Proceedings of
INTERNATIONAL CONFERENCE ON INNOVATIVE TRENDS IN ENGINEERING RESEARCH (ICITER-2016)
International Journal of Innovations in Engineering, Research and Technology,IJIERT-ICITER-16,ISSN:2394-3696
26th June,2016

CONTENT CENTRIC NETWORKING FOR REDUCTION OF INTEREST FLOODING ATTACKS IN MIXED TOPOLOGY

[PAPER ID: ICITER-D156]

ROHIT AGNIHOTRI
Mahakal Institute of Technology, Ujjain, India
Email: agnihotrirohit0@gmail.com

ABHISHEK TIWARI
Mahakal Institute of Technology, Ujjain, India
Email: abhi.tiwari23@gmail.com

Dr. PRASHANT BANSOD
SGSITS, Indore, India
Email: ppbansod43@gmail.com

ABSTRACT:

The Content Centric Networking is an architecture proposed to deal with current leading issues in networking scenarios. The security mechanism is the key aspect for any communication between the peer and by focusing this only the secure communication can be achieved. The current internet protocols mostly secures the dedicated channels which are used in the communication whereas the Content Centric Networking is intended to focus over securing the data itself by introducing the naming convention which is used for the easy and secure access. The various security issues which exist when the actual communication happens, thwarts the security and produces the irrelevant results and threat of attackers. Such threats exist in the Internet Protocol and the Content Centric Network as well. The issue of the Interest Flooding Attacks actually floods the source node and slower down the mechanism of it. The various concerns of the newer architecture are regarding the existing threats which are caused due to adversarial attacks and such can be reduced to a minimum level in order to achieve secure and efficient communication. The major focus of this work is to undergo rigorous study regarding the Interest Flooding Attack, its types and preventions, also the study& Implementation of it having attack scenario within Mixed Topology with the increase in the no. of the malicious nodes which can cause multiple situations within the network.

KEYWORDS: Content Centric Networking, Denial-of-Service Attack, Interest Flooding Attack, Named data Network.

INTRODUCTION:

In the present scenario the internet is being used as a key concept for the purpose of communication, resource sharing in the vast communication network through various wired or wireless media at a higher data transfer rate over the Internet Protocol (IP) network. Since the IP addresses are being consumed already at the huge rate and there is the need for the extension of IPV4 to IPV6, and other such internet accessing mechanism, the future proposed architecture is conceptualized and formulated in form of Content Centric Networking (CCN) [i] in the project of the Palo Alto Research Centre (PARC) [i], [ii]in the year 2009. The basic protocol used in the CCN not varies much from the IP but the CCN can be applicable over and above all the tier-2 layers, which is justified as in Fig. 1. The CCN structure is based on the typical content naming and its secure communication through various signature algorithms and other cryptographic algorithms. CCN practically follows the Uniform Resource Identifier (URI) based naming scheme for accessing the content over the host or nearby neighbor node in a form having the label and name segment for identification of the label and its value. The names in CCN can be in both human readable and non-human readable format, such as like the usual domain format which is used in the IP address as files secure.com /node1/ file1/ secureddata.pdf/…. The CCN objects are of two types, which are also well known as 'Interest Packet' and the 'Data Packet'. These objects contain the name as well as the Payload. Thus the various cryptographic algorithms, Authentication mechanism, Message Integrity Check (MIC), validation schemes etc. are contained within it. The 'Interest Packet' is also known as the request message and 'Data

Packet' also known as the response message which is collectively known as the Content Object (CO) as given in Fig.2.

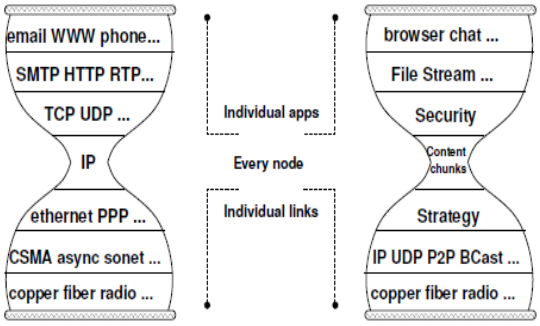

Fig. No.1. General Protocols used in CCN [i]

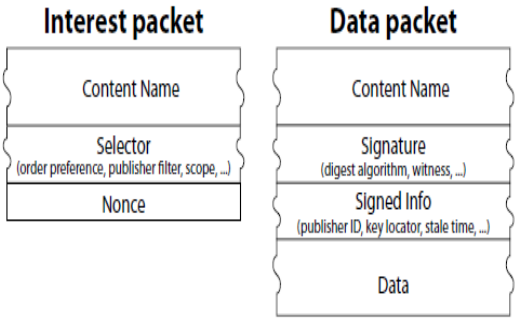

Fig. No.2. Content Objects Format [i]

The CCN's node structure for the CO is been classified mainly having the three structures as the Content Store (CS), Pending Interest Table (PIT), Forwarding Information Base (FIB) [i], [ii], [iii]. The major functions of the three structures are given below by mentioning the similarities with the IP node structure which are as depicted in Fig. 3.

1. Content Store (CS):- This structure is used to store the content in the memory for each CCN node, this actually relates with the IP node structure having the working similarity like the buffer memory for storing and holding the data.
2. Pending Interest Table (PIT):- The interest those requested from the downstream nodes towards upstream nodes and are not satisfied or not found are collectively stored in this data structure.
3. Forwarding Information Base (FIB):- This data structure is very much useful in CCN since this prevents the duplicate interest occurrence in the node. The FIB has prefixes and the various faces which calls them or through which it is being requested.

The CCN adds the security to its data by applying the cryptographic algorithms, signing mechanisms etc. [i], [iv]. Also conventional naming scheme makes the data easily accessible. The next sections in this paper consists of Interest Flooding Attack in Section II, whereas Section III consists of Implementation, Section IV has the Proposed Algorithmic Variations, Section V gives the previous works for IFA and lastly Section VI concludes the paper with future scope .

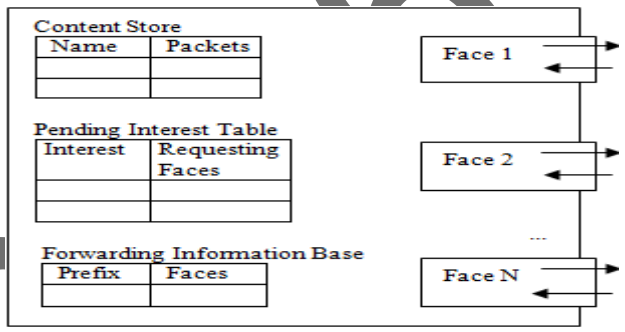

Fig. No.3. CCN node structure [iv]

INTEREST FLOODING ATTACK:

The Interest Flooding Attack (IFA) is the terminology which intimates us regarding the third party attack within the communication for the content in the CCN or the during the transfer of CO's during the communication. Basically IFA used as a synonym for the Denial-of-Service (DoS) attack which is already well known. Before actual IFA scenario (as in Fig. 4) the content namespace is being formulated, which consist off the domain, content name, its version and segment number. The attack prepared from the adversary &attacker is chosen to slow down the host or the server. The adversary firstly takes a domain randomly and then assumes a content name which is used as request and finally allots segment number which is collectively fired as Interest for the sake of IFA [v].

In brief, when the data structures in the CCN node structure are totally filled, say e.g. the CS, PIT, FIB is been filled out the inbound interest from the near-by intermediate nodes are discarded, thus the host not accepts the interest to be admitted at its end after certain threshold limit, when a lots of intermediate nodes/routers or a single node/router issues multiple interests for slowing down the host and the host in such condition not agrees for accepting the interests via the data structures and satisfaction of such interest becomes impossible due to mismatch in the ratio of the inbound

interest acceptance rate to outbound interest satisfaction rate for a node/host then such a node is identified as flooded given as Fig. 4 and the attack is known as IFA as depicted in Fig. 5.

The IFA [v-vii] situation can be aroused due to multiple reasons but some of them are caused due to FIB based attack, Broadcast based attacks [xi], PIT based attacks etc, cache attacks [ix-xv] etc.

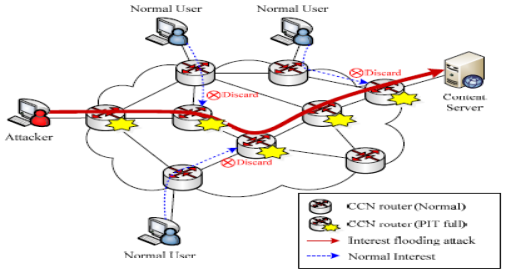

Fig. No.4. IFA Scenario [v]

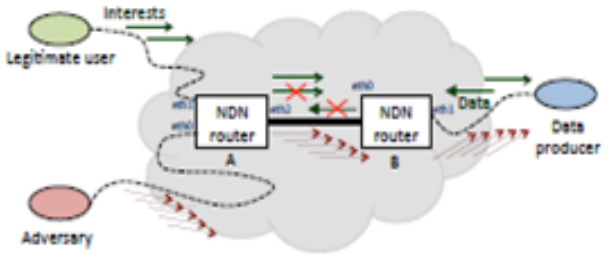

Fig. No.5.IFA attack by Adversary [vi]

The major classification of IFA attacks can be done in three categories as 1) Static Attack Model 2) Dynamic Attack Model 3) Random or Non-existent Attack Model as given in Fig. 6 [vii].

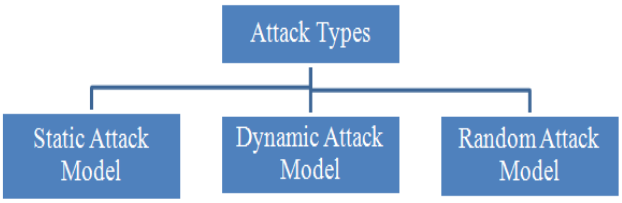

Fig. No.6. Classification of Attack Categories [vii]

IMPLEMENTATION:

The IFA is caused due to the prefix hijacking[vii], network and data thefts and third-party attackers through the help of prefix compression[vii][xii].The IFA mitigation strategy was implemented earlier in the work of Afanasyev et al.[vi] through the various algorithms implemented as Token bucket with per interface fairness & Intelligent attack mitigation which are having the types as Satisfaction Based Interest Acceptance (SBIA) and Satisfaction Based Pushback (SBP) Algorithm [xii], within which SBP algorithm was proved the most optimal so SBP algorithm and its study and further implementation has been focused mainly in this work, by extending the previous work [vi] and applying the topology as Mixed topology which is the advanced form for previously used small-scale binary tree topology. Although the work of SBP algorithm [vi] has been included briefly in this paper. The basic simulation environment is same as that of previous work i.e. use of the ndnSIM package [viii] which works with the NDN protocol structure with NS-3 network simulator. The previous work by Afanasyev et al. [vi] extended the ndnSIM for above mentioned algorithm with the metric used as "percentage of satisfied Interest for Legitimate users over malicious nodes". We have also used the ndnSIM package for extending the small-scale binary tree topology to Mixed topology (combination of tree & star) as mentioned in Fig. 7, whose structure consist of the Total 66 nodes overall, within that 32 nodes as leaf nodes 16 as gateway nodes in grey color and remaining as Backbone nodes which basically forwards the Interest displayed in black color. The attackers and the legitimate users are present at the leaf nodes. The colors of the attackers are red and green for the legitimate users. Since we have tried to run simulation with the random attack pattern which follows the uniform distribution i.e. affixed random variation within the no. of attackers. It is applied for worst case that attackers send the junk request as fast as possible which was assumed previously [vi]. The working of the routers has been set for the single-path Interest forwarding mechanism for the dedicated single producer displayed in blue color with the prefix under attack; only node which can satisfies all the Interests. Since the binary tree topology under worst case situation can defend the attacks as IFA [vi], so we have extended the binary tree topology [vi] to Mixed topology.

PROPOSED ALGORITHMIC VARIATIONS:

SIMULATION ENVIRONMENT: The simulation is performed over the ndnSIM package [viii], [xvi] as mentioned earlier by extending SBP algorithm [vi] for the Mixed topology as depicted in Fig.7. The delay is being set as 80 mS, and the data size is 1100 bytes for the simulation performed in each run. The bandwidths

allotted to each link are 10 Mbps and the random propagation delay is being set within multiple values between 1 Mbps to 10 Mbps. The previous work [vi] use the percentage of attackers from 6% to 50% but this work focuses over the study of SBP algorithm at higher attacker percentage levels i.e. from 45% to 68.7% and then observe the satisfaction percentage of the legitimate users. Also we have changed the network topology which can give various results as well. The attack time exist near to 5 min and 9 runs each for each of percentage attack. At the time of attack the Average Interest satisfaction percentage is being calculated. We plot the Average Interest Satisfaction ratio in 1min, with attackers varying in no. from 14 to 22 out of total 32 leaf nodes and displayed with the help of Fig. 8.Graph for the Satisfied Interest from the single producer-root node is given in Fig. 9.

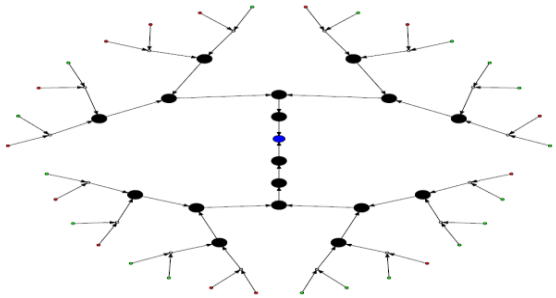

Fig. No.7.Mixed Topology with legitimate & malicious users

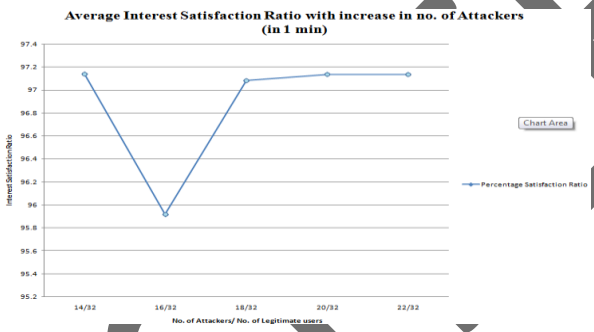

Fig. No.8.Average Interest Satisfaction Ratio in 1 min for attack of 45% to 68.7 %

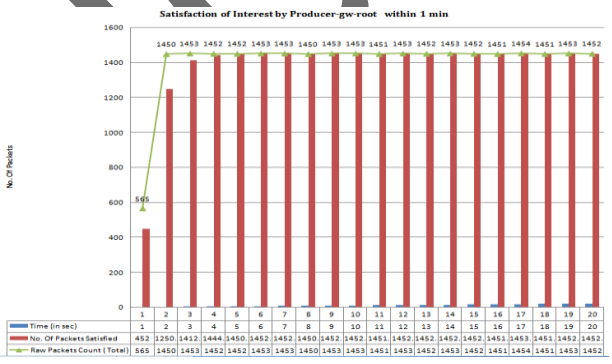

Fig. No.9. Satisfied Interest by Single Producer-root within 1 min.

RELATED WORK:

The various approaches for the mitigation of the IFA are having impactful and preventive measures. The key focus of these research works was to detect the IFA and to overcome the IFA attacks. IFA is a major cause for the blocking the legitimate interests and forwarding the adversarial interest most of the time which can increase the processing overhead as well, as mentioned by Choi et al.[iv]. The adversaries try to attack statically, dynamically, or randomly to the server or the router which is probably having the information, so the router statistics observation i.e. detection of the unfulfilled entries and further throttling of PIT for inbound interest and reporting this issue to nearby routers denotes that PIT is full [xxiv] which can help in the Pushback Mechanism which is used for the adversarial interest as given by Gasti et al. [vii]. The various concerns like content and cache based privacy; Signature based and name privacy issues and their potential solutions like hierarchical bloom filter for the detection of interest in namespace format was given. Since the interest available are returned directly but unavailable interest are searched in the bloom filter entries and corresponding PIT entries are searched, if entry is found the counting bloom filter increases count and thus if the interest are not found by any means the bloom filter entries are searched from end to start until some entry is being found which can reduce overhead of size on PIT structure this was suggested by Abdelberi et al.[ix]. The other work is proposed as Poseidon which is algorithm which can be implemented and executed over the routers for observing various traffic anomalies, IFA, per interface traffic rate and unsatisfied interest as well. This algorithm can ensure that IFA is controlled if within the consecutive interfaces any IFA is observed then alert message can be generated for it over the corresponding path which was proposed by Compagno et al. [x],[xiii] proves as hindrance for IFA. Another implementation proposed by Afanasyev et al. [vi] which is having intelligent mitigation of IFA through the traffic symmetry observation in Named Data Network (NDN) which is an either form of CCN by the application of pushback mechanism through the SBIA, SBP algorithms which ensured the maximum prevention under the IFA attack scenario and which also acts as conceptual initiation for the current work presented by us for Mixed Topology. Further classifying the forwarding based attacks there can be two types of attacks as FIB based IFA and broadcast based IFA given by Tang et al. [xi], in which method of two phase detection algorithm for IFA was focused. In this algorithm initial rough detection is

performed with the Relative Strength Index (RSI) for each per interface and the initial threshold against it, if threshold exceeds then the identification for the unsatisfied interest can be done with the help of the expired name prefix and its corresponding expired ratio. Next approach for the IFA reduction was the implementation of the algorithms like Non Cluster Mode Algorithm (NCMA) (2) Cluster Mode Algorithm (CMA) (3) Terrain Information table (TINT)-CMA Algorithm and their comparative study by Ekambaram et al. [xii]TINT proves to be the better algorithm than CMA. Since the TINT-CMA maintains the terrain information table on each higher gateways and backbone routers, the router has the mechanism to check the correct path thus the adversarial interest if not found primarily at the higher gateway it can't enter to associated routers. Thus memory requirement is greater in TINT but its size at each router is small. An important study in the CCN, NDN and IFA issues are as shown in Table No.1.

CONCLUSION AND FUTURE SCOPE OF WORK:

In this paper, we have focused mainly over the newer architecture as CCN and its various advantages as naming, security of content, redundancy control, signature algorithms, and flow control etc. The various adversarial attacks can harm the on-going communication, DoS attack as IFA and other attack patterns [v-vii], [ix-xv] in CCN are also observed concentrating over the major issues of IFA. The related work presented deals with the various attack patterns via IFA and various IFA mitigation strategies and algorithms as applied [v], [vii], [xxvi]. The proposed variation algorithm focuses over the implementation of the SBP algorithm and its strategies over Mixed topology and the study over the observed facts and results with the increase in the no. of malicious nodes within the topology through experiment [viii], [xvi]. Lots of finer steps can be taken to resolve the IFA issue using the cache & collaborative approaches [xvii-xxiii] of the nearby nodes. The CCN is having all the possible aspects, issues which are moreover lesser as compared to the current internet architecture issues [iv]. Today the convenience and ease for the communication is having much higher concern and CCN can prove to be a better counterpart for the communication via internet giving benefit to the user through its implementation. In Future Project can be extended with the dynamic attack scenarios and the variation of malicious nodes to have the more realistic analysis and idea with the larger no. of nodes, delay & bandwidth variation. The scope of the CCN is much vaster which will increase with the incremental implementation and developments within the CCN and NDN platforms which can further can meet the need of networking paradigms to increase with attack prone mechanisms and secure access.

TableNo.1 Brief Overview of Related Work & their Merits

No.	Related Works on CCN & IFA By various Authors	Merits
1.	Van Jacobson et al. [i]	Proposed CCN, NDN
2.	Priya Mahadevan [iv]	CCN details & Advantages
3.	Seungoh Choi et al.[v]	Adversarial attacks & results
4.	Afanasyev et al.[vi]	IFA attacks & their Solutions in different topologies, with the help of various implemented algorithms
5.	P. Gasti et al. [vii]	Important attack types like DoS, DDoS, their Classification
6.	Abdelberi et al.[ix]	Cache-privacy issues & Solutions
7.	Alberto Compagno et al.[x]	Poseidon Algorithm for alerts regarding IFA over routers & traffic patterns.
8.	V. Ekambaram and K. Sivalingam [xii]	IFA, Clustering Algorithms for IFA Mitigation
9.	Master Thesis by T. Lauinger [xv]	Gives Various Attacks like IFA etc.
10.	Gergely Acs et al. [xxi]	Cache Privacy Issues
11.	Jason Min Wang et al. [xxii]	Cooperative Caching & Caching Solutions
12.	Van Jacobson et al. [xxv]	NDN, Tech. Report

REFERENCES:

i. Van Jacobson et al. "*Networking Named Content*" ACM CoNEXT'09,December 2009, Rome, Italy ACM 978-1-60558-636-6/09/12, pp. 1–4, 2009.
ii. CCN Project CCNx™,<http://www.ccnx.org/>, September 2009.
iii. Named Data Networking (NDN) Project, <http://www.named-data.net/>,2010.

iv. Priya Mahadevan "*CCNx 1.0 Tutorial"*, Palo Alto Research Centre (PARC), 16 March, 2014.

v. Seungoh Choi et al. "*Threat of DoS by Interest Flooding Attack in Content centric Networking*", IEEE, 2013.

vi. Afanasyev et al. "*Interest Flooding Attack and Countermeasures in Named Data Networking*", IEEE, 2013.

vii. P. Gasti et al. "*DoS & DDoS in Named-Data Networking*", arXiv preprint arXiv: 1208.0952, 2012.

viii. A. Afanasyev, I. Moiseenko and L. Zhang, "*ndnSIM: NDN simulator for NS-3*," NDN, Technical Report NDN-0005, 2012.

ix. Abdelberi et al. "*Privacy in Content-Oriented Networking: Threats and Countermeasures*", ACM SIGCOMM Computer Communication Review Vol. 43 N0.3, July 2013.

x. Alberto Compagno et al. "*Poseidon:Mitigating Interest Flooding DDoS attacks in Named Data Networking*", IEEE, August 2013.

xi. Jianquiang Tang, Zhongyue Zhang, Ying Liu, Hongke Zhang, " *Identifying Interest Flooding in Named Data Networking*", IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, 2013.

xii. Vijay Ekambaram and Krishna M. Sivalingam. "*Interest Flooding Reduction in Content Centric Networks*", IEEE 14th International Conference, 2013.

xiii. Alberto Compagno, Mauro Conti, Paolo Gasti, Gene Tsudikz, "*NDN Interest Flooding Attacks and Countermeasures*", IFIP Networking Conference, IEEE, 2013.

xiv. D. Smetters and V. Jacobson, "*Securing network content*", PARC, Technical. Report, October 2009.

xv. T. Lauinger "*Security & Scalability of Content Centric Networking*", Master Thesis TU Darmstadt, 2010.

xvi. A. Afanasyev et al., ndnSIM-ddos-interest-flooding Project, GitHub Repository, <https://github.com/cawka/ndnSIM-ddos interest-flooding/>, 2013.

xvii. Tobias Lauinger et al. "*Privacy Risks in Named data Networking: What is the Cost of Performance?*", ACM SIGCOMM Computer Communication Review, Volume 42 , No. 5, October 2012.

xviii. Yusung Kim, Ikjun Yeom. "*Performance analysis of in-network caching for content-centric networking"*, Computer Networks 57(2013), , ELSEVIER, 8th April 2013, pp. 2465-2482.

xix. L. Deng, Y. Gao, Y.Chen, and A. Kuzmanovic, "*Pollution attacks and defenses for Internet caching systems,*" Computer Networks, vol. 52, No. 5, 2008, pp935-956.

xx. Y. Gao, L. Deng, A. Kuzmanovic, and Y. Chen, "*Internet cache pollution attacks and countermeasures*," in ICNP, IEEE Computer Society, 2006, pp. 54-64.

xxi. Gergely Acs, Mauro Conti, Paolo Gasti, Cesar Ghali, Gene Tsudik, " *Cache Privacy in Named-Data Networking*" , IEEE 33rd International Conference on Distributed Computing Systems, 2013.

xxii. Jason Min Wang, Jun Zhang, Brahim Bensaou, "*Intra-AS Cooperative Caching for Content Centric Networks*", ICN' 13, 12th August 2013.

xxiii. Konstantious Katsaros, George Xylomenos, George C. Poyzos, "*MultiCache: An overlay architecture for information-centric networking*", INFOCOMM IEEE Conference on Computer Communications Workshops, 2010.

xxiv. Kai Wang, Huachun Zhou, Yajuan Qin, Jia Chen, Hongke Zhang. "*Decoupling malicious Interests from pending Interest table to mitigate Interest Flooding Attacks*", Globecom Workshops (GC Wkshps), IEEE, 2013.

xxv. Van Jacobson et al. "Named Data Networking Project" Technical Report NDN-0001, October 2010.

xxvi. Rohit Agnihotri, Kshitij Pathak, Dr. Prashant Bansod, Chetan Chouhan, "*Content Centric Networking And Interest Flooding In Communication Networks: A Review*", International Conference on Advances in Computers, Communication and Electronic Engineering", ISBN: 978-93-82288-54-1 COMMUNE, 16–18 March 2015, pp. 280-285.