Privacy Preserving Participatory Sensor Network on Named Data Networking Infrastructure

M. Kaosar and X. Yi

Department of Computer Science and Software Engineering, RMIT University,
Melbourne, Australia

Abstract. The world of Internet of Things (IoT) and ubiquitous computing lead the computing systems integrate sensors and handheld devices into a common platform to offer new services. Participatory Sensor Network (PSN) is one of such a network which is formed in an ad-hoc basis. The success of such network always depends on the quality of data shared by the participants. Privacy concern is one of the main reasons why an individual may not prefer to share their sensitive data. Not many research works have been performed to preserve the privacy of individual data in a PSN. On the other hand, Named Data Network (NDN), an instance of Information-Centric Network (ICN), is an alternative of TCP/IP that inherently considers the concern of security as opposed to TCP/IP. By default, NDN ensures the privacy of the data consumer but it fails to ensure the same for data provider. In this paper, we propose a ring signature based NDN to ensure the privacy of the data provider. Our proposed solution seems to be effective based on the performance and security analysis.

Keywords: Named Data Networking, Participatory Sensor Network, Ring Signature, Information-Centric Network

1 Introduction

Making the good use of information is the essence of ICT itself. In other words, information itself cannot benefit if it is not harnessed properly. Participatory Sensor Network (PSN) is a dynamically formed network which depends on the data shared by participants. The growth of mobile devices such as smart phones, tablet computers, which have multiple sensors has increased the number of applications of PSN. Environmental database, weather forecasting, vehicular networks, cooperative societies, urban mobility, traffic congestion control etc. are some of the applications from endless possibilities that relies on the shared information in a PSN infrastructure. There are many challenges involved in PSN. Routing protocol, mobility management, security, privacy etc. are some of the challenges highlighted and some solutions provided in some of the research works - [1], [2], [3]. Privacy matters of PSN got attention in some works as well [4], [5]. But not many of them provide practical and efficient solution. Named Data Networking (NDN) [6] is an

DOI: 10.5121/ijwmn.2020.12101

alternative to TCL/IP that ensures some of the security aspects inherently by design. Naturally the question should arise, can NDN be used in PSN to resolve some of the security questions in PSN? But there is almost no work found to implement PSN on NDN infrastructure.

In this paper we propose a ring signature based NDN to preserve the privacy of data consumer and providers. This initiative is expected to encourage future research in the area of NDN based PSN applications. The rest of the paper is organized as follows: Section 2 discusses the necessary background information, section 3 discusses our proposed solution. Security of the proposed system is analyzed in section 4 and finally the paper is concluded in section 5.

2 Background

2.1 Participatory Sensor Network

In Participatory Sensor Network, the participating nodes join together to form a network in ad-hoc manner. As the popularity of Internet of Things (IoT) and ubiquitous computing increase, the research implication on PSN increases as well. Figure 1 briefly shows how the communication in a PSN is unsafe as intruders can intercept the communication between nodes. Many challenging issues in PSN can be explored in [7]. In this paper, we elaborate and provide a solution to the issue of participants' privacy. Since the participating nodes may belong to multiple owners, naturally they would not voluntarily participate if privacy is not preserved.

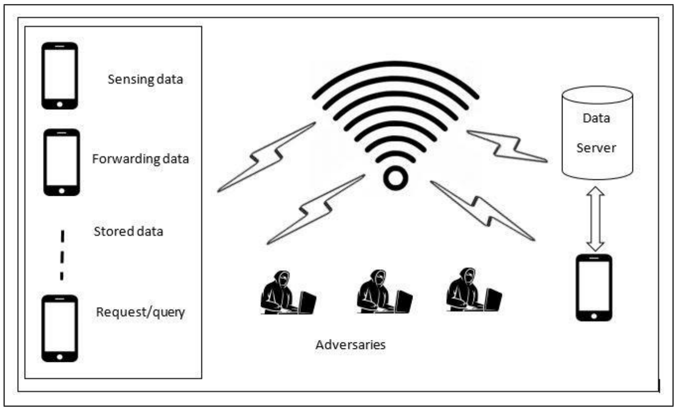


Fig. 1. A typical Participatory Sensor Network infrastructure

2.2 Privacy concerns in PSN

The data itself of a typical PSN can be secure enough in a sense that it is encrypted by the sender and only receiver can decrypt the data. But this does not ensure the privacy of the sender and receiver. There are several research works highlighting the privacy matters of such network using cryptographic techniques - [8], [9] and obfuscation technique - [4], [10], [11]. Though each of the techniques may have advantage over the other [12], we are not elaborating that in this paper as our objective is to ensure the privacy when PSN is deployed in NDN. Performance-wise the use of NDN in resource constrained networks like IoT is satisfactory [13] in terms of volume of data traffic and service delivery time.

Apart from the data itself, the privacy concerns in a PSN can be broadly classified into two categories:

- Location Privacy: Though the data shared by one node might be encrypted, it is not easy to hide the location of the node while preserving data integrity. The TCP/IP model keeps the source and destination IP address of every packet within the packet itself [14]. Some research works have been performed to secure the location privacy such as- [15],[16],[17] etc.
- Trajectory Privacy: Sometimes exact sensitive information of the node might be secure but it may reveal some other information which may help the adversary guess about some of the sensitive information. As for example, a node may secure its location but it may share the weather of the city it resides to the server. Now if the server has the weather forecasting of many cities, it can simply compare the weather and can guess about the location of the node. Some cryptography and trusted third party based solutions towards location privacy include [18], [19], [20] etc.

2.3 Named Data Networking

Before TCP/IP, the telephony used to deal point-to-point conversation between two parties. The solution offered by TCP/IP was immense and it was able to change the world drastically. The TCP/IP inherently designed without considering the security matter itself. This source and destination address/location centric approach has other problems as well, such as - scalability and mobility [6], [21].

These disadvantages of TCP/IP prompted researchers towards the concept of Information-Centric Network (ICN) [22]. NDN is a subset of ICN that identifies a chunk of data as the provider of information. In NDN project [6], NDN is described as layer of hourglass, same like that of Internet with some variations as depicted in figure 2 and discussed in detail in [21].

The data structure maintained, in each network device, by *NDN* has three major components as follows, also depicted in figure 4:

- Content Store (CS): This table keeps the valid data packet that is available to be used. If the requested data is found in CS table, the node can return the data and ignore the interest packet.

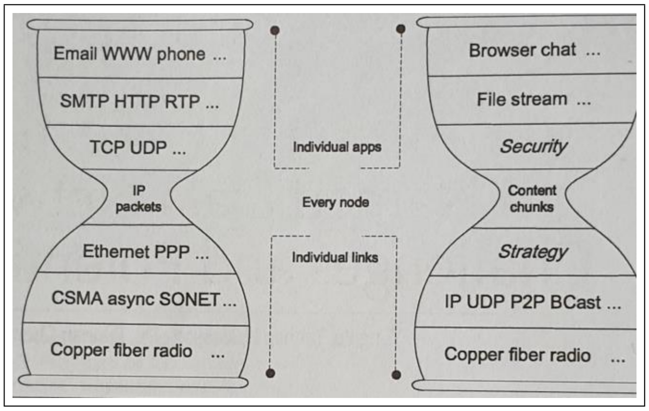


Fig. 2. Internet and NDN hourglass architecture [21]

- Pending Interest Table (PIT): If the requested data is not found in CS table, the node adds an entry in PIT to indicate that the response for this data is pending. Once the data is made available this entry is erased and the data is stored in CS.
- Forwarding Information Base (FIB): FIB works like a routing table. Based on the data name prefix, this table will indicate which face the Interest packet should be forwarded to.

There are two kinds of NDN packets - *Interest Packet* and *Data Packet*. When a consumer needs a data, it initiates the interest packet and sends to the router. When the router receives the requested data from the provider, known as the *Data Packet*, it forwards the packet to the consumer. A typical *InterestPacket* and *Data Packet* activities are depicted in the figure 3.

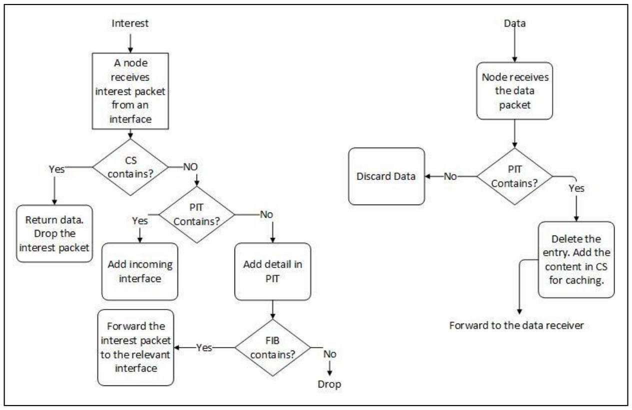

Interest
A node receives interest packet from an interface
CS contains?
Yes
NO
Return data. Drop the interest packet
PIT Contains?
Yes
No
Add incoming interface
Add detail in PIT
Forward the interest packet to the relevant interface
Yes
FIB contains?
No
Drop
Data
Node receives the data packet
PIT Contains?
No
Discard Data
Yes
Delete the entry. Add the content in CS for caching.
Forward to the data receiver

Fig. 3. NDN packet activity flow diagram

2.4 Privacy Concerns in NDN

The privacy concern of an NDN or content centric networking may arise in following areas [23].

- Content Privacy: The Deep Packet Inspection [24] of IP network is more applicable in the case of NDN since the data packets reside in routers which might be used by the attackers for analysis. In this paper we propose the ring signature based solution to address the content privacy.
- Signature Privacy: In NDN the signature and the data is coupled together to ensure data integrity. Attacker may learn easily about who produced a particular data. This signature privacy issue is also addressed in our proposed solution in this paper.
- Cache Privacy: In NDN data packets are cached in all the routers the data travel through. If the attacker analyze the timing of the data storage and retrieval, he may guess about the distance of the data consumer [25]. Some solution approaches are discussed in [23].
- Name Privacy: The name field of the interest and data packet is a public field which is used to reach the data producer. Moreover it may give an indication of the data type and producer' s location. As for example a name field $/samsung/aus/mel/branch5/dec2019/customer_list$ suggests that the data is about the list of customers of a branch of Samsung in Melbourne. Some solution can be proposed based on the direction discussed in [26], [27].

2.5 Ring Signature

In this proposed solution we use the concept of ring signature [28] to ensure the data provider' s privacy. $1-out-of-n$ signature scheme convinces a verifier that a message is signed by one of the members of a group of size n, without knowing the exact signer.

$1-out-of-n$ signature scheme, let' s say $S^{1,n}$, consists of three following functions [28]:

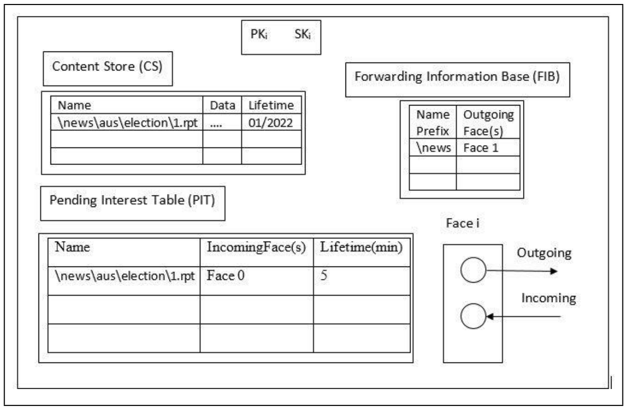
- Key generation: $tt^{1,n}(1^k)$ is a probabilistic algorithm that takes security parameter k and produce private key sk and public key pk. That is $(sk, pk) \leftarrow tt^{1,n}(1^k)$.
- Signature: $S^{1,n}_{sk}(m, L)$ takes message m and a list L of public keys and produce a ring signature δ. That is $\delta \leftarrow S^{1,n}_{sk}(m, L)$
- Verification: $V_L^{1,n}(m, \delta)$ takes message m and signature δ and produce the output 1 or 0. If the signature matches the output is 1, otherwise 0. That is $1/0 \leftarrow V_L^{1,n}(m, \delta)$

3 Proposed NDN based Privacy Preservation in PSN

In our proposed privacy preserved PSN let us assume there are maximum n number of participating nodes. They are randomly located within an area with any typical mobility model [29] and routing protocols [30]. For simplicity, we would not elaborate the issue of mobility or routing protocols in this solution. Next few subsections present our proposed solution in detail.

3.1 Components

- Node: There are n number of participants $N_1, N_2, ..., N_n$. Each one equipped with the necessary cryptographic keys, private key sk and public key pk as described in section 2.5. As these are also NDN nodes, the other data structures CS, PIT and FIB, as discussed in section 2.3, will be part of the nodes as depicted in figure 4. The list of interfaces, i.e. the list of neighboring nodes are also shown in the anatomy of the node.


PK_i SK_i
Content Store (CS)
Forwarding Information Base (FIB)
Pending Interest Table (PIT)
Face i
Outgoing
Incoming

Name	Data	Lifetime
\news\aus\election\1.rpt	....	01/2022

Name Prefix	Outgoing Face(s)
\news	Face 1

Name	IncomingFace(s)	Lifetime(min)
\news\aus\election\1.rpt	Face 0	5

Fig. 4. Anatomy of a participatory node

- Router: By definition, all participants in a PSN are eligible to work as a router.
- Interface (Face): Interface or in short Face is a list of neighboring nodes of a particular node. In figure 4 this particular node has one interface for incoming and another one for outgoing traffic.
- *Interest Packet*: Whenever any node would require to access any data, it will initiate an *Interest Packet*. The most important field of an *Interest packet* is the *Name* which is formed using a pre-stipulated mechanism detailed in [6].
- *Data Packet*: The provider creates a *Data Packet* that contains following important fields - Name, Metadata, Content and Signature, as shown in figure 5, which are computed by the provider as follows:

- *Name*: The *Name* field will be created as it is created in *Interest Packet*
- *Metadata*: This field contains the type, validity period etc. of the data.
- Content: Actual data in plain-text.
- Signature: The digital signature calculated using the ring signature mechanism discussed in section 2.5.

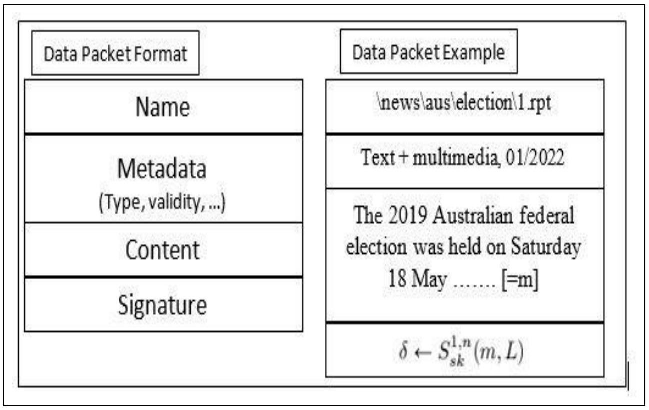

Data Packet Format
Name
Metadata
(Type, validity, ...)
Content
Signature
Data Packet Example
\news\aus\election\1.rpt
Text + multimedia, 01/2022
The 2019 Australian federal election was held on Saturday 18 May .... [=m]
$\delta \leftarrow S^{1,n}_{sk}(m, L)$

Fig. 5. Data packet structure and an example

3.2 Operations

In the proposed *PSN* there are n number of nodes $N_1, N_2, \dots N_n$. Each node N_i have public key pk_{Ni} and private key sk_{Ni} generated using the key generation algorithm. The list of public keys $L = \{pk_{N1}, pk_{N2}, \dots, pk_{Nn}\}$.

When any node has a chunk of data to share, it will create a data packet according to Algorithm 1 and enters the data in its *CS* table. When a node receives an *Interest Packet* from one of its incoming face, it runs the Algorithm 2. When a requester or an intermediate node receives a data packet, it takes action according to the Algorithm 3.

Algorithm 1 Create Data Packet

```
input : m, L
Begin
Name = CreateName()
Metadata = CreateMetadata()
$\delta \leftarrow S^{1,n}_{sk}(m, L$
DataPacket = FormDataPacket(Name, Metadata, m, $\delta$)
CS ← DataPacket
End
```

Algorithm 2 Response to *Interest Packet*

```
input : Face(), Interest Packet(IP )
output : Data Packet
Begin
if Name=IP.Name then
    return CS.Data
    discard IP
else
    /*Broadcast the interest packet to all faces*/
    add detail in PIT
    OF=getOutFace(FIB,IP.Name)
    CallRecursively(OF,IP)
end if
End
```

Algorithm 3 Reception of Data Packet

```
input : DataPacket(DP )
output : Face, Data Packet
Begin
CS.Data = DP
/*Gets the corresponding face from PIT table*/
OF = PIT.Face
/*Deletes the corresponding entry in PIT*/
Delete DP entry in PIT
return OF, DP
End
```

A participatory sensor node performs all the operations based on the input it may receive via any face and the state it is in. Let us name various states of a node N as follows:

- N_{CS} : N has the data in its cache if $N_{CS} = 1$. Otherwise $N_{CS} = 0$.
- $N_{P\,IT}$: If $N_{P\,IT} = 1$, N has an entry in PIT for the data asked. Otherwise $N_{P\,IT} = 0$
- N_{FIB}: If $N_{FIB} = 1$, N has an entry. Otherwise $N_{FIB} = 0$

Each node will move from state to state based on its current state and input it receives. The state diagram is shown in figure 6.

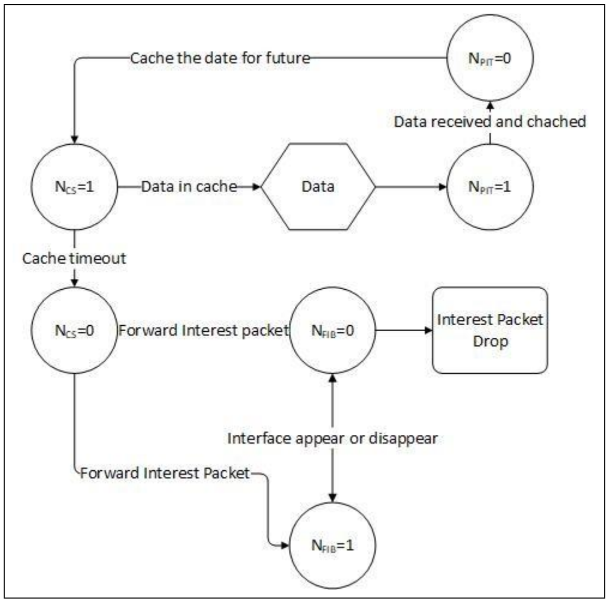


Fig. 6. State diagram of operations

4 Security Analysis

In this section we analyze the security of the, specifically the privacy of the participating node which shares some data. As the nature of NDN, the location of the node is unknown to anyone. The data of the $Data\ Packet$ is signed using ring signature to ensure the integrity without revealing the identity of the owner. Let us consider following scenario to analyze the security:

4.1 Data Consumer's Privacy

The data consumer node, let' s say node r initiates the *Interest Packet* which is then forwarded to the neighboring interface. The packet does not contain any information about the consumer' s identity. The neighboring interface has no means to guess whether the packet is initiated by node r or just forwarded by r as part of routing service. At the same time, when the *Data Packet* arrives back to r, the neighboring nodes will have no means to guess whether r receives the packet for itself or it will forward to other node. Hence, the receiver' s privacy is preserved.

4.2 Data Provider's Privacy

In the proposed solution, the data provider node, lets say d, is part of n number of participating nodes. By using the ring signature mechanism we ensure that no one within the network would be able to guess which node out of n nodes has provided the data. When d creates a data packet, it simply creates using the algorithm 1 and place the data in CS. Thus there would not be any difference if d is keeping its own data in CS or it received the data from neighboring interface.

5 Conclusion

Named Data Networking an instance of Information-Centric Network focuses on data as opposed to physical location of the involved parties. As security is a design consideration of NDN, it ensures some of the security issues, such as - data integrity, recipient privacy etc. Though the privacy of the data consumer is preserved, the data provider' s privacy is not ensured in NDN as the data consumer needs to use the public key of the provider for data integrity. In this paper, we proposed a ring key based digital signature based NDN to ensure data provider' s privacy in a Participatory Sensor Network. The proposed solution can be implemented in many PSN based applications which heavily depend on shared data.

References

1. M. Conti, S. Giordano, Mobile ad hoc networking: milestones, challenges, and new research directions, IEEE Communications Magazine 52 (1) (2014) 85 – 96.
2. M. Adimoolam, M. Sugumaran, R. S. Rajesh, The security challenges, issues and countermeasures in spatiotemporal data: A survey, in: J. Hemanth, X. Fernando, P. Lafata, Z. Baig (Eds.), International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018, Springer International Publishing, Cham, 2019, pp. 1216 – 1224.
3. D. E. Boubiche, M. Imran, A. Maqsood, M. Shoaib, Mobile crowd sensing – taxonomy, applications, challenges, and solutions, Computers in Human Behavior 101 (2019) 352 – 370.
4. R. N., S. Abraham, S. S. Das, A survey on trajectory privacy in participatory sensing applications, in: 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 2019, pp. 233 – 237.

5. M. Connolly, I. Dusparic, M. Bouroche, An identity privacy preserving incentivization scheme for participatory sensing, in: 2018 Eleventh International Conference on Mobile Computing and Ubiquitous Network (ICMU), 2018, pp. 1 – 6.
6. L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, B. Zhang, Named data networking, SIGCOMM Comput. Commun. Rev. 44 (3) (2014) 66 – 73. doi:10.1145/2656877.2656887.
   URL http://doi.acm.org/10.1145/2656877.2656887
7. T. H. Silva, P. O. S. Vaz de Melo, J. M. d. Almeida, A. A. F. Loureiro, Uncovering properties in participatory sensor networks, in: Proceedings of the 4th ACM International Workshop on Hot Topics in Planet-scale Measurement, HotPlanet ’ 12, ACM, 2012, pp. 33 – 38.
8. D. Tsolovos, Enforcing Privacy in Participatory Sensing Systems, in: Middleware Doctoral Symposium 2018, ACM, Rennes, France, 2018.
   URL https://hal.inria.fr/hal-01910067
9. S. Joshi, H. Saini, G. Rathee, Salt cryptography for privacy in mobile crowdsourcing, International Journal of Information Technology (Jan 2019).
10. K. L. Huang, S. S. Kanhere, W. Hu, Preserving privacy in participatory sensing systems, Computer Communications 33 (11) (2010) 1266 – 1280.
11. Y.-N. Liu, Y.-P. Wang, X.-F. Wang, Z. Xia, J.-F. Xu, Privacy-preserving raw data collection without a trusted authority for iot, Computer Networks 148 (2019) 340 – 348.
12. N. Bitansky, V. Vaikuntanathan, Indistinguishability obfuscation from functional encryption, J. ACM 65 (6) (2018) 39:1 – 39:37. doi:10.1145/3234511.
13. M. Amadeo, C. Campolo, A. Molinaro, G. Ruggeri, Iot data processing at the edge with named data networking, in: European Wireless 2018; 24th European Wireless Conference, 2018, pp. 1 – 6.
14. D. J. W. Andrew S. Tanenbaum, Computer Networkss, Fifth Edition, Pearson, 2012.
15. C. A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, P. Samarati, Location privacy protection through obfuscation-based techniques, in: S. Barker, G.-J. Ahn (Eds.), Data and Applications Security XXI, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007, pp. 47 – 60.
16. M. Yamac, M. Ahishali, N. Passalis, J. Raitoharju, B. Sankur, M. Gabbouj, Reversible pri- vacy preservation using multi-level encryption and compressive sensing, CoRR abs/1906.08713 (2019).
17. R. Paulet, M. G. Kaosar, X. Yi, E. Bertino, Privacy-preserving and content-protecting location based queries, IEEE Transactions on Knowledge and Data Engineering 26 (5) (2014) 1200 – 1210.
18. C.-Y. Chow, M. F. Mokbel, Trajectory privacy in location-based services and data publication, SIGKDD Explor. Newsl. 13 (1) (2011) 19 – 29.
19. S. Zhang, G. Wang, Q. Liu, J. H. Abawajy, A trajectory privacy-preserving scheme based on query exchange in mobile social networks, Soft Computing 22 (18) (2018) 6121 – 6133.
20. Y. Tian, X. Li, A. K. Sangaiah, E. Ngai, Z. Song, L. Zhang, W. Wang, Privacy-preserving scheme in social participatory sensing based on secure multi-party cooperation, Computer Communications 119 (2018) 167 – 178.
21. Y. Yu, Y. Li, X. Du, R. Chen, B. Yang, Content protection in named data networking: Challenges and potential solutions, IEEE Communications Magazine 56 (11) (2018) 82 – 87.
22. B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, B. Ohlman, A survey of information-centric networking, IEEE Communications Magazine 50 (7) (2012) 26 – 36.
23. A. Chaabane, E. De Cristofaro, M. A. Kaafar, E. Uzun, Privacy in content-oriented networking: Threats and countermeasures, SIGCOMM Comput. Commun. Rev. 43 (3) (2013) 25 – 33.
24. R. Bendrath, M. Mueller, The end of the net as we know it? deep packet inspection and internet governance, New Media & Society 13 (7) (2011) 1142 – 1160. doi:10.1177/1461444811398031.
25. E. Felten, M. Schneider, Timing attacks on web privacy (01 2001).

26. A. Broder, M. Mitzenmacher, A. B. I. M. Mitzenmacher, Network applications of bloom filters: A survey, in: Internet Mathematics, 2002, pp. 636 – 646.
27. W. You, B. Mathieu, P. Truong, J. Peltier, G. Simon, Realistic storage of pending requests in content-centric network routers, in: 2012 1st IEEE International Conference on Communications in China (ICCC), 2012, pp. 120 – 125.
28. M. Abe, M. Ohkubo, K. Suzuki, 1-out-of-n signatures from a variety of keys, in: Y. Zheng (Ed.), Advances in Cryptology — ASIACRYPT 2002, Springer Berlin Heidelberg, Berlin, Heidelberg, 2002, pp. 415 – 432.
29. R. A. Pushpa, A. Vallimayil, V. R. S. Dhulipala, Impact of mobility models on mobile sensor networks, in: 2011 3rd International Conference on Electronics Computer Technology, Vol. 4, 2011, pp. 102 – 106.
30. L. Junhai, Y. Danxia, X. Liu, F. Mingyu, A survey of multicast routing protocols for mobile ad-hoc networks, IEEE Communications Surveys Tutorials 11 (1) (2009) 78 – 91.