the multiple paths are formed between two end peers, but in ICN it’s not necessary to form connection between two end peers, it is connectionless and multiple paths can be created with the in-network or in-path node also because any node in network can provide a fraction of content if it has in its content store.

G. Load Balancing

ICN uses load balancing approach to achieve the fairness during content delivery over the multiple paths by offloading the highly loaded path and sharing the multiple paths and bandwidth.

H. Asynchronous Producer Mobility

ICN has the feature of any node mobility including any producer node also. A producer can create content on the fly in ICN and when request arrives, it directly delivers the content, a producer can move from one access point to another access point without disturbing the ongoing transmission, handover here is a smooth, easy and quick handover whereas it’s tedious in wireless TCP. This mobility model in ICN does not require an anchor node for communication whereas TCP/IP in legacy network needs an anchor node for communication, therefore ICN has anchorless mobility support. Here anchor node represents a network node like a server through which the communication must pass compulsorily.

I. Object Based Security

In TCP/IP networks two end point connections are secured but content itself is not secured, here content travel through a secure channel, but in ICN security is provided to content itself rather than securing the channel between two end points. ICN uses public key cryptography to secure the content, it uses encryption mechanism for assess control. [3]

III. Architectures of ICN

ICN follows communication model which is termed as receiver – driven meaning that the data will be retrieved only when there is an external request. Each routers in ICN will use location independent name prefix for forwarding the packet. On the other hand, IP follows sender – driven based communication model meaning that the sender will immediately create an IP packet with source and destination address in the IP header field of the packet and post the packet on to the network. Each routers in IP will use the packet’s destination address to forward the packet. ICN also uses the term “what” instead of “where” meaning that what data is requested is more important than where the data is presented. Several approaches came up with different kind of architectures for ICN, most prominent among them are DONA [4, 7, 8], PURSUIT [7], NDN [3, 5, 6, 7, 8], NetInf [9], SAIL [7] etc. [1] [2] summarizes different kind of approaches and its comparisons. [3] NDN is the approach initially proposed by Van Jacobson, and now Cisco has acquired this NDN project and made it as open source. NDN is implemented in the form of code in CCNx software and custom NS-3 based simulation package for NDN is also released. ICN networks works on the basis of content centric networking rather than host centric in the legacy systems. It states that packet address meant for content not for the location. In NDN architecture IP packets are replaced by content chunks (Figure 2) which are also represented by interest packet and data packet. The basic NDN packet forwarding engine is shown in Figure 3 which has three main data structures: Forwarding Information Base (FIB) for interest packets forwarding, content store which is same as buffer with different policy of replacement and Pending Interest Table (PIT) maintains the interest which is requested.

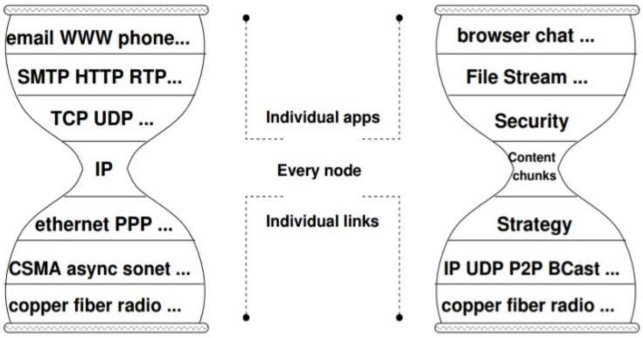

Fig 2: Shift from IP to content chunks in ICN [3]

In NDN architecture IP packets are replaced by content chunks which are also represented by interest packet and data packet, figure 4 depicts the packet structure where an interest packet contains the name selector and nonce and the data packet has name, security and data part.

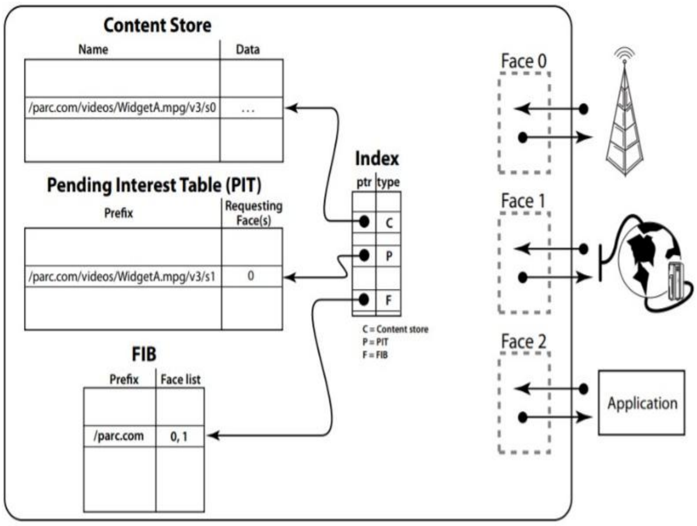

Fig 3: NDN forwarding engine and data structures [3]

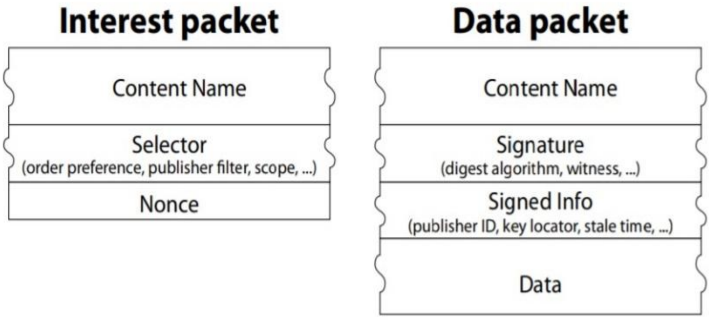
Interest packet
Content Name
Selector
(order preference, publisher filter, scope, ...)
Nonce
Data packet
Content Name
Signature
(digest algorithm, witness, ...)
Signed Info
(publisher ID, key locator, stale time, ...)
Data

Fig 4: NDN packet structures [3]

IV. Routing in ICN

According to the architecture of ICN there is need of new routing algorithms to work with data centric communication model and old legacy network routing algorithms can't be used as it is in ICN. Interest and data routing are impotent in ICN and they need careful design that is why routing is chosen to be reviewed in this article. Routing in ICN is finding the named data content using the name of the content which requesters provide initially. Routing in ICN has three different moves. First is name resolution, this step is related to resolving the name of the object into its location, next step is discovery where the interests are forwarded based on their locations and the last step is delivery where the responses are delivered back to the requester. There are three types of routing mechanism in ICN viz. routing by name (RBNR), Look-up-by-name (LBNR) and Hybrid routing consisting of first two routing jointly. Initially routing by name was the only routing mechanism proposed by the originating architectures like DONA and NDN but later other two routing mechanisms were proposed depending on current research challenges. In [10] authors have compared different caching and routing techniques and their features, also implemented and demonstrated the comparisons in the form of simulation using various network parameters. In [11] authors have proposed a name based routing protocol which uses distance information and does not need routing information and the physical network infrastructure.

A.Routing by Name

Routing by name does not require to go through the first step called name resolution because here name themselves are used for routing. This kind of routing is almost symmetric to IP routing because NDN architecture states that routing in NDN is done by lookup of prefix by longest match. Using names for routing may create problems when data objects in network increase to greater extent, because of many content availability the size of routing table will also increase, with this increase in routing entries there is another possibility of increase of length of the names also. So this is the main research challenge and there is some mechanism needed to resolve this issue. One way to resolve this issue is to introduce some aggregation mechanism so that data objects collectively can be aggregated and reduces the routing table size. This routing mechanism is very important because it skips the first step of name resolution and directly routes the objects by their names but routing only by names also faces challenge of retrieving location, there is need of location identifier to route the interests, for this purpose there is proposal of breadcrumbs routing [12] where interests travel towards the other edge by leaving 'breadcrumbs', pending interest table entries are the breadcrumbs here, routers keep track of the upstream forwarding interfaces so that responses are sent back by the same path. Another problem with this type of routing is immediate wide adoption in the internet and for this there is next routing mechanism below.

B.Look up by Name

In this routing first a name is mapped to IP address which is name resolution and then further two steps discovery and delivery are carried out. These two steps are carried out similarly as IP does because using IP address a location can be found and interest or content can be forwarded based on location. [13] MDHT is one of the related works which proposes this look up by name routing. Look up by name routing is currently reliable because it uses all the steps to get the content and can be used with current IP networks without replacing the current network layer. A challenge specifically to this kind of routing is fast lookup. Content name mapping to the locations including in-network copies must be done in fastest and reliable way, and another challenge is if the name of the original content is changed then how that name can be reflected to other copies in the network. Also this ICN natively supports mobility so nodes tend to change their locations fast and frequently and need to fix this for name resolution for frequent location changing data objects.

C.Hybrid Routing

Hybrid routing is the combination of the two previous routing mechanisms. Routing based on the names is adopted where there is necessary of overall reduction of latency by skipping the name resolution phase. Lookup by name can be used for routing between the two distinct domains who has their own location identifier or prefix.

Cisco is coming up with a new hybrid inter-networking for ICN called as Hybrid ICN (HICN) to be deployed in 5G networks, which is an incremental deployment solution for ICN. Need for this kind of proposal is that it's very difficult to replace whole network layer of TCP/IP with the network layer of ICN and to make ICN work in current networks this kind of hybrid solution is required. This solution preserves all kind of features of Information Centric Network by mapping the names into the IP addresses and it supports both name based as well as IP address based forwarding on the existing TCP/IP networks. The basic concept here is cisco is planning to embed ICN semantics into IP which preserves all the ICN principles.

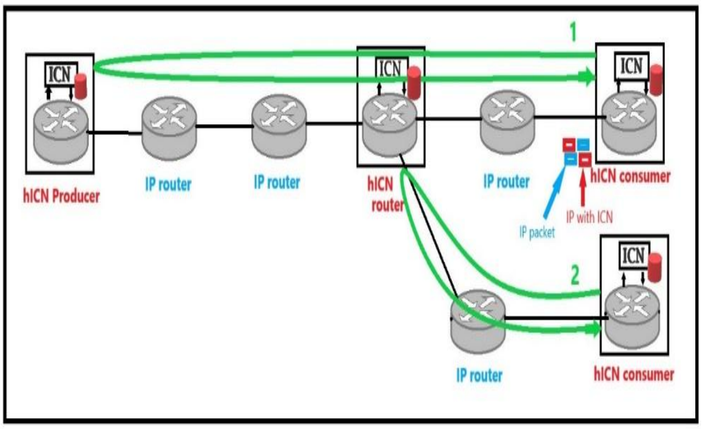

Fig 5: Hybrid ICN Architecture

In the above figure 5 there is one ICN producer serving two different ICN consumers. This complete scenario is upgraded using one hICN router in between the routes. Here the ICN requests called as interests are actually the names which are embedded in IP packet and forwarded towards producer. In this above scenario both hICN consumers will request for same content and the hICN in-network router will forward only one request towards the producer. When producer responds back with the actual content then the in-network hICN router will cache the content and will serve both the hICN consumers through regular IP infrastructure. Cisco is also planning to deploy this architecture in 5G networks for 4K video delivery using MPEG-Dash which is a dynamic adaptive streaming because they believe that future traffic of internet will comprise 82% of video in 2020.

V. TRANSPORT LAYER IN ICN

ICN is moving towards receiver driven congestion control and legacy networks transport model does not suit for ICN, so there is need of new transport protocols to work with receiver driven communication and cope up with network layer functions of ICN, this is the reason the review about transport layer is included in this article. ICN needs receiver driven congestion control protocols in order to resolve the problem of congestion and fairness among the requesters. In a receiver driven protocol for congestion, when a receiver requests for a content which is smaller than the highest packet size of the network then the content is sent as a response directly to the requester, but when the content is much greater than the highest attainable packet size of the network then content needs to be divided into various segments, and these segments are to be transmitted in network. According to receiver driven mechanism it is left upon the receiver to request the segments individually on its own, so for this a sender will send meta-data of the requested content as a response if the content size is higher than the maximum attainable packet size. This meta-data may contain segment identifiers for individual segments, security information of the content, content length and even integrity information also.

There is not much work carried out in the area of congestion control for content centric networks, few proposals have come up with receiver driven congestion control mechanisms. ConTug is one of such kind of receiver driven congestion control protocol whose implementation is based on Publish Subscribe architecture because authors believe that this is the suitable architecture for overall requirements. [14]ConTug uses a conceptual window for congestion control called CCWND, it is almost similar to TCP congestion window, ConTug forms this window at the receiver side as this ConTug is a receiver driven congestion control protocol, at the initial it starts in the slow start phase and as more and more reply channels join its increases the congestion window size. For a time out loss ConTug uses times for retransmission requests, here congestion is detected by the difference of expected rate and actual rate of transmission. This work is implemented in ns-3 simulations and the evaluations were carried out. Throughput of this receiver driven protocol is almost similar to TCP without using in-network cache and after using caching mechanism with ConTug has better flow completion times even with partial stateless senders, senders can join and leave any time without affecting the receiver's transmission. This protocol does not define any forwarding mechanisms and it depends upon other forwarding mechanisms.

There is another request control protocol i.e. ICP [15] which regulates sending requests in the network. It uses windowing mechanism for flow control, it follows the principle of additive increase to keep the requests regulated. Whenever an interest packet is sent through different faces, the timer is set, if the timer expires and no response in specified time then it is assumed that there is congestion and ICP uses multiplicative decrease to ease the congestion. However the interest re-expression timer must be set in such a way that there must be no faulty re-transmissions, much smaller value will make too many re-interests and much bigger value will delay performance. There may be delay in receiving response due to bottle neck topologies where keeping the timers to optimal value is very important. ICP's work is evaluated by the authors and its performance is well acceptable but at the same time another authors claim that it is very important to manage interests flowing through each and every hop, as there might be some problems at the hops having bottle neck like topologies. To overcome this problem these authors have extended the work of ICP and came up with new [16] hop by hop outlining the interests using the virtual interest queues for every flow at each and every outgoing interface of every router in the network path in the case of bottle neck topologies. For non-bottle neck topologies the interests are directly forwarded if content is not available with the router. This is a joint approach of ICP and hop by hop interest outlining using queue's to optimize receiver driven interest's control. The main research challenges with these transport protocols is that it's very difficult to distinguish between initial original request and retransmitted request. In [17] authors have proposed a novel hop by hop transport mechanism called R^2T where there is reliability of packet level high speed transport. They have experimented in real ICN implementation and results have shown that it gives better performance than TCP and has high bandwidth utilization, short and effective response latency and feasible in real world ICN implementations. In [18] authors displayed a depiction and a primer execution assessment of a Source Change Warning plan. Our answer, controls the Interest Retransmission Timeout estimation at the collector. A new information structure, called Interest Trace Table is presented in each NDN switch to keep the hint of fulfilled Interests. At the point when a switch that has served a Consumer can't fulfill further demands and Interests are sent to a more distant store, an unequivocal notice is sent back to the Consumer. This last expands its Intrigue Timer to stay away from pointless retransmission. To survey the exhibition of our proposition, we executed the proposed arrangement in ndnSIM and concentrated its conduct when combined with ICP and HoBHIS. This starter execution examine, indicates obviously that the Source Change Notification plan succeeds in decreasing the quantity of Interest break occasions in a multi-bounce, multi-discussion bottleneck situation.

From the study it is clear that most of the proposals of TCP in ICN is ready for Wired Networks not focusing towards Wireless Networks. For example proposal [19] focusses towards the twofold contributions as (i) they segment the content to be transmitted into two levels, with segmenting into chunks as first level and chunks are further segmenting into smaller data units at the second level. The ICN specific transport protocol proposed by the authors can able to take care of reliability and congestion control functions. (ii) The proposed transport protocol also works on the principle of ICN receiver driven, such that the receiver also adjusts the sending rate to control the congestion happens. The proposed architecture also elaborates various advantages like (i) elasticity in choosing the bandwidth to either increase or decrease the congestion. (ii) Fairness in the TCP flows coexistence with traditional systems without any starvation.

In [20] the authors proposes the TCP protocol that can be used in ICN architectures namely CCN, NDN [21] and hICN. They have shown the benefits of adopting their transport layer in existing application in order to evaluate CPU load reduction and a lower memory consumption.

VI. Security in ICN

In this section, we discussed about the various security features of ICN.

A. Data Integrity and Origin Authentication

ICN's security model is completely different from legacy networks, in legacy networks security was provided by sending content over encrypted path from source to destination, but this is not the case in ICN. In ICN contents are secured instead of securing the path they travel. Here content can be delivered from anywhere in the network so it's very important for ICN to verify the content integrity because in-network content can be modified maliciously. Solution to this problem is to bind name with content by hashing [22]. Another solution for this is using public key cryptography [23] to make the content distinguishable from original content and fake content by using hierarchical public key infrastructure. Content producer will sign the content before publishing it, requesters having public key of the producer can verify the originality of the content. Here the main research challenge is how efficiently public keys can be distributed so that public keys are easily available. Publisher identity is also a research challenge where it's necessary to know whether the content was published by authentic publisher.

B. Access Control Authorization

Since named data objects can be delivered from any in-network cache so it's very difficult to maintain access control over these contents, there is need of some mechanisms to manage the access control. There are mainly two approaches through which access control can be managed as follows:

C. Third party Access Control

In this approach [24] authors have introduced information distributer as a middleware between producer and the consumer. Here the content owner creates the access control policy and stores in the network through which it wants to communicate to its requesters. Access control URI is created for that content and this URI is passed to distributer, whenever consumer requests content to distributer then distributer just responds with URI of that content. Then consumer accesses the content by authenticating itself in the network where the content is stored. In this approach distributer neither stores the content nor has the access control policy with it, due to this kind of access control design authors assume that this approach will work with other architectures of ICN also but they have successfully tested this approach on PSRIP architecture. With this design all the consumer credentials are securely protected and even consumer privacy is preserved. The only problem with this design is it has some communication overheads. So challenges related to this design are to reduce possible communication overheads and the delay of authorization (when communicating to distributer).

1) Integrated Approach

This approach uses content encryption and distributing the keys in network [25]. It is completely de-centralized and does not require a middleware for communication. Here authors have presented a group based access control using the CCN protocol and then they have tried to initiate a broadcast based access control by enforcing broadcast encryption. This approach benefits from fast access because of no middleware but key distribution is one of the challenge. More challenges include managing the key revocations, applying access control on in-network cached dynamic contents, providing consumers with flexibility of access to individual in-network cached contents in scalable manner.

2) Traffic filtering and aggregation

To reduce the network overall traffic several requesters can be aggregated behind one request but this aggregation makes difficult to filter requesters. This is the major challenge to design a mechanism which allows aggregation of the requesters and filtering of the requesters. A possible solution for this approach is to mention a subset of requesters in the response of an aggregated request which allows only specific requesters to access the content and this approach requires collaboration from other routers in the network and this kind of approach is not suitable for caching the contents in the network. Another solution is to encrypt the content and make sure that only authorized requesters are allowed to decrypt. This solution does not require collaboration from other network routers. This can be achieved by using group signatures [26]

3) Denial – of – service attacks

Various ICN approaches like CCN implement their states in the network routers for routing and forwarding, and these approaches can experience denial-of-service attacks i.e. Interest flooding. [27, 28, 29, 30, 31] Few authors have tried to analyze these kind of threats in ICN along with various network instabilities. According to their analysis they are able to show that a strong coupling between control and data plane can be misused in various ways. They discuss these problems along with relevant theories and practical simulations to identify attack vectors in ICN. Research challenge here is how these denial-of-service attacks can be avoided which can prevent complete network infrastructure form attackers. There is another possible threat of exhaustion of resources if this kind of attack occurs, so mechanism to handle this kind of attacks is needed.

VII. Conclusion

We have discussed what are the problems with legacy networks and all the features of ICN which finally concludes that ICN is needed to overcome the problems faced by legacy networks and ICN better suited for the today's and future network requirements. If we start researching in ICN then network, transport and security are the three prominent areas of ICN where more efforts are required to come up with new proposals supporting all the research challenges mentioned in this article. If we focus on network protocols for 5G wireless networks then lookup by name routing is suitable but it won't provide pure ICN functionality because it uses one extra step for name resolution. Routing by name is the fastest one but it faces challenges related to location accuracy for current network deployments like LTE or 5G, in such cases hybrid routing may come in the scenario. Hybrid ICN is a new proposal to meet requirements of routing in ICN in 5G wireless networks. Interest control protocol (ICP) regulates interests in the network but lack in interest shaping where HRICP provides interest shaping for ICP and improves its performance. Traffic filtering, requester's access control by encryption and privacy and efficient key distribution are needed to be upgraded to support network and transport layer protocols of ICN. It is found that most of the transport layer proposals in ICN consider fixed and wired networks and does not work on wireless networks as intended, they will perform same as TCP in wireless scenarios, so for this problem there is need of transport layer proposals which are also optimized for wireless links. Based on this review we will be proposing transport layer protocols for wireless links as our future work.

REFERENCES

1. Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., and B. Ohlman, "A Survey of Information-Centric Networking", In Communications Magazine, IEEE, vol. 50, no. 7, pp. 26-36, DOI 10.1109/MCOM.2012.6231276, 2012.
2. G. Xylomenos et al., ``A survey of information-centric networking research," IEEE Commun. Surveys Tuts., vol. 16, no. 2, pp. 1024_1049, May 2014.
3. Jacobson, V., Smetters, D., Thornton, J., Plass, M., Briggs, N., and R. Braynard, "Networking Named Content", CoNEXT 2009, DOI 10.1145/1658939.1658941, December 2009.
4. Koponen, T., et al. (2007)."A data-oriented (and beyond) network architecture". In Proceedings of ACM SIGCOMM, Kyoto, Japan.
5. L. Zhang et al., "Named data networking (NDN) project", NDN, Tech.Rep. NDN-0001, October 2010.
6. L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named Data Networking",ACM SIGCOMM Computer Communication Review (CCR), vol. 44,no. 3, pp. 6673, Jul 2014.
7. George Xylomenos, christopher N, Vasilios A, Nikos fotiou, christos tsilopoulos "A Survey on Information Centric Networking Research" 2013 IEEE.
8. Md. Faizul Bari, Shihabur rahman choudary, Reaz Ahmed "A Survey of Naming and Routing in Information-Centric Networks" 2012 IEEE.
9. Ahlgren et al., "Second NetInf Architecture Description"', 4WARD EU FP7 Project, Deliverable D-6.2 v2.0,Apr. 2010, FP7-ICT-2007-1216041- 4WARD / D-6.2,http://www.4ward-project.eu/.
10. A. Seetharam, "On Caching and Routing in Information-Centric Networks," in IEEE Communications Magazine, vol. 56, no. 3, pp. 204-209, March 2018. doi: 10.1109/MCOM.2017.1700184
11. Garcia-Luna-Aceves, J. J. (2014, September). Name-based content routing in information centric networks using distance information. In Proceedings of the 1st ACM Conference on Information-Centric Networking (pp. 7-16). ACM. Doi: 10.1145/2660129.2660141
12. Rosensweig, E. and J. Kurose, "Breadcrumbs: Efficient, Best-Effort Content Location in Cache Networks", In Proceedings of the IEEE INFOCOM 2009, DOI 10.1109/INFCOM.2009.5062201, April 2009.
13. D'Ambrosio, M., Dannewitz, C., Karl, H., and V. Vercellone, "MDHT: A hierarchical name resolution service for information-centric networks", ACM SIGCOMM workshop on Information-centric networking Toronto, Canada, DOI 10.1145/2018584.2018587, August 2011.
14. Arianfar, S., Nikander, P., Eggert, L., Ott, J., and W. Wong, "ConTug: A Receiver-Driven Transport Protocol for Content-Centric Networks", Technical Report Aalto University Comnet, 2011.
15. G. Carofiglio, M. Gallo, and L. Muscariello. Icp: Design and evaluation of an interest control protocol for content-centric networking. In Proc. of IEEE INFOCOM NOMEN Workshop, 2012.
16. Carofiglio, G., Gallo, M., and L. Muscariello, "Joint hop-by- hop and receiver-driven interest control protocol for content-centric networks", In Proceedings of ACM SIGCOMM ICN 2012, DOI 10.1145/2342488.2342497, 2012.
17. Wang, Z., Luo, H., Zhou, H., & Li, J. (2018). R 2 T: A Rapid and Reliable Hop-by-Hop Transport Mechanism for Information-Centric Networking. IEEE Access, 6, 15311-15325.
18. Mejri, S., Touati, H., & Kamoun, F. (2016, May). Preventing unnecessary interests retransmission in named data networking. In 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.
19. Salsano, S., Detti, A., Cancellieri, M., Pomposini, M., & Blefari-Melazzi, N. (2012, August). Transport-layer issues in information centric networks. In Proceedings of the second edition of the ICN workshop on Information-centric networking (pp. 19-24). ACM.
20. Sardara, M., Muscariello, L., & Compagno, A. (2018). Efficient Transport Layer and Socket API for ICN.
21. Mastorakis, A. Afanasyev, and L. Zhang, "On the Evolution of ndnSIM: an Open-Source Simulator for NDN Experimentation," ACM SIGCOMM Computer Communication Review (CCR), July 2017.
22. Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, DOI 10.17487/RFC6920, April 2013, <http://www.rfc-editor.org/info/rfc6920>.
23. Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.
24. Fotiou, N., Marias, G., and G. Polyzos, "Access control enforcement delegation for information-entric networking architectures", Proceedings of the second edition of the ICN workshop on Information-centric networking (ICN '12) Helsinki, Finland, DOI 10.1145/2342488.2342507, 2012.
25. Kurihara, J., Uzun, E., and C. Wood, "An Encryption-Based Access Control Framework for Content-Centric Networking", IFIP Networking 2015, Toulouse, France, DOI 10.1109/IFIPNetworking.2015.7145300, September 2015.
26. Chaum, D. and E. van Heijst, "Group signatures", In Proceedings of EUROCRYPT, DOI 10.1007/3-540-46416-6_22, 1991.
27. Waehlisch M., Schmidt TC. , and M. Vahlenkamp, "Backscatter from the Data Plane - Threats to Stability and Security in Information-Centric Network Infrastructure", Computer Networks Vol 57, No. 16, pp. 3192-3206, DOI 10.1016/j.comnet.2013.07.009, November 2013.
28. AbdAllah, E. G., Hassanein, H. S., & Zulkernine, M. (2015). A survey of security attacks in information-centric networking. IEEE Communications Surveys & Tutorials, 17(3), 1441-1454. Doi: 10.1109/COMST.2015.2392629
29. Tourani, R., Misra, S., Mick, T., & Panwar, G. (2017). Security, privacy, and access control in information-centric networking: A survey. IEEE communications surveys & tutorials, 20(1), 566-600. Doi: 10.1109/COMST.2017.2749508
30. AbdAllah, E. G., Zulkernine, M., & Hassanein, H. S. (2016, May). DACPI: A decentralized access control protocol for information centric networking. In 2016 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE. Doi: 10.1109/ICC.2016.7511198
31. AbdAllah, E. G., Zulkernine, M., & Hassanein, H. S. (2018). Preventing unauthorized access in information centric networking. Security and Privacy, 1(4), e33. https://doi.org/10.1002/spy2.33

AUTHORS PROFILE

Mahesh R Patil received his M. Tech in Information Technology (Networking) from VIT University Vellore India in Aug 2016, later same year he worked as Assistant Professor at Walchand Institute of Technology Solapur India for one year and is currently a research scholar in VIT University Vellore India. His research interests include computer networks and future Internet technologies with a focus on Information-Centric Networking and Internet of Things.

L. Agilandeeswari is working as an Associate Professor in the School of Information Technology and Engineering (SITE) at VIT University, Vellore. She received her B. Tech in Information Technology and M.E in Computer Science and Engineering from the Anna University with honours during 2005 and 2009, respectively. She completed her PhD at the VIT University, Vellore with good number of publications indexed by Scopus and Thomson Reuters with an impact factor of > 4. She has also more than 20 international and national conference publications. She has around 11 years of teaching experience. She is a life time member in Computer Society of India. Her areas of interests include image and video watermarking, Information Centric Networks, Image and Video processing, Neural networks, and Data mining.