Computer and Telecommunication Engineering 2024, 2(2), 2669.
https://doi.org/ 10.54517/cte.v2i2.2669

Article

CORE: Counteracting overwhelming requests effectively—A method for ınterest flooding attack mitigation in NDNoT

Sedat Bilgili[1,*], Gökçe Ertit[2,*], Alper Kamil Demir[1,*]

[1] Computer Engineering, Alparslan Türkeş Science and Technology University, Adana 01020, Turkey
[2] Electric Electronic Engineering, Alparslan Türkeş Science and Technology University, Adana 01020, Turkey
*** Corresponding authors:** Sedat Bilgili, sbilgili@atu.edu.tr; Gökçe Ertit, gokcemanap@gmail.com; Alper Kamil Demir, akdemir@atu.edu.tr

CITATION

Bilgili S, Ertit G, Demir AK. CORE: Counteracting overwhelming requests effectively—A method for ınterest flooding attack mitigation in NDNoT. Computer and Telecommunication Engineering. 2024; 2(2): 2669. https://doi.org/10.54517/cte.v2i2.2669

ARTICLE INFO

Received: 7 April 2024
Accepted: 23 May 2024
Available online: 12 July 2024

Abstract: The Named Data Network (NDN) is a promising architecture for the near future. NDN communicates by naming data, unlike IP-based Internet architecture. Architectural understandability, ease of use, security, content presentation and simplicity of data exchange logic make this architecture preferable. The NDNoT approach, which recently combines IoT and NDN, enables Internet of Things applications using NDN naming conventions and basic data structure. However, increasing technological applications bring security vulnerabilities. In this study, we propose a new method called CORE that will secure the intended data transfer. The presented CORE mechanism was developed as a countermeasure against the Interest Flooding attack, one of the NDN security attacks. Tests were carried out in the Cooja simulation environment using three different topology scenarios. CORE's performance metrics were evaluated based on success rate, average delay and Interest traffic. The results showed that when the CORE mechanism was active, there was an improvement in the success rate and average delay. In terms of Interest traffic, at least a 70% success rate was achieved compared to scenarios in which the CORE mechanism was not operated.

Keywords: Named Data Networking of Thing (NDNoT), interest flooding, contiki, cooja

1. Introduction

Technology and science move forward because new design approaches are emerging. In such, how we communicate changed from a host centric approach to a content (information, data) centric approach. Today's TCP/IP based Internet was designed for point-to-point communication for IP packet exchange where IP data packets are generated generally on end-hosts and associated with IP addresses without any interrelations between data and address. The fundamental idea is to deliver data packets from one source IP address to destination IP address [1]. However, the current demand of the Internet has shifted from host-centric resource or information sharing to content-centric resource or information sharing. Named data networking (NDN), related to information-centric networking (ICN) [2], content-based networking, data-oriented networking or information-centric networking, is one of proposed Future Internet Architecture (FIA) motivated by years of observational research into network design for unsolved problems of contemporary internet architectures like Internet Protocol (IP) [3]. NDN is designed with this trend where it focuses addressing data rather than individual hosts (nodes or devices). For example, as a solution, the need for accessing content in today's IP world has been facilitated via Content Delivery/Distribution Network (CDN) and Peer-to-Peer (P2P) as an overlay on top of IP [4].

The Internet of Things (IoT) concept describes attaching everyday objects having processing, sensing, actuating and communication abilities with other devices and systems over the Internet [5]. The enormous set of applications have been introduced into our daily life with the IoT notion [6]. Before the ICN approach, the Internet protocol suite has been adapted as a natural design choice for IoT architecture. However, the research showed that the data centric design approach of ICN suits better for IoT applications [7]. Therefore, the Named Data Networking of Things (NDNoT) framework has been realized as an alternative design method for IoT architecture [8,9]. The results indicate that NDNoT approach suits and fits better to design networked applications for those everyday objects.

Various protocols and adaptation layers that can impose heavy burdens on restricted devices are unnecessary in the NDN network. The fact that the NDN network does not require the use of TCP/IP as in IP is advantageous for many IoT devices [10]. Thanks to less resource consumption, the NDN protocol stack is well-suited for resource-constrained IoT networks. The concept of Named Data Network of Things (NDNoT) [8,9]refers to the combination of NDN protocol stack with IoT network, which has less resource/memory consumption. However, NDN architecture also has its own challenges. Since this architecture is based on a fundamentally different data structure and data flow logic, it requires new developable solutions. Inheriting the basic data structure and features of NDN, NDNoT network automatically adopts vulnerabilities and attacks. Therefore, solutions to existing security vulnerabilities in the NDN network can also be adapted to the NDNoT network.

The transition to content-centered data exchange brings with it various security problems. NDN needs new solutions against unique attack threats and vulnerabilities that require its own defense mechanism. These new solution efforts appear as important investments in the future of NDN.

One of the most popular attacks in NDN networks is the Interest Flooding attack [11–14]. In this type of attack, the attacker node sends a large number of interest packets to occupy and neutralize the target node. This directs interest packets to search for data that is not available on the network. Interest packets that have no response and circulate in large numbers in the network keep the network nodes busy and tire the network. When we consider such a scenario, since the devices in the NDNoT network have limited resources, memory and bandwidth, the network becomes significantly unable to function properly and the communication quality is negatively affected.

Data naming is an important issue in NDN. A well-designed naming scheme facilitates mechanisms such as routing and caching. On the other hand, in NDN security attacks, the lack of naming scheme rule information may go unnoticed by the attacker. In scenarios where the attacker does not care about naming rules when producing randomly generated Interest packages, Interest packages are ignored when they do not comply with the canonically created naming structure. We proposed a new approach to attacker blocking methods with the CORE mechanism. The naming structure designed specifically for the application ignores Interest packages that do not comply with this rule. In this case, the attacker’s idea of generating a large number of random Interest packets and occupying the network is refuted.

We provided Materials and Methods that used in this study in Section 2. Section 3 details the proposed CORE mechanism. We focused into Simulation Environment in Section 4 and Results in Section 5. Finally, in Section 6, we concentrated on Conclusion & Discussion.

2. Materials and methods

2.1. Named Data Networking (NDN)

Information Centric Networking (ICN) [2]promotes a communication model that is fundamentally different from the traditional IP address-centric model. The ICN approach consists of retrieving content with (unique) names. Named Data Network (NDN) [3,15]is derived from the CCN (Content Centric Network) approach under the umbrella of ICNs (Information Centric Networks). NDN addresses data rather than addressing nodes in the network.

The basis of the IP network is location-based. Everything has an IP address that identifies "where" its location is. However, in information-centered network architecture, there is an approach that describes the content rather than using "where" IP addresses. In fact, NDN and IP architectures fundamentally share the same layered hourglass architecture. The difference of IP architecture is that in the OSI data exchange model, the Internet Protocol (IP) is located at the Network layer. There is no need for IP addresses in the NDN model. Therefore, source and destination IP address and port overhead and requirement are eliminated.

NDN offers location-independent naming for searching and retrieving the content of a requesting user [15]. It uses data packets containing content names instead of source and destination addresses. It uses a naming convention created directly by the application and expressed in variable lengths. Data packets are independent of each other and where they are received and where they are transmitted is completely independent. NDN architecture with these features also helps caching content within the network to meet future demands and needs and also supports consumer/data mobility [16].

In NDN, communication is accomplished through the exchange of two types of packets: Interest and Data. Both types of packets carry a name that identifies a piece of data (prefix) that can be transmitted in a Data packet. Routers use this name to transmit Data of Interest.

NDN policy

Each node in the NDN architecture contains three basic data structures; Content store (CS), Pending Interest Table (PIT), and Forwarding Information Base (FIB). The Content Store maintains a table of records of named data. It is a caching mechanism. Pending Interest Table is the table that keeps records of Interest information that has not yet been answered and has been transmitted. Interest packets can be requested by more than one interface. Forwarding Information Base is a routing table that holds records that route data names or prefixes to interfaces.

A requested data is sent as an Interest packet. The router queries whether this Interest package exists in the Content Store (CS). If the requested data is not available in the CS, the NDN node queries the Pending Interest Table (PIT) to check if there is

a previous request for the same data. If there is a PIT entry for this data before, this data has already been requested. If there is no previous record from this interface, the interface to which the Interest Package reaches is added to the interfaces table at the PIT entry. The router then queries the Forwarding Information (FIB) to determine the path to where to forward the Interest. When correct data transmission occurs with appropriate routing protocols, the Interest is forwarded to a node containing data. The content is sent back to the Data Packets, taking the opposite path to the requesting Interest Packet.

2.2. Named data networking of things

NDNoT networks consists of resource and memory constrained devices that has different types of network traffic and small data exchange [9]. Our NDNoT design includes the basic data structures and functions required by the NDN architecture [17]. NDNoT combines the basic principles of IoT network and NDN architecture. It aims at both the transmission of Interest and Data packets of content-based networks and the communication of resource-constrained devices with each other according to NDN logic [18].

Naming data

Naming scheme is important in NDN. It has implications for data availability, expression of user requests, data retrieval, and security [19]. Naming ability also affects how long it takes to obtain the desired data [20]. There are several naming variants in NDN. Flat naming, hierarchical naming, hybrid naming are a few of these examples. Various naming schemes are available in the literature. The naming structure used in this study is hierarchical.

Packet types

NDN architecture contains two packet types; Interest and Data. Interest packets can be characterized as data-seeking packets. In NDNoT, Interest is a packet type that contains 6-byte header information and 24-byte name ex pressing requested data. Data packets containing the requested data (max. 72-bytes) have 6-byte header and 24-byte name information.

Data Structures in NDNoT

NDN contains three kinds of tables to forward the Interest and data packets; PIT (Pending Interest Table), FIB (Forwarding Information Base) and, CS (Content Store).

PIT (Pending Interest Table): PIT table is the data structure in NDN architectures where Interest packet information is kept.

FIB (Forwarding Information Base): The FIB table is a data structure that keeps the addresses where the searched data can be, paired with data names or prefixes. In NDNoT, the FIB table works with prefixes instead of full names. Thus, when another data with the same prefix is searched, it is known where it might be.

CS (Content Store): Content Store is the table where named data is kept. When an Interest package arrives, the first area to check on the network is the Content Store. If the requested data has a record in the content store, it returns the data directly. Although the data in this table is mostly managed by the application layer, mechanisms such as caching can also modify this table. Data in CS can be generated statically or dynamically, depending on the application layer.

3. CORE mechanism

In the architecture of Named Data Networking (NDN), giving attention to data naming can be a critical aspect. The process of categorizing data according to specific naming conventions is foundational. Effective implementation of a well-designed naming scheme not only facilitates mechanisms such as routing and caching but also optimizes the operation of pivotal components like PIT/FIB tables. Moreover, the adoption of systematic naming patterns within NDN infrastructure extends beyond mere organizational convenience; it establishes a standardized framework that enhances interoperability and facilitates efficient data retrieval and dissemination processes across diverse network environments. Consequently, the utilization of coherent naming schemas serves not only as a practical strategy for managing data but also as a fundamental principle guiding the architecture's functionality.

In NDN networks, when considering interest flooding attacks, it is conceivable that the attacking node may lack knowledge about the network and, consequently, the NDN naming scheme. In such a scenario, the attacking node can propagate Interest packets containing randomly generated Data names, which, in reality, do not correspond to any actual Data. Consequently, this situation prompts nodes to search for a nonexistent data packet, leading to the generation of intensive network traffic.

A well-defined naming scheme enables nodes in a network to verify the appropriateness of the naming scheme in the Interest packets they receive when shared among knowledgeable nodes in the network. Consequently, they can prevent an increase in network traffic by dropping packets that do not correspond to Data packets, thus thwarting the efforts of malicious nodes attempting to manipulate the network.

The CORE mechanism we propose operates based on a naming scheme. Incoming Interest packets are forwarded within the network according to compliance with the designated naming scheme defined within the mechanism; otherwise, they are dropped. As an example, consider a naming scheme where categories are separated by the '/' symbol. In such a scheme, a naming such as "node/data/health" would be considered correct (safe) for a Data packet. In the mechanism we propose, it is possible to use a naming scheme other than the one given in the example. In summary, the Core mechanism checks whether Interest names adhere to a specific pattern. Due to its low system requirements, the Core mechanism is highly suitable for IoT devices with limited hardware.

The algorithm of the proposed Core mechanism is presented in Algorithm 1. An example network is provided in **Figure 1**. In this example scenario, it is assumed that node 3, which is unaware of the naming scheme used in the network, is a malicious node. Node 3 continuously generates Interest packets with random Data names in order to slow down or render the network unusable. In the absence of the Core mechanism, nodes 2, 4, and 9, which are neighbors of node 3, will forward these Interest packets to their neighbors in search of the nonexistent Data packet. As a result, the nodes in the network will expend time, energy, processing power, and bandwidth searching for a nonexistent Data packet. However, when the Core mechanism is active, nodes 2, 4, and 9 will ignore these Interest packets if they do not match to the naming pattern when examining the packets received from node 3. Thus, other nodes in the network will not waste resources searching for nonexistent Data packets.

Algorithm 1 Pseudo code of proposed CORE algorithm

```
1: while Node running do
2:    if Received Interest packet from a neighbor then
3:       if InterestName matches pattern then
4:          if contentStore has corresponding Data then
5:             forwardData
6:          else
7:             add/update PIT entry
8:             forwardInterest
9:          end if
10:    else if Received Data packet from a neighbor then
11:       if DataName matches the pattern then
12:          if PIT has corresponding Entry
13:             forwardData
14:          else
15:             Drop packet
16:          end if
17:       end if
18: end while
```

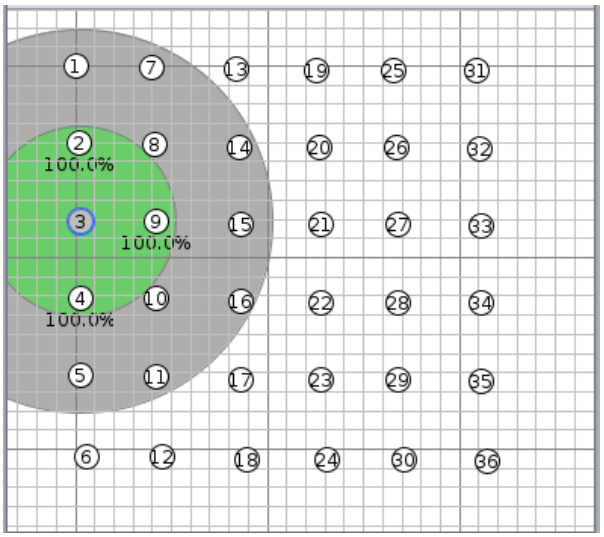

Figure 1. Example network topology with 36-nodes.

In NDNoT, there are limited studies in the literature on preventing/mitigating interest flooding attacks. Due to the limited resources of NDNoT environments, it is not possible to implement most of existing methods in NDN environments. The proposed CORE mechanism is capable of operating in NDNoT environments with limited resources without excessive resource consumption. In summary, the proposed CORE mechanism aims to minimize the negative effects of potential interest flooding attacks in NDNoT environments with limited resources.

4. Simulation environment

Contiki NG OS and Cooja simulator

Contiki OS is an open source operating system used for embedded devices with limited power and memory [21]. It operates at low power and has standard protocols that allow data exchange. It supports working on embedded systems, rapid prototyping and testing of applications. The platform used in this study, Contiki NG operating system, is the most current version of Contiki OS.

Cooja network simulator is a simulator that supports Contiki NG OS and is compatible across platforms [22]. It is mostly used for wireless sensor networks. This environment is a Java-based network simulator that simulates network implementation of various power and memory constrained devices.

In our simulation tests, we designed a grid topology with the number of nodes as 16, 25 and 36. All of our three-scenario network topology design consists of grid topology type. At the same time, all tests were repeated 3 times. In all three topology scenarios, only one of the nodes acts as the attacker node. Additionally, all nodes are producers.

The variables and their values used in the simulations are presented in **Table 1**.

Table 1. Simulation variables.

Node Count	16, 25, 36	Forwarding Mechanism	RONR
Interest Packet Size (bytes)	55	Data Packet Size (bytes)	127
Max. PIT Entries	128	Max. FIB Entries	36
Request Rate (ms)	400–1100	Attack Rate (ms)	25–100
Total Requests	100 * (NodeCount-1)	TTL	16

5. Results

5.1. Success rate

The success rate metric represents the percentage of the ratio of the number of interest packets in the network to the responses to interest packets, that is, the number of data packets. It is assumed that a corresponding data packet exists for each Interest packet.

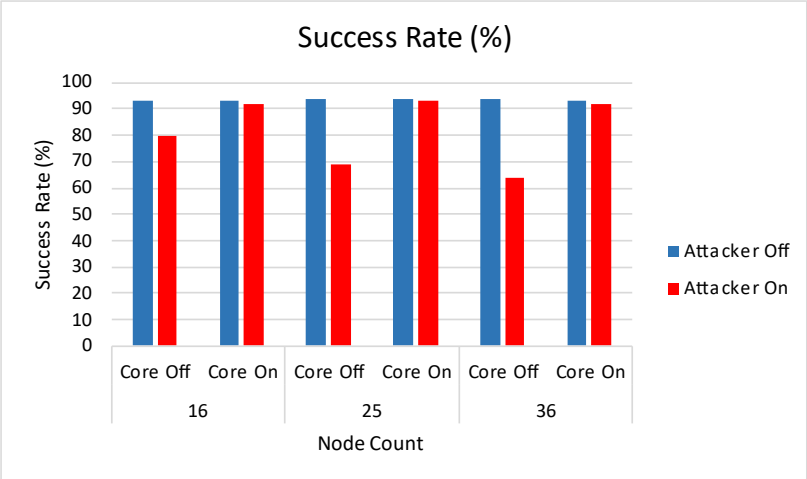

Figure 2. Succes rate results with 16, 25 and 36 nodes.

Naturally occurring losses such as non-availability of data, corruption and loss of Interest and Data packages are ignored. This is because it accurately tests the success of the CORE mechanism. As seen in **Figure 2**, blue columns indicate that there is no attacker, and red columns indicate that there is an attacker node in the network. At the same time, scenarios where the CORE mechanism is active refer to CORE on, and scenarios where it is passive refer to CORE off situations.

Our results show that the CORE mechanism is successful in networks where the attacker exists. In scenarios where the attacker is active, the number of Interest packets increased. The circulation of fake Interest packets in the network has made it difficult for real Interest packets to reach the relevant node. Therefore, data loss occurred. However, we see that in all three scenarios, the success rate when CORE is active is higher than the success rate when CORE is passive.

5.2. Average latency

This metric expresses the average time in ms between the delivery of the Interest packet propagated through the network and the Data packet returned against it. While the attacker is active, more Interest is circulating in the network, resulting in more intense network traffic, which naturally increases the average delay. At the same time, as seen with both the activeness of the attacker and the increase in the number of nodes, the delay increased even more. As we see in **Figure 3**, the average delay in scenarios when the CORE mechanism is active is lower than in scenarios when CORE is passive.

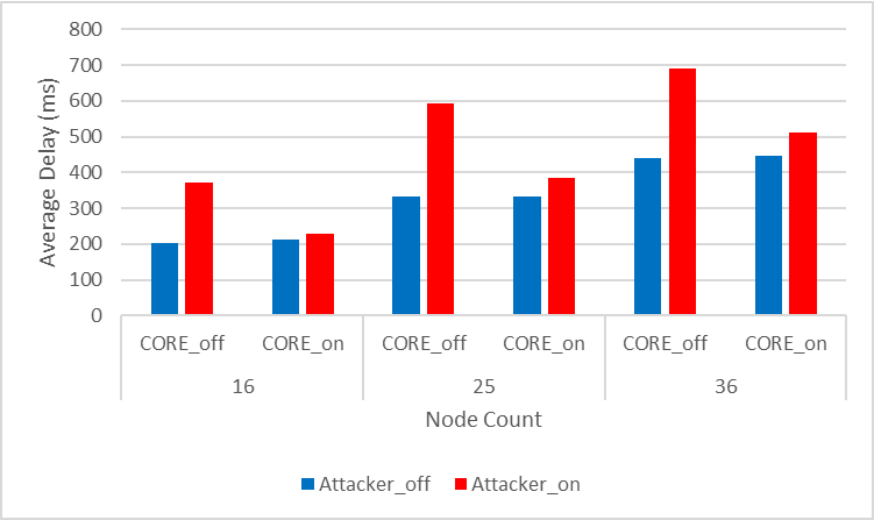

Figure 3. Average delay results with 16, 25 and 36 nodes.

5.3. Total interest traffic

This metric expresses the total size of Interest packets in the network in KB. Scenarios in which the attacker was active in the network contained more Interest packets, resulting in more intense network traffic. Moreover, it is clearly seen in **Figure 4**, that as the number of nodes increases, the Interest packet density increases. The CORE mechanism reduced this network traffic load by at least 70% in all three scenarios.

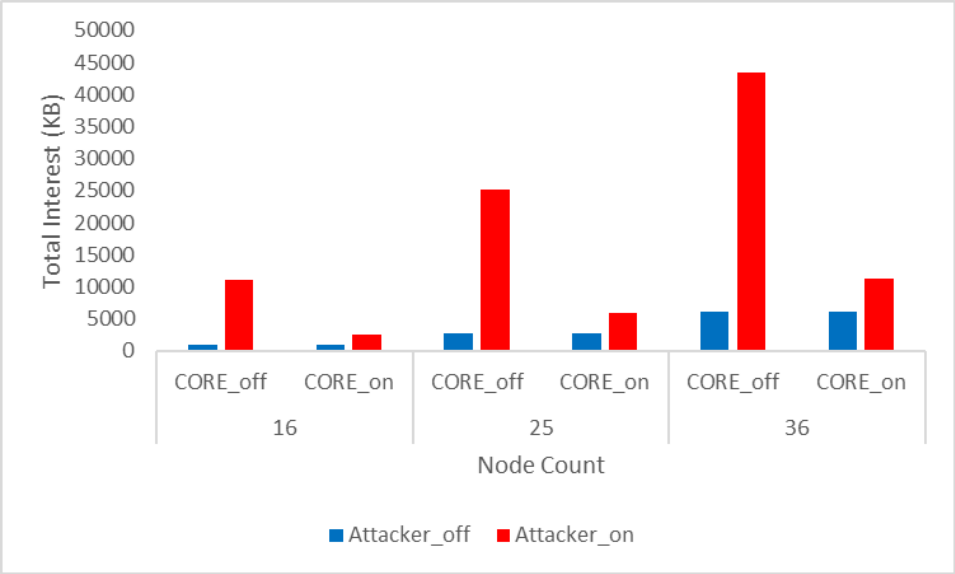

Figure 4. Total interest traffic results with 16, 25 and 36 nodes.

6. Conclusion and discussion

In this study, a defense mechanism is presented against the Interest Flooding attack by abusing the normal data exchange logic of the NDN architecture, which can operate in Internet of Things networks. At the same time, this study may shed light on the future as an overview of the NDNoT approach. In the study, we presented the prominent features and advantages of the NDN network. We have presented a detailed and descriptive description of the NDNoT network, clearly expressing its basic data structure and operating logic. NDNoT provided a modern and practical perspective by adding NDN characteristics to IoT applications that will shape the future. Naturally, from this perspective, as a result of increasing applications and data, it brought new problems or attacks.

CORE appears as a precaution and defense mechanism against Interest Flooding attacks. By disabling randomly generated Interests that do not comply with the naming rule, this mechanism does not tire the network traffic and does not occupy the nodes unnecessarily. Our results show that when working with the NDN basic structure (when CORE is not active), when the attacker is active in the network, there is an intense Interest packet traffic, the delay increases and naturally the data exchange success decreases. With the operation of the CORE mechanism, this Interest attack was reduced, there was no significant delay and the total Interest traffic was reduced by 70%.

This study can be seen as a part of more comprehensive studies that can give hope for the future. In particular, it can provide a basis for precautions and studies that can be taken against Interest Flooding attacks. The CORE mechanism has shown us that it is not only a precaution against attacks, but also the importance of an effective naming structure for the protection of the network. In addition to protecting the network, it also allows increasing data exchange efficiency and quality. Our future goal is to develop and advance this work. This study showed us that it is possible and successful to design stronger and more robust defense mechanisms in NDNoT.

Author contributions: Conceptualization, SB, GE and AKD; methodology, SB; software, SB; validation, GE and AKD; formal analysis, GE; investigation, SB, GE and AKD; data curation, SB and GE; visualization, GE; supervision, AKD; project administration, AKD. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

1. Arjunwadkar DP. Introduction of NDN with Comparison to Current Internet Architecture based on TCP/IP. International Journal of Computer Applications. 2014; 105(5): 31-35. doi: 10.5120/18376-9536
2. Ahlgren B, Dannewitz C, Imbrenda C, et al. A survey of information-centric networking. IEEE Communications Magazine. 2012; 50(7): 26-36. doi: 10.1109/mcom.2012.6231276
3. Zhang L, Afanasyev A, Burke J, et al. Named data networking. ACM SIGCOMM Computer Communication Review. 2014; 44(3): 66-73. doi: 10.1145/2656877.2656887
4. Passarella A. A survey on content-centric technologies for the current Internet: CDN and P2P solutions. Computer Communications. 2012; 35(1): 1-32. doi: 10.1016/j.comcom.2011.10.005
5. Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Computer Networks. 2010; 54(15): 2787-2805. doi: 10.1016/j.comnet.2010.05.010
6. Asghari P, Rahmani AM, Javadi HHS. Internet of Things applications: A systematic review. Computer Networks. 2019; 148: 241-261. doi: 10.1016/j.comnet.2018.12.008
7. Aggarwal CC, ed. Managing and Mining Sensor Data. Springer US; 2013. doi: 10.1007/978-1-4614-6309-2
8. Shang W, Bannis A, Liang T, et al. Named Data Networking of Things (Invited Paper). 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI). Published online April 2016. doi: 10.1109/iotdi.2015.44
9. Zhang Z, Lu E, Li Y, et al. NDNoT. Proceedings of the 5th ACM Conference on Information-Centric Networking. Published online September 21, 2018. doi: 10.1145/3267955.3269019
10. Aboodi A, Wan TC, Sodhy GC. Survey on the Incorporation of NDN/CCN in IoT. IEEE Access. 2019; 7: 71827-71858. doi: 10.1109/access.2019.2919534
11. Rai S, Dhakal D. A survey on detection and mitigation of interest flooding attack in named data networking. Springer, Singapore ; 2018.
12. Hidouri A, Hajlaoui N, Touati H, et al. A Survey on Security Attacks and Intrusion Detection Mechanisms in Named Data Networking. Computers. 2022; 11(12): 186. doi: 10.3390/computers11120186
13. Afanasyev A, Mahadevan P, Moiseenko I, et al. Interest flooding attack and countermeasures in named data networking. In: 2013 IFIP Networking Conference; 2013; Brooklyn, NY, USA. pp. 1-9.
14. Lee RT, Leau YB, Park YJ, et al. A Survey of Interest Flooding Attack in Named-Data Networking: Taxonomy, Performance and Future Research Challenges. IETE Technical Review. 2021; 39(5): 1027-1045. doi: 10.1080/02564602.2021.1957029
15. Saxena D, Raychoudhury V, Suri N, et al. Named Data Networking: A survey. Computer Science Review. 2016; 19: 15-55. doi: 10.1016/j.cosrev.2016.01.001
16. Feng B, Zhou H, Xu Q. Mobility support in Named Data Networking: a survey. EURASIP Journal on Wireless Communications and Networking. 2016; 2016(1). doi: 10.1186/s13638-016-0715-0
17. Bilgili S, Demir AK. A Named Data Networking Stack for Contiki NG OS. 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET). Published online March 3, 2022. doi: 10.1109/iraset52964.2022.9738034
18. Djama A, Djamaa B, Senouci MR. Information-Centric Networking solutions for the Internet of Things: A systematic mapping review. Computer Communications. 2020; 159: 37-59. doi: 10.1016/j.comcom.2020.05.003
19. Shannigrahi S, Fan C, Partridge C. What's in a Name? Proceedings of the 7th ACM Conference on Information-Centric Networking. Published online September 22, 2020. doi: 10.1145/3405656.3418717
20. Nurhayati A, Mayasari R, Ahdan S, et al. Naming Scheme on Named Data Networking: A Survey. 2022 8th International

Conference on Wireless and Telematics (ICWT). Published online July 21, 2022. doi: 10.1109/icwt55831.2022.9935350
21. Oikonomou G, Duquennoy S, Elsts A, et al. The Contiki-NG open source operating system for next generation IoT devices. SoftwareX. 2022; 18: 101089. doi: 10.1016/j.softx.2022.101089
22. Osterlind F, Dunkels A, Eriksson J, et al. Cross-Level Sensor Network Simulation with COOJA. Proceedings 2006 31st IEEE Conference on Local Computer Networks. Published online November 2006. doi: 10.1109/lcn.2006.322172