ISSN: 2249-7196
IJMRR/ Dec 2022/ Volume 12/Issue 4/-/13-34

Analytical survey of existing research on anonymous communication technologies and directions for further study

Mehran Alidoost Nia, A. Ruiz-Martínez

[a] *School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran*
[b] *Department of Information and Communications Engineering, Faculty of Computer Science, Campus of Espinardo, Murcia, 30100, SPAIN*

Abstract

Privacy is an important research topic due to its implications in society. Among the topics covered by privacy, we can highlight how to establish anonymous communications. Dur- ing the latest years we have seen an important research in this field. In order to knowwhat the state of the art in the research in anonymous communication systems (ACS) is, we have developed a systematic literature review (SLR). Namely, our SLR analyzes several issues: activity performed in the field, major research purposes, findings, what the most ACS study, the limitations of current research, how is leading the research in this field and the most highly-cited articles. Our SLR provides an analysis on 203 papers found in con- ferences and journals focused on anonymous communications systems between 2011 and 2016. Thus, our SLR provides an updated view on the status of the research in the field and the different future topics to be addressed.

Keywords: Anonymous communications Anonymous communication systems Privacy Anonymity Systematic literature review

Introduction

Progressively, citizens perform more activities on the Internet such as surfing on the Web, establishing Voice over IP communications, sending and receiving instant messages (e.g. through WhatsApp Messenger), which facilitates that different entities such as Internet Service Providers, websites, advertisers, and governments can obtain more information on their activities and can create users' profiles [1–6] or surveillance them.

At the same time, in order to prevent this gathering of information as well as personally identifiable information (PII) can obtained and managed without users' consent, both technical solutions and regulations (mainly in Europe) are being developed to protect our privacy and anonymity [7–12].

There are different technologies to protect privacy on the Internet, named Privacy Enhancing Technologies (PETs) [13], from these technologies, we can point out anonymous communication systems (ACS).

This kind of systems are fundamental to preserve freedom of speech and avoid censorship [2,14,15]. Indeed, they are the cornerstone to define and develop different kind of systems that need to preserve privacy and anonymity such as electronic voting system, anonymous payment systems, anonymous Voice Over IP (VoIP) communications based on SIP [16–18], and electronic auctions [5,11,19].

ACS aim is to protect communications between entities from traffic analysis by providing unidentifiability and unlinka- bility [20]. Depending on the system, sender identity, receiver identity or sender and receiver identity will be preserved. A formal definition of these concepts can be found in [14,21].

For this purpose, these ACS define different architectures, types of networks (wired, wireless or hybrid), algorithms to establish a path between the sender and the receiver (establishing the length of the path and selecting the nodes), and cryptographic techniques.

In a general way, ACS can be classified into high-latency systems and low-latency systems [14,22,23] depending on whether it is important or not the delay in the communication.

High-latency systems (e.g. Mixminion or Mixmaster) are suitable for non-interactive applications and often provide stronger anonymity than low-latency systems (e.g. Tor, I2P or Crowds), which aim to support real-time communications such as web browsing or instant messaging. In order to deanonymize them there are two general kinds of attacks [22]: application based attacks (try to obtain user's IP by means of applications that do not consider privacy) and network level attacks (trying exploiting ACS limitations or trade off made in its design).

Due to the importance of ACS, a significant research work is being made in the latest years on the existing ACS, its fea- tures, possible improvements, its attacks and possible countermeasures as well as the proposal of new systems considering different approaches or scenarios.

In this paper we aim to provide an analysis of the state of the art in ACS and open challenges. Namely, we have managed to focus on any

research work which its main goal is to provide an application for new trends of anonymous systems. Any researcher who wants to start a research work in this area should know about recent trends and current research directions in ACS.
To perform the review of the state of the art we have made a systematic literature review (SLR). This SLR responds to the growing body of knowledge in accordance with various categorization of studies such as new problems, novel applications, future issues, and security analysis of the current ACSs. To the best of our knowledge this is the first SLR that is developed in the field of anonymous communication systems.
We have tried our best to review recent studies in two main directions. The first direction is research works which their goal is related to new applications for ACSs. The second one is new applications or new versions of current applications that some security and performance issues have been solved. A lot of quality and quantity factors are included in this SLR. We have classified research papers by their types (either journal or conference paper), number of citations, number of references, year of publication, their main goal, researchers countries, type of ACS, and etc.
We have analysed the most cited papers, distribution of researchers by countries, current trends and studies, future directions, limitations of the proposals, and the source of publications.
This literature review attempts to sum up recent publications from popular academic databases like IEEE Xplore, Sco- pus, and ACM Digital Library. We discovered some useful information from these papers that is very applicable for young researchers or beginners in the research field who are going to work on the related subjects. This paper systematically re- views the papers and extract their strong features. Also, some research questions are answered during this work and hot topics are explored.
It must be taken it into account that the selection process of the papers is systematically organized by the predefined criteria and it does not depend on our personal view.
The rest of this paper is organized as follows. Section 2 is a background section that presents previous research made in anonymous communications systems and introduces SLR. Section 3 presents the different research questions that our SLR aims to answer. Next, in Section 4 we present how we have developed the SLR. Section 5 presents the results of the SLR we have conducted. Based on the results obtained, we made a discussion on Section 6. Finally, Section 7 presents the main conclusions of our work and introduces future work.

Background

This background section provides a literature review on previous surveys on ACS, present systematic literature reviews and point outs the main feature about this SLR.
To the best of our knowledge, this is the first SLR on anonymous communication systems. Although there are no previous SLR, in this section, we comment the main surveys on ACS that have been performed so far. We also present SLR and point out its main advantages in comparison to the other surveys.

1.1. Previous surveys on ACS

Recent surveys focusing on ACS are organized according to two popular approaches. The first approach is to select the main topic, collect all the related papers via undefined academic databases, summarize issues and trends, and compare original researches together. The output of such papers will be presented as tables/graphics with quality measurements. They may discuss on the issues and give some recommendations on how to continue the work for future researches. We have classified three review papers with this manner in the current SLR.
The first paper is concentrated on anonymity technology usages [24]. The authors have tried their best to present anonymity from usage metrics point of view. As the first level priority, they have not focused on ACS tools and features. However, they provide some basic details.
The second review paper is about comparing tools for privacy enhancement in web communications [2]. The author introduced different communication tools which their main goal is to enhance privacy of the users through the Internet. In this survey, the mentioned tools are categorized by the layers which they work through them. ACSs are part of this survey where an introduction to main technologies is presented. However, this survey does not present either current state-of-the- art in the research field or it would respond to many current trends in anonymous technology.
The third paper in our database is only focused on anonymity technology in mobile and ad-hoc systems [25].
Another useful survey is Danezis and Diaz's work [26] which is one of the frontiers dedicated to anonymous technology. The advantage of their work is a set of perfect technical details. But the main disadvantage of this work is that it does not reflect current state-of-the-art and recent advances in the field. It is a paper that any beginner should read in order to understand basic terms, requirements related to this technology and the main issues it aims to cover.
One of the other popular surveys which is somehow related to ACS is the work presented by Lin [27]. It has the same disadvantage as the previous for current trends in ACS, it is outdated.
Ren and Wu [19] presented other survey, which is about anonymous communications in computer networks. It is classi- fied in tutorial surveys which aim to learn basic knowledge required for entering to the related research topics.
The other type of surveys is research/review surveys. The authors try to indicate their findings of a research by surveying it. They would have basic comparisons and more precise analysis. But the scope of the survey will be limited to their research topic.
In this SLR, we have reviewed two of this type of surveys. The first survey is about challenges of anonymous communica- tions in United Kingdom [8]. The author investigates regularity challenges posed by ACSs in UK. As mentioned, the scope is limited to a specific country, but it gives some good results that may be applicable to other researches globally. The second work surveys attacks and defenses in ACSs through practical investigations and analysis [28]. It is a well-structured survey but its constraint would be the restricted challenges that they aim to investigate.

1.2. Systematic literature review

A systematic literature review (SLR) is a study that reviews studies that investigate a specific research question on an important issue with

the aim of providing a synthesized review of the issue or topic following a transparent, methodical, and reproducible procedure [29–32]. Thus, for the elaboration of this kind of study, it is followed a well-defined methodology that allows the identification, analysis, and interpretation of all available evidence related to a specific research issue, at the same time that is thorough, fair and repeatable [29].
Kitchenham and Charters [29] elaborated some guidelines to perform a SLR. They defined three phases for the review: planning, conducting and reporting. In the planning phase, the review protocol is established in base of the need for review and the research questions. Conducting the review supposes to select the primary studies and apply the criteria established in the review protocol to analyze them. Finally, in the reporting phase is the elaboration of the report. For the development of this SLR we have followed these guidelines.

1.3. About this systematic literature review

As stated in our current study, the main goal is to collect all the issues regarding anonymous communication systems.As we know, researchers in ACS area are interested in both the theoretical methodology and experimental evaluations. Our work is not limited to survey a specific issue and covers both. However, it mainly emphasizes on the experimental result. In contributing SLR, we investigate recent works by responding to a series of research questions. The questions are prepared in advance to give the entire work a systematic structure. We do not limit our work to either one or several databases, however, a set of targeted academic databases must be defined in adverse. We present the most updated original research works by performing a systematic search approach in all the mentioned databases.
The main advantage of our work is a micro classification of research works. Before any contribution, the gathered re- search papers will be classified according to the authors, years, citations, countries, type of research work, title of jour- nal/conferences, research questions, etc. It would help to provide systematic results with a high quality. For example, the most cited papers illustrates the most validated papers from researchers point of view. Future directions (as an answer to the one of the provided research questions) may help young researchers or beginners in ACS to find their way and define a proper research work or prevent an improper research direction. So, this SLR on ACS is more useful to analyze research backgrounds and gives definitely more structured details about current and future trends of ACS. Comparing to the classic surveys, this SLR would be best for young researchers especially those who want to start a new research work in ACS.

Research questions

In general, our aim with the SLR is to obtain knowledge on the status of the art in anonymous communication systems, limitations of current research and future work. Thus, in order to have this knowledge in our investigation we have defined the following Research Questions (RQ):

- RQ1: How much research activity on anonymous communication systems has there been in the last years (from 2011 to 2016)?
- RQ2: What are the major research purposes and findings in anonymous communication systems?
- RQ3: What are the main anonymous communication systems where research is being made?
- RQ4: What are the limitations of current research or main problems that still need to be addressed?
- RQ5: What are the future research lines to be investigated?
- RQ6. How is leading anonymous communication system research?
- RQ7. What are the highly-cited articles in anonymous communication systems?

2. Method

As research method to perform a review of the literature, we have decided to follow a systematic approach to review the literature in the field of anonymous communication systems. Thus, we have performed a Systematic Literature Review (SLR) based on the guides proposed by Kitchenham [29]. Unlike a review made by an expert reviewer by selecting ad hoc literature, an SLR is a review of research results made according to a rigorous methodology [30]. Next, we explain the steps we have followed and the considerations we have made to conduct the review and answer research questions.

2.1. Search process

Our search process was made initially on November 2015 and was based on query on the most relevant main bibli- ographic databases of papers published in journal and in conferences regarding the topic of anonymous communication systems. Later, in August 2017 we update it with information from 2015 and 2016.
The databases we have queried are: ACM Digital Library, Elsevier Science, Google Scholar, IEEE Xplore, ISI Web of knowl- edge, Scopus and Wiley InterScience.
For our search we have introduced the following terms: *Anonymous communication system*, *anonymous communication network*, *anonymity network*, *anonymous communications*, *anonymous protocol*.
The period of time that we have decided to cover for our research work is established between 2011 and 2016 (inclusive).
Thus, we will limit the different queries to this period.
Once we have obtained the results of the different queries to the different databases, we have applied the inclusion and exclusion criteria defined in Section 4.2 in order to select the relevant papers to perform the analysis.

Inclusion and exclusion criteria

Next we present the different criteria that we have established in order to select the papers that will be part of our analysis.

The inclusion criteria are:

- The paper must be published from 1 January 2011 to 31 December 2016.
- The paper must be published in a journal or conference proceeding.
- The focus must be on anonymous communication systems.
- The paper has to address some issue regarding anonymous communications systems.
- The paper has to be written in English.

The exclusion criteria are:

- Book chapters.
- Patents.
- Citations.
- Papers that do not address some issue regarding anonymous communication systems

2.2. *Data collection*

From each paper selected, we have extracted the following data:

- Bibliographic information of the paper: title, authors (and their countries), publication, and year of publication.
- Number of references included in the paper.
- Citations received.

Table 1
Results provided by the different bibliographic databases obtained in November 2015 and in August 2017.

Query date	November 2015	August 2017
Database	Results period 2011–2015	Results period 2016–2017
ACM Digital Library	143	63
Elsevier Science	31	67
Google Scholar	1970	961
ISI Web of Knowledge	56	51
IEEE Xplore	26	21
Scopus	395	184
Wiley	23	54

2.3. *Data analysis*

The data obtained was tabulated to show the following information:

- Authors.
- Countries.
- Type of publication: Journal/Conference.
- Journal/Conference Name.
- Number of cites.
- Number of references used.
- Type of paper: research or review.
- Main topic area.

To this end, we have executed a standard query string on different databases. It returns a number of results based on related keywords. When the results appear, the analytical process would be started.

According to the inclusion/exclusion criteria, a number of papers are added to the final list. So, aforementioned information is elicited from each result.

After all records are integrated in our database, statistical analysis begins. In this step, each paper is scrutinized precisely in accordance with the content of the paper and relevance level to the scope of the current study. This allows us to classify them by defining its main topic area, identify the different research purposes that the paper covers and the different future work is proposed. Finally, we made an analysis of main research purposes, issues and future work to group them in general categories that allows use a reduced number of categories.

3. Results

In this section we present the results obtained following the method proposed in Section 4.

Search results

The different queries made to the different bibliographic databases produced the results shown in Table 1.
It is important to point out that the results of some databases as Google Scholar, ISI Web of Knowledge and Scopus may contain part of the results that appear in databases such as ACM, IEEE, Elsevier or Wiley. However, this does not have influence in the

final result since the papers selected will be the same.
From the results we can see that Google Scholar provides an important number of results. However, many results are citations, patents or other kind of documents that did not satisfy the selection criteria and, therefore, they will be filtered (see next section).

Papers selected using inclusion and exclusion criteria

After applying the different inclusion and exclusion criteria and removing duplicated results obtained from different databases, we got 203 papers. We can see the results in the Appendix A.

4. Discussion

In this section, we discuss about our findings to answer the research questions.

Table 2
Number of publications by year.

Year	Number of publications
2016	41
2015	88
2014	21
2013	18
2012	17
2011	18

Table 3
Number of publication in which the different authors participate.

Number publications authors participate	Number of authors
1 publication	467
2 publications	61
3 publications	15
4 publications	3
5 publications	2
6 publications	0
7 publications	0
8 publications	0
9 publications	3
10 publications	1

6.1. *RQ1: How much research activity on anonymous communication systems has there been in the last years (from 2011 to 2016)?*

As mentioned the number of selected papers were 203. 112 papers were published as conference papers and 91 in journals. The distribution of papers selected in the different years can be seen in Table 2. In this table we can also see that the number of papers published in the different years range from 17 to 88.
Until 2015 we can see that there is a growing tendency in the number of publications. In 2016 we observe that there is an important decrement in the number of papers as for the previous year. From our point of view, this is a provisional result. Research databases take some time in being updated. Indeed, when we made our initial search process performed in November of 2015, from 2015, there only were 18 publications. When, we repeated this analysis in August 2017 we obtained
88. Therefore, with a high probability, if we repeat next year the analysis of 2016 we will obtain more publications. In any case, if we compare the publications selected from 2011 or 2012 and we compare with 2015 or 2016, we can state that it is reflected the increasing importance of the topic in the research field.
We have also analysed how many different authors have participated in the analysed papers. In Table 3 we can see that there are 552 different authors that have participated in the 203 analysed publications. These authors, in general, only have contributed with 1 or 2 publications.
In this analysis there is a set of authors that have contributed with more of 5 publications: Weijia Jia (Department of Computer Science and Engineering, Shangai Jiao Tong University, China) (5 publications), Wei Yu (Department of Computer and Information Sciences, Towson University, USA) (9 publications), Xinwen Fu (Department of Computer Science, University of Massachusetts, USA) (9 publications), Zhen Ling (School of Computer Science and Engineering of Southeast University, China) (9 publications) and Junzhou Luo (School of Computer Science and Engineering, Southeast University, China) (10 publications).

6.2. *RQ2: What are the major research purposes and findings in anonymous communication systems?*

The different selected papers show that there are different possibilities of research in ACS. In Table 4 we can find a listof the different purposes that have been investigated with the list of references.
These research purposes have arisen a set of findings that we mention next. In general, the findings are result of the different research purposes and have produced improvement in the research field they have worked. Therefore, the different issues in which we can classify the finding are similar to those shown in Table 4, but next we provide some details on the main findings

related to the research purposes. Next, in the following sections we present the main relevant data for each research purpose in Table 4.

Reviews of the state of the art

As we can see in Table 4 there are several publications that cover the analysis of the state of the art. This is analysed from several point of views, such as the tools available for anonymous Web communications [2], its situation in MANETs

Table 4
Research purposes.

Research purpose	Reference(s)
Reviews of the state of the art	[2,8,24,25,28,33–37]
Anonymity modeling and measurement	[38–77]
Attacks	[36,41,42,44,78–88,88–103]
Protection against attacks	[78,81,94,104–107]
Traffic analysis	[46,87,93,108,109]
Improving security and anonymity	[46,56,69,110–128]
Performance evaluation	[44,129,130]
Improvement performance/efficiency	[37,55,74,114,115,121,129,131–138]
Tor bridge discovery	[84,139]
Tor path selection algorithm	[121,140]
Cryptographic constructions for ACSs	[75,138,141–143]
Designing new ACS	[8,39,47,49,56,103,111,115,142–152,152,153,153–202]
Payment for ACS	[203]

[25,34], the technology usage [24], attacks and defenses [28], network topology [33,35], deanonymization of hidden services [36], performance and security [37] or regulation [8].

In particular, Ruiz-Martínez [2] presents a analysis of the different risks a user is exposed when he/she is surfing on the Web and a set the different solutions and tools that could be used to mitigate those risks.

In [25] we can find the main concepts related to anonymity, the main proposals for a wired and MANET environments and a taxonomy of anonymous routing protocols for MANETs according type of routing, delivery method and addressing scheme.

Li et al. [24] review the most used anonymity technologies, assess their usage levels, analyses the usage of Tor and the applications that use these tecnologies.

Lu et al. [33] and Kang [35] present a study of the main universities and research organizations that are researching inthe ACS regarding network topology and present a framework of anonymous network topology and a progression of the research work in network topology and node discovery in anonymous communication.

Nepal et al. [36] survey the main methods used to anonymize hidden services (Manipulating Tor cells, cell counting and padding cell) and perform a comparison as for the deanonymizing time, the true positive rate and the required number of compromised entry nodes.

Alsabah and Goldberg [37] survey research advances in the performance and security of low-latency anonymous commu- nication systems, particularly focused on Tor network. They also present some issues to be addressed regarding the threat of Tor-based botnets, blocking resistance, hidden services, time analysis problem and performance.

Horsman [8] analyzes regulatory challenges that present the use of anonymous communications in the United Kingdom and for this purpose they try to show their limitations when an offender's identity want to be determined, they present an scenario based on Yik Yak communications made using an iPhone.

Anonymity modeling and measurement

The study of anonymity through its analysis, the definition of models, taxonomies and measures have been addressed in a number of papers (see Table 4, research purpose: Anonymity modeling and measurement).

Next we mention some proposals related to modeling of several issues of ACS.A taxonomy of anonymous routing protocols for MANETs is presented in [25].

D'Arco and De Santis [59] define a formal model for secret sets and broadcast encryption facilitating the evaluation of privacy-enhancing technologies proposals.

In [45] QoS and anonymity have been modeled.

Vakde et al. [39] defined a model for Delay Tolerant Networks (DTN).

Fuchs et al. [66] propose two complementary models: one for extracting workloads from real scenarios and the second one for replaying workloads in simulations.

In [44] the authors point out that the composition of multiple anonymity channels can weaken overall security.

Backes et al. [61] define a formal technique for analyzing Tor against malicious or overly curious network infrastructure. Next we present different measures that have been defined.

Mahmoud et al. [156] defined two novel measures of information leakage and information.

In [54] is measured the impact of mobility on low-latency anonymity networks, in [55] opportunistic bandwidth, and in [57] end-to-end selection node probability.

Trust in presence of adaptive attackers has been considered in [56].

The study of the use of dummy messages is made in [46], also regarding dummy messages, Berman et al. [62] point out that is not necessary to send dummy messages and a high overhead when only a few nodes (n) (being $n << N$, where N represent all nodes) want to send messages assuming an adversary model where the adversary only controls a fraction of the links in the network.

Shirazi et al. [51] indicate how to measure resilience, Kang et al. [5] calculate the compromise rate for high bandwidth malicious nodes to know the effect of malicious nodes on Tor security, and in [48] they define how to gather client statistics from anonymity network egress nodes.
A new technique that is used to measure latencies between arbitrary Tor nodes from a single vantage point that can be used to improve anonymity and performance is presented in [64].
Zhioua [58] define several information leak measures for measuring the degree of anonymity in mix networks and their variants. In [47], a novel lightweight privacy metric is proposed.
PrivCount [67] is proposed as a system to Tor measurement.In [71] Tor code is analysed to understand it better.
NavigaTor [72] is used to perform the first large-scale measurements on the live Tor network. In [73] they define how to identify traffic to detect malicious traffic.
Finally, we can also mention the analysis of anonymity in particular scenarios such as hidden services [103], anonymous blackmailing systems [40], WSN [53], anonymous microblogging [70] or anonymous social networks [68].

Attacks
There are different findings covering attacks, how to detect them and how to establish countermeasures.
The different kind of attacks has been found are: Cell-Counting-Based Attack [83], packect size based attacks [79,81,86], attacks based on virtual network coordinate systems [41], Side-Channel Attack [101], de-anonymize attack based on traffic analysis attacks [85], redirection and replay attacks [80], Least Squares Disclosure Attack [82], Stealthy Attack [95], appli- cation classification attack [94], inferring application type information [90], flow fingerprinting [102] and traceback attack [96]. In most of the works, the authors describe possible countermeasures to the attacks identified.
We can also find some works that addresses attacks to exit relays [91], deanonymizing Tor Hidden Services in [36,89,97], and deanonymization in THEMIS [100].
Mittal and Borisov [42] present attacks on the lookup mechanism of structured peer-to-peer (P2P) anonymous commu- nication systems. They state that with the combination of both passive and active attacks, anonymity can be compromised much more effectively.
Danezis and Ksper [44] analyses the composition of multiple anonymous channels and point out that its composition can weaken overall security.
Ling et al. [88] present protocol-level attacks and DoS attack in Tor and confirm that by means of the manipulation ofone single cell, anonymous communication relationships can be confirmed quickly and accurately.
Park et al. [98] present an attack by increasing the Tor data transmission rate through the manipulation of the speed of the anonymous network.
Wang et al. [108] present different mechanisms to perform traffic analysis in MANETs.
The following works: [93,118,122] present different ways to detect eavesdropping, malware and connection detection based on Tor.

Protection against attacks
Some papers are mainly devoted to cover how to establish countermeasures [38,81,122].
He et al. [94] propose 3 different approaches to be protected: traffic padding, traffic morphing and traffic hiding. Hoang et al. [106] propose to extend Tor to offer protection against routing attacks.
In [107] a proposal for mitigating attacks in WSN is proposed.

Traffic analysis
There are different solutions to prevent traffic analysis [46,87,109] or for traffic identification [73,76].

Improving security and anonymity
As there are ACS based on mixes, that is a well-known solution for high latency communications, Mahmoud et al.
[156] and Rebollo-Monedero et al. [115] have studied different optimization strategies for mixing.
Zhang et al. [38] have defined strategies for trust and reputation in P2P systems to enhance P2P communications. In this paper, the authors also show that in some cases, an increase in the system scale does not mean that anonymity is enhanced. Furthermore, the use of too long anonymous tunnels not always suppose an increase in the anonymity but it would decrease the performance of ACS.
Hopper [123] proposes several changes to the Tor protocol for protecting from a botnet that uses hidden services as its primary Command and Control channel, and they propose four technical approaches: resource-based throttling, guard node throttling, reuse of failed partial circuits, and hidden service circuit isolation.
Haraty and Zantout [124] dealt with how to assure data integrity at the same time that it avoids traffic analysis. For this purpose, they propose a collaborative based approach which allows the client to validate the authenticity of the received data.
In [125] the authors explain how to protect smart home appliances by means of TOR.
In [126] an anonymous top-level domain (TLD) and resolution service for the Internet is proposed to ensure a high- performance architecture that is resistant to domain takedowns.

Feng and Matsuura [127] present a stronger bridge mechanism for Tor and Hamadou et al. [56] extend Crowds to offer protection against adaptive attackers.
Palmieri [69] proposes changes to the structure of Tor with the goal of improving its resilience in difficult or hostile settings, such as during crises and conflicts.
Barton and Wright [128] propose DeNASA (Destination-Naive AS-Awareness in Anonymous Communications), which reduces Tor stream vulnerability.

Performance
Emura et al. [138] propose the use of KEM/DEM-based constructions for improving efficiency of a prior solution. For improving performance, Sangeetha and Ravikumar [55] propose a traffic dividing and scheduling mechanism.
Another solution so that Tor hidden services can be used for botnet C&C without resulting in network congestion and reduced performance is proposed in [134]. For improving TCP performance, Watfa et al. [136] propose a hybrid approach based on monitoring real packet loss.
For supporting bulk data transfers without degrading the performance of interactive traffic, a multi-path Tor (mTor) routing algorithm has been proposed [137]. Also, in Annessi and Schmiedecker [72], the authors propose how to find faster paths.
A performance evaluation in delay-Tolerant wireless friend-To-friend networks has been studied in [130]. Latencies has been studied in [64] and workload in [66].
Bushnag et al. [74] present some source location privacy techniques for improving the performance of WSN at the same time that a high level of anonymity is provided in situations where a local adversary is capable of monitoring the entire traffic in the network.

Cryptographic constructions for ACS
For building and improving security, privacy or performance several cryptographic constructions has been defined. Emura et al. [138] state that for creating a secure and anonymous communication protocol, it is not required Identity-based Encryption (IBE), and propose a protocol that achieve the same security level based on the KEM/DEM framework [204].
Yajam et al. [141] develop a generalization of the definition of universal cryptosystems and the notion of universal semantic security to ID-based cryptography. Then, the authors propose two ID-based universal cryptosystem schemes.
Gomaa et al. [75] explain the use of Identity-Based Encryption (IBE) and Pseudonym-Based Encryption (PBE) to implement Virtual Identities (in virtual environments as Cloud).
Wu et al. [142] present optical encryption and key generation techniques.
Finally, in Ghosh and Kate [143], the authors show the utility of lattice-based cryptography so that one-way authenticated key exchange protocol can resist against quantum attacks.

Designing new ACS
There are a number of papers whose aim is to define new ACS for improving previous work in the field, or new ACS, or the application of them to cover new specific scenarios.
Gañán et al. [144] and Caballero-Gil et al. [189] define solutions for vehicular networks.
Schwarte et al. [145] propose a solution for social networking. There is also a solution for bulletin board application in [8].
Le Blond et al. [146] and Sabra and Artail [197] define solutions and systems for preserving anonymity in VoIP systems. New solutions for MANETs (Mobile Ad Hoc Networks) are defined in a number of papers:
[133,150,152,154,160,164,165,175,205,206]. A solution in Hybrid Ad Hoc Wireless Networks is proposed in Mahmoud et al. [156].
As for mobile opportunistic networks we can find the solution proposed by Radenkovic and Vaghi [111].
For Wireless Sensor Networks (WSN) there are also several proposals from Abuzneid et al. [150], Chen et al. [207], and Gagneja [176].
Zou et al. [208] and Lin et al. [202] propose systems for secure group communication, Shi et al. [153] and Antunez-Veas and Navarro-Arribas [169] propose some solutions for Delay Tolerant Networks (DTN).
Pereñíguez García et al. [148] define how to protect anonymity in Kerberos and it supposes an improvement of previous privacy solutions for Kerberos such as PrivaKERB [209].
Arnedo-Moreno et al. [149], Arnedo-Moreno et al. [210], Lv et al. [158], Lu et al. [200], Hermoni et al. [174], and Tan et al. [180] cover how to offer anonymous P2P services and file-sharing.
As censhorship resistant systems we can find several proposals [120,181,191].
Considering Mix-based solutions, we can mention a solution based on Multi-Binomial mixes [157] or in a verifiable identity-based mix network in [182].
For providing anonymity in a hot topic as Internet of Thing (IoT) we can find some proposals [163,198].
Another hot topic as Software-Defined Networking (SDN) is considered in [193] where they propose a solution for this kind of environment.

Table 5
Issues and references.

Issue	Reference(s)
Anonymity and/or security analysis	[2,24,28,35,38,51,57,60,61,63,67,77,89,93,97,109,122,135,206]
Analysis Tor Code	[71]
Resilience analysis	[51]
Latency and/or performance	[55,64,72,76,114,121,131,132,134,137]
Congestion	[134,212]
Path selection algorithm	[35,81,131,132,137,140]
Bridge discovery	[84,127,139]
Hidden services	[36,77,89,97,123,126]
Attack detection mechanisms and different kind of attacks (de-anonymization, sybil, cell-attack, application classification attack, etc)	[36,69,81,83,85,88–91,94,95,98,101,102,104,106]
Improving anonymity	[28,37,78,81,97,116,124,131,132,145,183]
Improving security	[37,42,55,69,93,106,114,118,121–124,126,127]
Use of Tor in applications	[40,125,134,148,174,213]

In Baek et al. [170], 198] there are solutions for protecting anonymity in e-healtcare systems when user is being moni-tored.
Anonymity in publish-subscribe systems has also considered in [161].
Group communication in device to device communication in LTE-A has been considered in [166].
Multiparty shuffling is considered in [177] and the use of random walk has been considered in [162].The design of a solution for mutual anonymous communications is presented in [178].
Efficient message submission is covered in [201].
The anonymity of delay-sensitive services has been considered in [179].
Solutions for commercial transactions has been proposed in [184,187], for roaming in [185], and for long distance geocast services [188].
For content-based infrastructures we can mention solutions for content-sharing and content-centric networking in[190,199], Peer-assisted Content Delivery Networks (CDNs) in [103], and anonymous data transmission system for cluster organised Space Information Network in [192].
In [117] the authors propose a quantum multiparty solution and in [194] a self-tallying quantum anonymous voting.
Finally, some proposals are extensions of well-know systems. Hence, we can mention Hamadou et al. [56]'s proposal to extend Crowds considering trust. Safaka et al. [183] propose a solution that can obtain a similar level of anonymity to Tor within a group of nearly half the network size.
Related to new onion routing-based ACSs, we can consider a proposal that defines onion routing at network layer in [168] or a proposal for improvement one-way authenticated key exchange protocol based on Diffie-Hellman (DH) and lattice Ghosh and Kate [143]. Anonymity in optical transmission has also been considered in [142].
As for the proposals related to new ACSs for MANETs, we can point that they are covering different issues related to vehicular network such as anonymous communications based on a combination of geographical location-based routing and greeder perimeter stateless routing [164], anonymous multicasting [165,206], multipath [160], providing both message sender and recipient privacy protection[133], and location-based routing [147,175].
Bultel et al. [186] propose SPADE, the fist distance-bounding protocol that provides anonymity, revocability and provable resistance to standard threat models.

Other findings
Another interesting findings that we can mention are: Ling et al. [84] and Ling et al. [139] have proposed mechanismsfor bridge discovery, Tian et al. [211] presented a new loop handling schema, Singh et al. [155] present a solution that, in post-quantum cryptography, can replace universal re-encryption scheme, and, a Garbled framework [119] that allows the unification of different ACS. Finally, Palmieri and Pouwelse [203] have designed a payment system to renumerate nodes in Tor network.
In Fig. 1 we depict a timeline with the most relevant papers analysed in this SLR.

RQ3: What are the main anonymous communication systems where research is being made?

Currently, Tor is clearly the main anonymous communication system where research is being made. From the differ- ent papers analysed, 70 papers are devoted to the study of Tor. Namely, the research in Tor is focused in these differentissues: in path selection algorithm, improving anonymity, attack detection mechanisms and different kind of attacks (de- anonymization, sybil, cell-attack, etc), latency and/or performance, anonymity analysis, use of Tor in applications, Tor bridge discovery, improving security, resilience analysis and hidden services. In Table 5 you can find the list of references associated to the issues we have just mentioned.

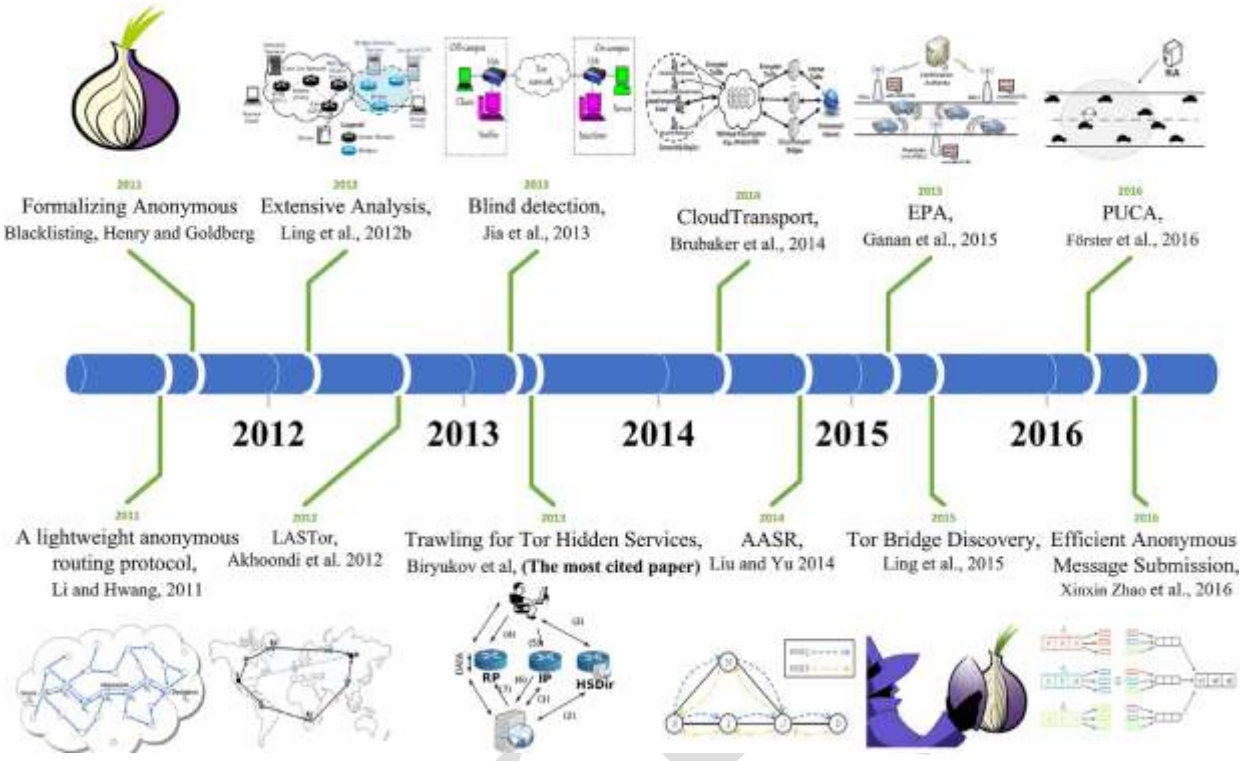

Fig. 1. Timeline - ACS development through the recent years.

Table 6
Types of limitations of the proposals.

Index	Classification of limitations	Number of publications
1	Evaluation Methods	9
2	Dataset and small number of samples	4
3	Security and reliability concerns	23
4	Performance issues	15
5	Design and architectural constraints	17
6	The result is based on either simulations or theory	33

After Tor, Crowds is the following anonymous communication system more studied with 10 publications. The main re- search regarding this ACS is related to: anonymity analysis [38,44,50,58,99,134], designing anonymous protocols for vehicular communications [144], anonymous communication in a lossy network [45] or in MANETs [34] and including trust [56].
Mixes and Mixnet are the following anonymous communication system more studied with 9 publications. The issues covered for this ACS are: improving security and anonymity [46,110,113,114,155], performance [114,115,129], traffic analysis [108] and evaluation of anonymity [46,50].
AP3, ANODR, and Salsa has been considered in 4 paper each of them. I2P has received attention in 2 papers related to its use as an anonymous communication system [2,24]. Freenet has also been considered in 2 papers [105,211]. Also, THEMIS, ALERT, Cashmere, RAPS and Torsk among other. Anonymizer has also been covered in 2 papers covering attacks [79,86].
Other known systems are only covered in 1 paper: Morphix [38], Tarzan [38], AN.ON [80], and Hordes [44]. Finally, the rest of papers propose new anonymous communication systems.

RQ4: What are the limitations of current research or main problems that still need to be addressed?

In this section, we provide a realistic view on the current research limitations of anonymous communication systems.
We have classified the limitations of proposals into six categories, which are shown in Table 6. Some of them are related to evaluation methods. For example, in [214] and [68], they have presented measuring anonymity loss as a limitation for the proposed system. This type of limitation is observed in papers that contain high level complexity and strong theoret- ical background. In this case, the researchers could not find a proper evaluation method to represent the strength of the proposed method.

Table 7
Classification of future directions.

Index	Classification of suggested plans	Number of publications
1	New applications for ACS	7
2	Implementation in new network environments	9
3	New protocols for ACS	5
4	ACS security enhancement	26
5	ACS performance improvement	35
6	Security analysis	21
7	Implementation in the real environments	11
8	Location privacy	6
9	Comparing to the other ACS	3
10	Designing new ACS	7

In [195] and [75], limitations are beyond that the results are based on theory and have not been tested in real environ- ments. It refers to part of papers that could not deal with real applications and it may have some negative effect on the validity of the proposed method.
According to our investigations, security and reliability are considered as a common limitation among researches con- ducted on anonymous communication systems as mentioned in [202] and [91]. The researchers who are working on anony- mous communication systems, try to improve security features. But at the same time, they should cope with several security issues. When they improve a security feature, it could undermine the other one. So, this is a trade-off for researchers to fo- cus on which security issue in the same situations.
Our findings reveal that the most important limitation is lack of implementation in real environments. Various reasons may cause the same limitation including complexity of the proposed architecture [187], no access to real traffic data [162], existing simulator environments [179], theoretical aspects of implementations [182], and the process of formalization [215]. Design constraints [184], and performance issues [48] are some examples of other limitations in ACS research lines.
Design limitations in ACS applications is a real issue. For example, Tor uses many volunteer middle servers to build its own topology of the mixed network. But, for a research work with limited resources, it is very hard to think of this huge design framework.
Table 6 shows a categorization of the aforementioned limitations in various research studies. Unfortunately, the limita- tions have not been directly addressed in the most of the research papers. This is considered one of the serious weak points of researches conducted in this area of science.

6.3. *RQ5: What are the future research lines to be investigated?*

Our investigation shows that the popular part of future researches will be dedicated to new applications of anonymous communication systems, especially the ones related to new strategies for computer networks like [211] and [75]. The rea- son of this trend is behind the popularity of anonymous applications and recent global concerns about privacy protection through the Internet. Unfortunately, in a considerable amount of the most cited papers, researchers have not specified a pre- cise future direction for their conducted research studies as in [216] and [91]. But we elaborated some useful information by investigating through the papers and extract their possible future work.
Study for anonymous routing protocols is one of the most frequent future directions. It includes creation of protocols for MANET networks [25], sensor networks [53], VANET networks [208], and P2P network infrastructure [38]. Routing protocols are important because of providing privacy of the senders/receivers. When an application uses anonymous routing protocol, it means that it tries to protect privacy of users against network devices.
A large portion of future work is dedicated to performance and security improvements for prior anonymous systems. It consists of proposing new defense strategies against common attacks [86], protocol level attack [88], security methods against external adversaries [112], detection of smart attacks [87] and [98], trust mechanisms [80], performance/security enhancement [217], safety measuring [67]. As we know, many ACS applications contain security bugs and suffer from seri- ous performance issues. These are the most important motivations for researchers to dedicate their future work to improve currently proposed ACSs.
Other suggestions come up with applying prior systems to the new environments [47,89], design of new anonymous communication systems [48], implementing some proposed systems in the real environments [75,189], performance anal- ysis of the proposed systems [140], improving location privacy [218,219], and comparing the work to the similar systems [149,194].
We have classified our findings about future directions in the form of Table 7. It illustrates that security enhancement and performance improvement are two of the most significant concerns in next generations of anonymous communication systems. It is comprehensible that security improvement is one of the main goal of each anonymous communication system. But it is interesting that most of research lines are suggested to conduct for new performance solutions and techniques.

Table 8
Number of researchers who are working on ACS.

Index	Country	Number of researchers
1	United States of America	117
2	China	113
3	India	45
4	Spain	42
5	Germany	42
6	Japan	27
7	United Kingdom	23
8	South Korea	15
9	Canada	11
10	Austria	11
11	France	11
12	Iran	8
13	Luxembourg	8
14	Brazil	7
15	Pakistan	7
16	Switzerland	7
17	Israel	6
18	Australia	4
19	Singapore	4
20	Czech Republic	4
21	Greece	4
22	Italy	4
23	Lebanon	4
24	Belgium	3
25	Tunisia	3
26	Poland	3
27	Taiwan	3
28	Thailand	3
29	United Arab Emirates	3
30	Morocco	2
31	Russia	2
32	Netherlands	1
33	Egypt	1
34	Norway	1
35	Qatar	1
36	Saudi Arabia	1
37	Sweden	1

In the next generation of ACSs, quality of service is a fundamental rule. Along with anonymity improvement in ACS protocols, designers are searching for solutions in order to improve quality of service and consequently, acquire users satisfaction. It is crucial for designers to make their product more popular.

On the other hand, we face a new future direction for security analysis of current ACSs. It is significant to cope with security bugs, and it requires a life-cycle for update and delivery of ACS products. So, it is expected to focus on business ACSs in the near future.

6.4. *RQ6: How is leading anonymous communication system research?*

Our investigations indicate that in the recent years, the number of researchers who involve in projects related to anony- mous communication systems are gradually growing. It is due to the ongoing trends and hot topics appeared in anonymous communication systems research directions. The need for anonymity and privacy motivates researchers in all over the world to start working on existing open problems.

A large portion of these studies belongs to the researchers from the United States. As shown in Table 8, the United States of America (USA) has more researchers who are working in the area of anonymous communication systems and its applications. After that, we can see China, India, and Spain that are following the USA. According to our findings, Chinese researchers are surpassing others in this research scope since 2016. This scope of science and its applications are also dom- inated by European countries (165 researches are from European Union countries) which is considered as one the main origins of trends about anonymous systems.

The statistics elicited from our investigations shows that the USA, European Union (EU) countries, and China have the most researchers studying anonymous communication systems.

The above gives a view based on quantity of conducted researches in anonymous communication systems.

From quality points of view, the most cited paper receives to Luxembourg's researchers [89], Chinese professionals [205], and the American specialists [131,132] since 2010.

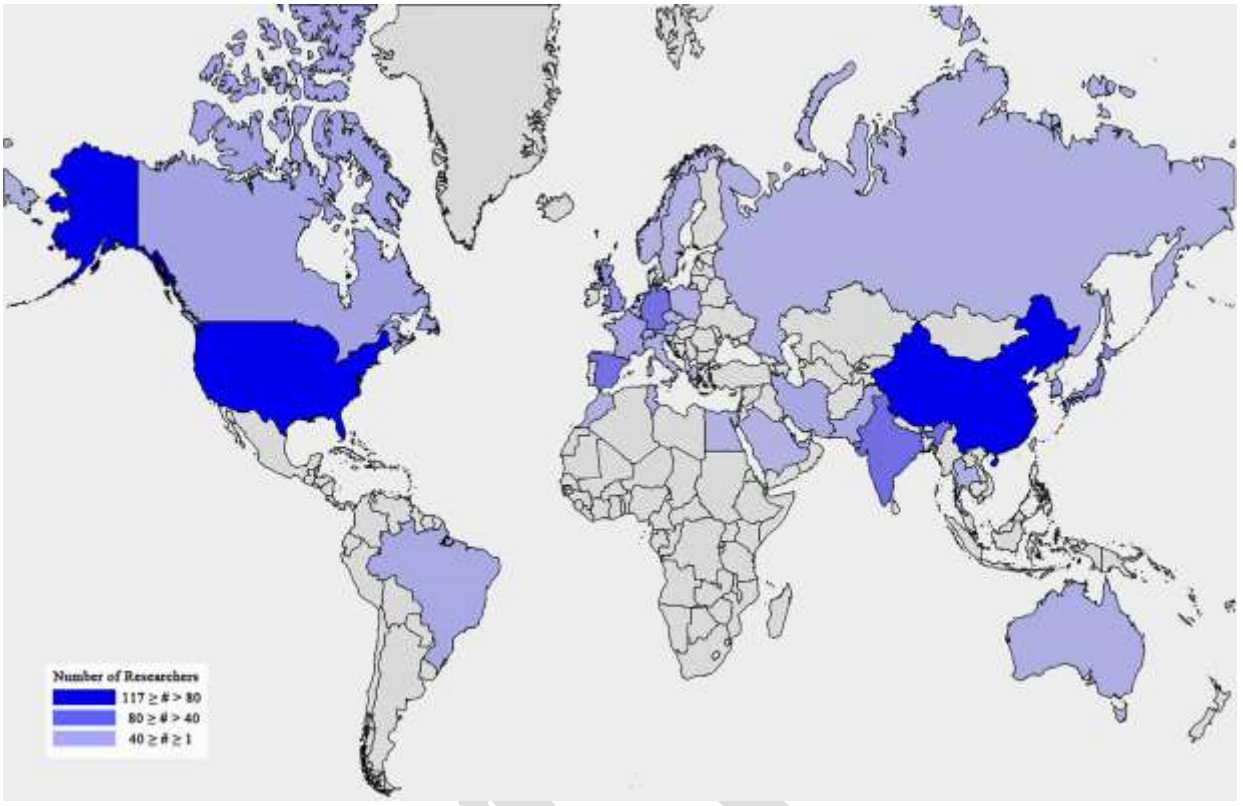

Fig. 2. SLR map - A graphical representation of ACS research work conducted in all over the world.

We have also classified the papers according to the number of their citations. By looking at the top ten papers, it is obvious that they have mainly published by researchers from the United States, China, and European countries.
New trends since 2016 shows that countries like India and Iran are developing new applications of anonymous commu- nication systems and it is predictable that they would start more research work related to the subject in the near future. Among European countries, Spanish researchers are still leading.
The most cited paper of 2015 belongs to a joint work between Chinese and American researchers which is dedicatedto Tor bridge discovery and it is published by IEEE Transactions on Parallel and Distributed Systems [139]. The mentioned research studies include the both practical and theoretical aspects of anonymous communication systems. Also, the most cited paper of 2016 belongs to American researchers who worked on performance improvement in anonymous message submission [201] which is published by IEEE Transactions on Dependable and Secure Computing.
The result of SLR shows that most of the researchers are interested in publishing their paper in professional journals and the minority of the papers belong to the conferences especially since 2015.
In the European countries, Spain, Germany, the UK, Austria, France, Luxembourg, Czech Republic, Switzerland, Greece, Italy, Belgium, Netherlands, Poland, Sweden, and Norway have conducted many research work in the same area of science.
Other countries include Japan, South Korea, Canada, Brazil, Lebanon, Australia, Russia, Tunisia, Qatar, Taiwan, Thailand, the UAE, Saudi Arabia, and Morocco have also become parts of research trend in anonymous communication systems. For more details, you can see Table 8. In Fig. 2 we present a graphical view to shows the distribution of researchers by countries who are working on ACS.

RQ7: What are the highly-cited articles in anonymous communication systems?

From the list of papers, the most cited paper is related to Tor Hidden Services [89] with 48 references. Next, with 38 references we found a paper about anonymous routing protocol for wireless ad hoc networks [205]. Then, in the third position we can find a paper proposing a low-latency AS-Aware Tor client [131,132].
The papers analysed are receiving, in average, almost 6 citations. From the 85 papers, 56 have received, at least, 1 citation. As for the number of references used, the work that have referenced more papers is a survey on solutions and main free tools for privacy enhancing Web communications [2] with 167 references. Then, with 81 references, we can find a paperthat deals with attacks and defenses of Anonymous Communication Systems [28]. Finally, in third place, a paper about optimizing the design parameters of threshold pool mixes for anonymity and delay [115] uses 78 references. In average,

the different works analysed are using 33 references. The paper with least references is a conference paper about sampling traffic analysis of anonymous communications in mobile ad hoc networks, with 5 references.

Limitations of this study

This SLR has a number of limitations. The results of this SLR are limited by the search terms used, publications chosen and time of period selected for the SLR, as in any other SLRs.
This study has been developed from the different queries we made on August, 2017. Probably, for the different biblio-graphic databases it takes some time to update the information. Thus, it would be recommended to repeat this study 18 months later so that the information on 2016 is consolidated. Even though, our study reflects the research situation in ACS between 2011 and 2016, and this information is significant to know the state of the art and future trends.
Next time, this study could be also developed for a higher number of authors so that the period between the information is gathered, analyzed, and written as a manuscript and sent to journal is shorter.
In spite of these limitations, the different papers analyzed in this SLR provide a comprehensive snapshot of research on ACS, which is representative of the state of the art at this time.

Conclusions

Nowadays we live in a digital era where using communications systems we chat, exchange information, access social networks, entertain, etc. These communications can be traced and/or eavesdropped in order to obtain valuable information on users such as personally identifiable information, communications habits, etc., which allows the creation of users' profiles. In order to preserve our privacy, anonymous communications systems has been proposed.

In ACS an important research activity has been developed in the latest years. In order to know the state of the art in this field we performed this SLR, which covers a recent period of time and that allow any research interested in this field to know the state of the art. We can also point out that to the best of our knowledge this is the first SLR that is developed in the field of anonymous communication systems.

This SLR is the result of the analysis of 203 papers. From this analysis, in response to our research questions, we have obtained several findings: first, there is an important activity in ACS. Second, within this field there is an important number of issues to be addressed in different scenarios. Third, as expected, Tor is the main ACS where research is being made. Four, there are still different issues to be addressed that we have classified them into six categories. Fifth, this issues have derived different future research lines, being security enhancement and performance improvement the most significant concerns Sixth, the countries that are leading research in ACS are USA, China, India, and Spain. Finally, as for citations, the paper most cited is related to Tor hidden services.

As future work, we could repeat again the SLR in order to check whether the different research databases have updated all the information regarding to the period of this SLR.

Acknowledgments

This work has been partially funded with support EDISON with code TIN2014-52099-R (from the Spanish Ministry of Economy and Competitiveness) and the European Commission (FEDER / ERDF) DHARMA – Dynamic Heterogenous threAts Risk Management and Assessment with code TIN2014-59023-C2-1-R from the SDHARMA – Dynamic Heterogenous threAts Risk Management and Assessment with code TIN2014-59023-C2-1-R and the European Commission (FEDER / ERDF), and CHISTERA PCIN-2016-010.

Appendix A

Next we present a table including three parts (Tables A.9, A.10, and A.11) with the list of the papers that have been analysed in this study.

References

Wills CE, Tatar C. Understanding what they do with what they know. In: WPES 12. ACM; 2012. p. 13–18. ISBN 978-1-4503-1663-7.
Ruiz-Martínez A. A survey on solutions and main free tools for privacy enhancing web communications. J Netw Comput Appl 2012;35(5):1473–92.
Such JM, Garcia-Fornes A, Botti V. Automated buyer profiling control based on human privacy attitudes. Electron Commer Res Appl 2013;12(6):386–96.
Kambourakis G. Anonymity and closely related terms in the cyberspace: an analysis by example. J Inf Secur Appl 2014;19(1):2–17.
Kang R, Dabbish L, Sutton K. Strangers on your phone: why people use anonymous communication applications. In: CSCW '16. ACM; 2016. p. 359–70. ISBN 978-1-4503-3592-8 doi: 10.1145/2818048.2820081.
Khazaei T, Xiao L, Mercer R, Khan A. Privacy behaviour and profile configuration in Twitter. In: WWW 16 Companion. International World Wide Web Conferences Steering Committee; 2016. p. 575–80. ISBN 978-1-4503-4144-8 doi: 10.1145/2872518.2890088.
Acar G, Juarez M, Nikiforakis N, Diaz C, Grses S, Piessens F, et al. FPDetective: dusting the web for fingerprinters. In: CCS 13. ACM; 2013. p. 1129–40. ISBN 978-1-4503-2477-9.
Horsman G. The challenges surrounding the regulation of anonymous communication provision in the united kingdom. Comput Secur 2016;56:151–62.
Kerber W. Digital markets, data, and privacy: competition law, consumer law, and data protection; 2016. ID 2770479.
Xu K, Yan Z. Privacy protection in mobile recommender systems: a survey. In: Lecture Notes in Computer Science. Springer International Publishing; 2016. p. 305–18. ISBN 978-3-319-49147-9.
Gibson JP, Krimmer R, Teague V, Pomares J. A review of e-voting: the past, present and future. Ann Telecommun 2016;71(7–8):279–86. doi:10.1007/ s12243-016- 0525-8.
Ganesh MI, Deutch J, Schulte J. Privacy, anonymity, visibility: dilemmas in tech use by marginalised communities; 2016. 00000.
Goldberg I., Wagner D., Brewer E. Privacy-enhancing technologies for the Internet. 1997, p. 103–109. doi:10.1109/CMPCON.1997.584680.
Yener B, Edman M. On anonymity in an electronic society: a survey of anonymous communication systems. ACM Comput Surv 2009;42(1):1–35. doi:10.1145/1592451.1592456.
Khattak S, Elahi T, Simon L, Swanson CM, Murdoch SJ, Goldberg I. Sok: making sense of censorship resistance systems. Proc Privacy Enhancing Technol 2016;2016(4):37–61. doi:10.1515/popets-2016-0028.
Karopoulos G, Kambourakis G, Gritzalis S, Konstantinou E. A framework for identity privacy in sip. J Netw Comput Appl 2010;33(1):16–28. doi:10. 1016/j.jnca.2009.07.004.
Karopoulos G, Kambourakis G, Gritzalis S. Privasip: ad-hoc identity privacy in sip. Comput Stand Interfaces 2011;33(3):301–14. doi:10.1016/j.csi.2010. 07.002.
Karopoulos G, Fakis A, Kambourakis G. Complete SIP message obfuscation: PrivaSIP over Tor; 2014. p. 217–26. doi:10.1109/ARES.2014.36.
Ren J, Wu J. Survey on anonymous communications in computer networks. Comput Commun 2010;33:420–31. ACM ID: 1710240 https://doi.org/10. 1016/j.comcom.2009.11.009
Kelly D, Raines R, Baldwin R, Grimaila M, Mullins B. Exploring extant and emerging issues in anonymous networks: a taxonomy and survey of protocols and metrics. IEEE Commun Surv Tutorials 2012;14(2):579–606. doi:10.1109/SURV.2011.042011.00080.
Pfitzmann A, Hansen M. A terminology for talking about privacy by data minimization: anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management; 2010.
Erdin E, Zachor C, Gunes MH. How to find hidden users: a survey of attacks on anonymity networks. IEEE Commun Surv Tutorials 2015;17(4):2296– 316. doi:10.1109/COMST.2015.2453434.
Hopper N, Vasserman EY, Chan-TIN E. How much anonymity does network latency leak? ACM Trans Inf Syst Secur 2010;13(2) 13:1–13:28.
Li B, Erdin E, Gunes MH, Bebis G, Shipley T. An overview of anonymity technology usage. Comput Commun 2013;36(12):1269–83. doi:10.1016/j. comcom.2013.04.009.
Ncher M, Calafate CT, Cano J-C, Manzoni P. An overview of anonymous communications in mobile ad hoc networks. Wireless Commun Mobile Comput 2012;12(8):661–75. doi:10.1002/wcm.990.
Danezis G, Diaz C. A survey of anonymous communication channels; 2008. MSR-TR-2008-35 http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1. 138.7951.
Linn J. Technology and web user data privacy: a survey of risks and countermeasures. IEEE Secur Privacy 2005;3(1):52–8.
Lu T, Yao P, Zhao L, Li Y, Xie F, Xia Y. Towards attacks and defenses of anonymous communication systems. Int J Secur Appl 2015;9(1):313–28.
Kitchenham B, Charters S. Guidelines for performing systematic literature reviews in software engineering; 2007. EBSE-2007-01
Kitchenham B, Pearl Brereton O, Budgen D, Turner M, Bailey J, Linkman S. Systematic literature reviews in software engineering - a systematic literature review. Inf Softw Technol 2009;51(1):7–15.
Gough D, Oliver S, Thomas J. An introduction to systematic reviews. SAGE Publications Ltd; 2012. ISBN 978-1-84920-181-0.
Borrego M, Foster MJ, Froyd JE. Systematic literature reviews in engineering education and other developing interdisciplinary fields. J Eng Educ 2014;103(1):45–76. doi:10.1002/jee.20038.
Lu T, Du S, Li Y, Dong P, Zhang X. A framework for analyzing anonymous network topology. Int J Future Gener Commun

Netw 2015;8(4):1–16.
Fang W, Wang J, Shi Z, Li F, Shan L. A study on anonymous communication technology in MANET. In: Lecture Notes in Computer Science. Springer, Cham; 2015. p. 73–81. ISBN 978-3-319-32556-9.
Kang S. Research on anonymous network topology analysis. In: Advances in intelligent systems research, 3. Atlantis Press; 2015. p. 2080–5.
Nepal S., Dahal S., Shin S. Deanonymizing schemes of hidden services in tor network: a survey. 2015, p. 468–473. doi:10.1109/ICOIN.2015.7057949.
Alsabah M, Goldberg I. Performance and security improvements for tor: a survey. ACM Comput Surv 2016;49(2) 32:36–32:1. doi:10.1145/2946802.
Zhang J, Duan H, Liu W, Wu J. Anonymity analysis of p2p anonymous communication systems. Comput Commun 2011;34(3):358–66.
Vakde G, Bibikar R, Le Z, Wright M. Enpassant: anonymous routing for disruption-tolerant networks with applications in assistive environments. Secur Commun Netw 2011;4(11):1243–56. doi:10.1002/sec.246.
Henry R, Goldberg I. Formalizing anonymous blacklisting systems; 2011. p. 81–95. doi:10.1109/SP.2011.13.
Ries T., State R., Engel T. Measuring anonymity using network coordinate systems. 2011, p. 366–371. doi:10.1109/ISCIT.2011.6089954.
Mittal P, Borisov N. Information leaks in structured peer-to-peer anonymous communication systems. ACM Trans Inf Syst Secur 2012;15(1) 5:1–5:28. doi:10.1145/2133375.2133380.
Xu G, Aguilera L, Guan Y. Accountable anonymity: a proxy re-encryption based anonymous communication system; 2012. p. 109–16. doi:10.1109/ ICPADS.2012.25.
Danezis G, Ksper E. The dangers of composing anonymous channels. Springer-Verlag; 2013. p. 191–206. ISBN 978-3-642-36372-6.
Rebollo-Monedero D, Forn J, Pallars E, Parra-Arnau J, Tripp C, Urquiza L, et al. On collaborative anonymous communications in lossy networks. Secur Commun Netw 2014;7(12):2761–77. doi:10.1002/sec.793.
Oya S, Troncoso C, Prez-Gonzlez F. Do dummies pay off? Limits of dummy traffic protection in anonymous communications. In: Lecture Notes in Computer Science. Springer International Publishing; 2014. p. 204–23. ISBN 978-3-319-08505-0.
Ma R, Rath HK, P B. Design of a mix network using connectivity index- a novel privacy enhancement approach; 2014. p. 512–17.
Elahi T, Danezis G, Goldberg I. PrivEx: private collection of traffic statistics for anonymous communication networks. In: CCS 14. ACM; 2014. p. 1068–79. ISBN 978-1-4503-2957-6.
Trushina OV, Gabidulin EM. A new method for ensuring anonymity and security in network coding. Prob Inf Transm 2015;51(1):75–81. doi:10.1134/ S0032946015010081.
Mhamdi T, Hasan O, Tahar S. Evaluation of anonymity and confidentiality protocols using theorem proving. Formal Methods Syst Des 2015;47(3):265– 86. doi:10.1007/s10703-015-0232-5.
Shirazi F, Diaz C, Wright J. Towards measuring resilience in anonymous communication networks. In: WPES 15. ACM; 2015. p. 95–9. ISBN 978-1-4503-3820-2.
Venkitasubramaniam P, Mishra A. Anonymity of memory-limited chaum mixes under timing analysis: an information theoretic perspective. IEEETrans Inf Theory 2015;61(2):996–1009.
Chaudhari M, Dharawath S. Toward a statistical framework for source anonymity in sensor network using quantitative measures; 2015. p. 1–5. doi:10.1109/ICIIECS.2015.7193169.
Doswell S, Kendall D, Aslam N, Sexton G. A longitudinal approach to measuring the impact of mobility on low-latency anonymity networks; 2015. p. 108–13. doi:10.1109/IWCMC.2015.7289066.
Sangeetha K, Ravikumar K. A novel traffic dividing and scheduling mechanism for enhancing security and performance in the tor network. Indian J Sci Technol 2015;8(7):689–94. doi:10.17485/ijst/2015/v8i7/62882.
Hamadou S, Sassone V, Yang M. An analysis of trust in anonymity networks in the presence of adaptive attackers. Math Struct Comput Sci 2015;25(2):429–56. doi:10.1017/S0960129513000650.
Dahal S, Lee J, Kang J, Shin S. Analysis on end-to-end node selection probability in Tor network; 2015. p. 46–50. doi:10.1109/ICOIN.2015.7057855.
Zhioua S. Analyzing anonymity attacks through noisy channels. Inf Comput 2015;244:76–112. doi:10.1016/j.ic.2015.08.003.
D'Arco P, De Santis A. Anonymous protocols: notions and equivalence. Theor Comput Sci 2015;581:9–25. doi:10.1016/j.tcs.2015.02.042.
Koch R, Golling M, Rodosek GD. Disequilibrium: tors exit node selection under the stereoscope, 1; 2015. p. 942–9. doi:10.1109/Trustcom.2015.468.
Backes M, Koch S, Meiser S, Mohammadi E, Rossow C. POSTER: in the net of the spider: measuring the anonymity-impact of network-level adversaries against tor. In: CCS 15. ACM; 2015. p. 1626–8. ISBN 978-1-4503-3832-5.
Berman R, Fiat A, GomuÁkiewicz M, Klonowski M, KutyÅowski M, Levinboim T, et al. Provable unlinkability against traffic analysis with low message
overhead. J Cryptol 2015;28(3):623–40. doi:10.1007/s00145-013-9171-8.
Khan M., Saddique M., Pirzada U., Zohaib M., Ali A., Wadud B., et al. The effect of malicious nodes on Tor security. 2015, p. 1–5. doi:10.1109/ARCSE. 2015.7338140.
Cangialosi F, Levin D, Spring N. Ting: measuring and exploiting latencies between all tor nodes. In: IMC 15. ACM; 2015. p. 289–302. ISBN 978-1-4503-3848-6.
Priyaa MN, Ravi G. Trust based anonymous authenticated secure routing for manets. Int J Sci Eng Res 2015;6(4):192–6.
Fuchs K-P, Herrmann D, Federrath H. Workload modelling for mix-based anonymity services. Comput Secur 2015;52:221–33. doi:10.1016/j.cose.2015. 02.004.
Jansen R, Johnson A. Safely measuring tor. In: CCS 16. ACM; 2016. p. 1553–67. ISBN 978-1-4503-4139-4.
Xue M, Ballard C, Liu K, Nemelka C, Wu Y, Ross K, et al. You can yak but you can't hide: localizing anonymous social network users. In: IMC 16. ACM; 2016. p. 25–31. ISBN 978-1-4503-4526-2.
Palmieri P. Anonymity networks and access to information during conflicts: towards a distributed network organisation; 2016. p. 263–75. doi:10. 1109/CYCON.2016.7529439.

Senftleben M, Barroso A, Bucicoiu M, Hollick M, Katzenbeisser S, Tews E. On the privacy and performance of mobile anonymous microblogging. IEEETrans Inf Forensics Secur 2016;11(7):1578–91. doi:10.1109/TIFS.2016.2541633.
Lu T., Wang Y., Zhao L., Lin Y., Zhang X. Code analysis and improvement of onion routing anonymous systems. Int J Future Gener Commun Netwa; 9(8):345–362.
Annessi R, Schmiedecker M. NavigaTor: finding faster paths to anonymity; 2016. p. 214–26. doi:10.1109/EuroSP.2016.26.
Nia MA, Atani RE, Fabian B, Babulak E. On detecting unidentified network traffic using pattern-based random walk. Secur Commun Netw 2016;9(16):3509–26. doi:10.1002/sec.1557.
Bushnag A, Abuzneid A, Mahmood A. Source anonymity in wsns against global adversary utilizing low transmission rates with delay constraints. Sensors 2016;16(7):957. doi:10.3390/s16070957.
Gomaa IA, Abd-Elrahman E, Abid M. Virtual identity approaches evaluation for anonymous communication in cloud environments. Int J Adv Comput Sci Appl 2016;7(2):367–76.
Nia MA, Babulak E, Fabian B, Atani RE. An analytical perspective to traffic engineering in anonymous communication systems; 2016. p. 1–6.
Owen G, Savage N. Empirical analysis of tor hidden services. IET Inf Secur 2016;10(3):113–18. doi:10.1049/iet-ifs.2015.0121.
Yang M, Sassone V. Minimising anonymity loss in anonymity networks under DoS attacks. In: Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2011. p. 414–29.
Ling Z, Fu X, Jia W, Yu W, Xuan D. A novel packet size based covert channel attack against anonymizer; 2011. p. 186–90.
Westermann B, Kesdogan D. Malice versus AN.ON: possible risks of missing replay and integrity protection. In: Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2011. p. 62–76. ISBN 978-3-642-27575-3.
Ling Z, Luo J, Yu W, Fu X. Equal-sized cells mean equal-sized packets in tor?; 2011. p. 1–6. doi:10.1109/icc.2011.5962653.
Qin Y, Huang D. Least squares disclosure attack in mobile ad hoc networks; 2011. p. 1–5.
Ling Z, Luo J, Yu W, Fu X, Xuan D, Jia W. A new cell-counting-based attack against tor. IEEE/ACM Trans Networking 2012;20(4):1245–61.
Ling Z, Luo J, Yu W, Yang M, Fu X. Extensive analysis and large-scale empirical evaluation of tor bridge discovery; 2012. p. 2381–9. doi:10.1109/ INFCOM.2012.6195627.
Song M, Xiong G, Li Z, Peng J, Guo L. A de-anonymize attack method based on traffic analysis; 2013. p. 455–60.
Ling Z, Fu X, Jia W, Yu W, Xuan D, Luo J. Novel packet size-based covert channel attacks against anonymizer. IEEE Trans Comput 2013;62(12):2411–26.
Jia W, Tso FP, Ling Z, Fu X, Xuan D, Yu W. Blind detection of spread spectrum flow watermarks. Secur Commun Netw 2013;6(3):257–74. doi:10.1002/ sec.540.
Ling Z, Luo J, Yu W, Fu X, Jia W, Zhao W. Protocol-level attacks against tor. Comput Netw 2013;57(4):869–86. doi:10.1016/j.comnet.2012.11.005.
Biryukov A, Pustogarov I, Weinmann R-P. Trawling for tor hidden services: detection, measurement, deanonymization. In: SP 13. IEEE Computer Society; 2013. p. 80–94. ISBN 978-0-7695-4977-4.
He G, Yang M, Luo J, Gu X. Inferring application type information from tor encrypted traffic; 2014. p. 220–7. doi:10.1109/CBD.2014.37.
Winter P, Kwer R, Mulazzani M, Huber M, Schrittwieser S, Lindskog S, et al. Spoiled onions: exposing malicious tor exit eelays. In: Lecture Notes in Computer Science. Springer, Cham; 2014. p. 304–31. ISBN 978-3-319-08505-0.
Thandra PK, Rajan J, Satyamurty SAV. Unconditionally anonymous controllable id-based ring signatures. J Discrete Math Sci Cryptography 2015;18(6):849–67.
Chakravarty S, Portokalidis G, Polychronakis M, Keromytis AD. Detection and analysis of eavesdropping in anonymous communication networks. Int J Inf Secur 2015;14(3):205–20. doi:10.1007/s10207-014-0256-7.
He G, Yang M, Luo J, Gu X. A novel application classification attack against tor. Concurrency Comput 2015;27(18):5640–61. doi:10.1002/cpe.3593.
Li Q, Liu P, Qin Z. A stealthy attack against tor guard selection. Int J Secur Appl 2015;9(11):391–402.
Tian G, Duan Z, Baumeister T, Dong Y. A traceback attack on freenet. IEEE Trans Dependable Secure Comput 2015;14(3):294–307. doi:10.1109/TDSC. 2015.2453983.
Matic S, Kotzias P, Caballero J. CARONTE: detecting location leaks for deanonymizing tor hidden services. In: CCS 15. ACM; 2015. p. 1455–66. ISBN 978-1-4503-3832-5.
Park KC, Shin H, Park WH, Lim JI. New detection method and countermeasure of cyber attacks in mix networks. Multimed Tools Appl 2015;74(16):6509–18. doi:10.1007/s11042-014-2127-7.
Panchenko A. On the impact of cross-layer information leakage on anonymity in crowds. ACM; 2015. p. 35–42. ISBN 978-1-4503-3757-1.
Kosugi T, Hayafuji T, Mambo M. On the traceability of the accountable anonymous channel; 2015. p. 6–11. doi:10.1109/AsiaJCIS.2015.29.
Arp D, Yamaguchi F, Rieck K. Torben: a practical side-channel attack for deanonymizing tor communication. In: ASIA CCS 15. ACM; 2015. p. 597–602. ISBN 978-1-4503-3245-3.
Xue Y, Vasserman EY. Simple and compact flow fingerprinting robust to transit through low-latency anonymous networks; 2016. p. 765–73. doi:10. 1109/CCNC.2016.7444875.
Jia Y, Bai G, Saxena P, Liang Z. Anonymity in peer-assisted cdns: inference attacks and mitigation. Proc Privacy Enhancing Technol 2016;2016(4):294– 314. doi:10.1515/popets-2016-0041.
Zang W, Zhang P, Wang X, Shi J, Guo L. Detecting sybil nodes in anonymous communication systems. Proc Comput Sci 2013;17:861–9. doi:10.1016/j. procs.2013.05.110.
Baumeister T, Dong Y, Tian G, Duan Z. Using randomized routing to counter routing table insertion attack on Freenet; 2013. p. 754–9. doi:10.1109/ GLOCOM.2013.6831163.
Hoang NP, Asano Y, Yoshikawa M. Anti-RAPTOR: anti routing attack on privacy for a securer and scalable Tor; 2015. p. 147–54. doi:10.1109/ICACT. 2015.7224775.
Alsemairi S, Younis M. Clustering-based mitigation of anonymity attacks in wireless sensor networks; 2015. p. 1–7. doi:10.1109/GLOCOM.2015. 7417501.
Wang ZJ, Pei HR, Wang Y. Sampling traffic analysis of anonymous communications in mobile ad hoc networks; 2013. p. 233–9. doi:10.1109/MSN. 2013.38.

Mittal P, Khurshid A, Juen J, Caesar M, Borisov N. Stealthy traffic analysis of low-latency anonymous communication using throughput fingerprinting.
In: CCS 11. ACM; 2011. p. 215–26. ISBN 978-1-4503-0948-6
Das A, Borisov N. Securing anonymous communication channels under the selective DoS attack. In: Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2013. p. 362–70.
Radenkovic M, Vaghi I. Adaptive user anonymity for mobile opportunistic networks. In: CHANTS 12. ACM; 2012. p. 79–82. ISBN 978-1-4503-1284-4.
Rass S, Wigoutschnigg R, Schartner P. Crowds based on secret-sharing. In: ARES 11. IEEE Computer Society; 2011. p. 359–64. ISBN 978-0-7695-4485-4.
Mallesh N, Wright M. An analysis of the statistical disclosure attack and receiver-bound cover. Comput Secur 2011;30(8):597–612. doi:10.1016/j.cose. 2011.08.011.
Peng K. How to communicate anonymously in a network: study and optimisation of efficiency and security of anonymous communication networks. Int J Secur Netw 2012;7(3):133–47. doi:10.1504/IJSN.2012.052525.
Rebollo-Monedero D, Parra-Arnau J, Forn J, Diaz C. Optimizing the design parameters of threshold pool mixes for anonymity and delay. Comput Netw 2014;67:180–200. doi:10.1016/j.comnet.2014.04.007.
Nia MA, Atani RE, Ruiz-MartÃnez A. Privacy enhancement in anonymous network channels using multimodality injection. Secur Commun Netw 2015;8(16):2917–32. doi:10.1002/sec.1219.
Bouda J, Å projcar J. Quantum communication between anonymous sender and anonymous receiver in the presence of strong adversary. Int J Quant
Inf 2011;9(2):651–63. doi:10.1142/S0219749911007691.
Ghafir I, Svoboda J, Prenosil V. Tor-based malware and Tor connection detection; 2014. p. 1–6. doi:10.1049/cp.2014.1411.
Madani S, Khalil I. Garbled routing (gr): a generic framework towards unification of anonymous communication systems. Journal of Network and Computer Applications 2014;44:183–95.
Brubaker C, Houmansadr A, Shmatikov V. CloudTransport: using cloud storage for censorship-resistant networking. In: Lecture Notes in Computer Science. Springer International Publishing; 2014. p. 1–20. ISBN 978-3-319-08505-0.
Snader R, Borisov N. Improving security and performance in the tor network through tunable path selection. IEEE Trans Dependable Secure Comput 2011;8(5):728–41. doi:10.1109/TDSC.2010.40.
Ling Z, Luo J, Wu K, Yu W, Fu X. TorWard: discovery of malicious traffic over Tor; 2014. p. 1402–10. doi:10.1109/INFOCOM.2014.6848074.
Hopper N. Challenges in protecting tor hidden services from botnet abuse. In: Lecture Notes in Computer Science. Springer, Berlin, Heidelberg; 2014. p. 316–25. ISBN 978-3-662-45471-8.
Haraty RA, Zantout B. A collaborative-based approach for avoiding traffic analysis and assuring data integrity in anonymous systems. Comput Human Behav 2015;51:780–91. doi:10.1016/j.chb.2014.09.031.
Hoang NP, Pishva D. A TOR-based anonymous communication approach to secure smart home appliances; 2015. p. 517–25. doi:10.1109/ICACT.2015. 7224918.
Scaife N, Carter H, Traynor P. OnionDNS: a seizure-resistant top-level domain; 2015. p. 379–87. doi:10.1109/CNS.2015.7346849.
Feng F, Matsuura K. Stronger bridge mechanisms of tor which take into consideration exhaustive adversarial models. J Inf Process 2015;23(5):646–54. doi:10.2197/ipsjjip.23.646.
Barton A, Wright M. Denasa: destination-naive as-awareness in anonymous communications. Proc Privacy Enhancing Technol 2016;2016(4):356–72. doi:10.1515/popets-2016-0044.
Mishra A, Venkitasubramaniam P. Admissible length study in anonymous networking: a detection theoretic perspective. IEEE J Sel Areas Commun 2013;31(9):1957–69. doi:10.1109/JSAC.2013.130926.
Barroso A, Hollick M. Performance evaluation of delay-tolerant wireless friend-to-friend networks for undetectable communication; 2015. p. 474–7. doi:10.1109/LCN.2015.7366356.
Akhoondi M, Yu C, Madhyastha HV. LASTor: a low-latency AS-aware tor client; 2012. p. 476–90. doi:10.1109/SP.2012.35.
Akhoondi M, Yu C, Madhyastha HV. Lastor: a low-latency as-aware tor client. IEEE/ACM Trans Netw 2014;22(6):1742–55. doi:10.1109/TNET.2013. 2291242.
Bolla JV, Vatsavayi VK, Murthy JVR. Anonymity and security in mobile Ad Hoc networks. In: Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2012. p. 71–82.
Kang L. Efficient botnet herding within the tor network. J Comput Virol Hack Tech 2015;11(1):19–26. doi:10.1007/s11416-014-0229-4.
Kale TG, Ohzahata S, Wu C, Kato T. Evaluation of dynamic circuit switching to reduce congestion in Tor; 2015. p. 326–31. doi:10.1109/ATNAC.2015. 7366834.
Watfa MK, Diab M, Stephen N. Improving TCP performance in mix networks. In: Advances in Intelligent Systems and Computing. Springer, Cham; 2015. p. 423–8. ISBN 978-3-319-08421-3.
Yang L, Li F. mTor: a multipath Tor routing beyond bandwidth throttling; 2015. p. 479–87. doi:10.1109/CNS.2015.7346860.
Emura K, Kanaoka A, Ohta S, Takahashi T. A KEM/DEM-based construction for secure and anonymous communication, 3; 2015. p. 680–1.
Ling Z, Luo J, Yu W, Yang M, Fu X. Tor bridge discovery: extensive analysis and large-scale empirical evaluation. IEEE Trans Parallel Distrib Syst 2015;26(7):1887–99. doi:10.1109/TPDS.2013.249.
Milajerdi SM, Kharrazi M. A composite-metric based path selection technique for the tor anonymity network. J Syst Softw 2015;103:53–61.
Yajam HA, Mohajeri J, Salmasizadeh M. Identity-based universal re-encryption for mixnets. Secur Commun Netw 2015;8(17):2992–3001. doi:10.1002/ sec.1226.
Wu B, Shastri BJ, Mittal P, Tait AN, Prucnal PR. Optical signal processing and stealth transmission for privacy. IEEE J Sel Top Signal Process 2015;9(7):1185–94. doi:10.1109/JSTSP.2015.2424690.
Ghosh S, Kate A. Post-quantum forward-secure onion routing. In: Lecture Notes in Computer Science. Springer, Cham; 2015. p. 263–86. ISBN 978-3-319-28165-0.

Gañán C, Muñoz JL, Esparza O, Mata-D˜ıaz J, Alins J. Epa: an efficient and privacy-aware revocation mechanism for vehicular ad hoc networks. Perva- sive Mob Comput 2015;21:75–91.
Schwarte P, Bourimi M, Heupel M, Kesdogan D, Gimenez R, Wrobel S, et al. Multilaterally secure communication anonymity in decentralized socialnetworking; 2013. p. 498–504.
Le Blond S, Choffnes D, Caldwell W, Druschel P, Merritt N. Herd: a scalable, traffic analysis resistant anonymity network for VoIP systems. In: SIGCOMM 15. ACM; 2015. p. 639–52. ISBN 978-1-4503-3542-3.
Khasnikar AK. Anonymity protection using ALERT in MANET; 2015. p. 1–3.
Pereñíguez García F, Marín-López R, Kambourakis G, Ruiz-Martínez A, Gritzalis S, Skarmeta-Gómez AF. Kamu: providing advanced user privacy in kerberos multi-domain scenarios. Int J Inf Secur 2013;12(6):505–25. doi:10.1007/s10207-013-0201-1.
Arnedo-Moreno J, Prez-Gilabert N, Domingo-Prieto M. Anonymously accessing jxta community services through split message forwarding. Math Comput Model 2013;58(5–6):1313–27. doi:10.1016/j.mcm.2013.01.005.
Abuzneid A-S, Sobh T, Faezipour M, Mahmood A, James J. Fortified anonymous communication protocol for location privacy in wsn: a modularapproach. Sensors (Basel, Switzerland) 2015;15(3):5820–64. doi:10.3390/s150305820.
Hibaoui AE, Vallet L. Hypergraph model for anonymous communications; 2012. p. 888–94. doi:10.1109/ICMCS.2012.6320207.
Jiang R, Xing Y. Anonymous on-demand routing and secure checking of traffic forwarding for mobile ad hoc networks; 2012. p. 406–11. doi:10.1109/ SRDS.2012.6.
Shi C, Luo X, Traynor P, Ammar MH, Zegura EW. Arden: anonymous networking in delay tolerant networks. Ad Hoc Netw 2012;10(6):918–30. doi:10. 1016/j.adhoc.2011.11.008.
Campos J, Calafate CT, Ncher M, Manzoni P, Cano J-C. HOP: achieving efficient anonymity in MANETs by combining HIP, OLSR, and pseudonyms. In: OOPSLA 06. ACM; 2006. p. 975–85. ISBN 978-1-59593-491-8.
Singh K, Rangan CP, Banerjee AK, Singh K, Rangan CP, Banerjee AK. Lattice based mix network for location privacy in mobile system, lattice based mix network for location privacy in mobile system. Mob Inf Syst Mob Inf Syst 2015:e963628. doi:10.1155/2015/963628. 2015, 2015
Mahmoud MMEA, Taha S, Misic J, Shen X. Lightweight privacy-preserving and secure communication protocol for hybrid ad hoc wireless networks. IEEE Trans Parallel Distrib Syst 2014;25(8):2077–90. doi:10.1109/TPDS.2013.298.
Madani S, Khalil I. Multi-binomial mixes: a proposal for secure and efficient anonymous communication. Comput Netw 2015;93(Part 1):41–53. doi:10. 1016/j.comnet.2015.10.007.
Lv J, Zhang T, Li Z, Cheng X. Pacom: parasitic anonymous communication in the bittorrent network. Comput Netw 2014;74(Part A):13–33. doi:10. 1016/j.comnet.2014.08.015.
Manjuladevi V, Bharathi RJ. Anonymous location aided secure routing protocol; 2014. p. 1–6. doi:10.1109/ICICES.2014.7034099.
Chen S, Wu M. Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks, 1; 2010. p. 582–5. doi:10.1109/ICMTMA. 2010.602.
Vo B, Bellovin S. Anonymous publish-subscribe systems. In: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommu- nications Engineering. Springer, Cham; 2014. p. 195–211. ISBN 978-3-319-23828-9.
Fleming C, Zhou X, Liu D, Liang H. DiffuseNet: a random walk based anonymity network; 2014. p. 877–81. doi:10.1109/ICSPCC.2014.6986323.
Jebri S, Abid M, Bouallegue A. An efficient scheme for anonymous communication in IoT; 2015. p. 7–12. doi:10.1109/ISIAS.2015.7492763.
Imran S, Karthick RV, Visu P. DD-SARP: dynamic data secure anonymous routing protocol for MANETs in attacking environments; 2015. p. 39–46. doi:10.1109/ICSTM.2015.7225388.
Xiao H, Song H, Wang W. EPAMP: an anonymous multicast protocol in mobile Ad Hoc networks. In: Lecture Notes in Computer Science. Springer, Cham; 2015. p. 276–89. ISBN 978-3-319-27160-6.
Hsu RH, Lee J. Group anonymous D2D communication with end-to-end security in LTE-A; 2015. p. 451–9. doi:10.1109/CNS.2015.7346857.
Lo NW, Chiang MC, Hsu CY. Hash-based anonymous secure routing protocol in mobile Ad Hoc networks; 2015. p. 55–62. doi:10.1109/AsiaJCIS.2015.27.
Chen C, Asoni DE, Barrera D, Danezis G, Perrig A. HORNET: high-speed onion routing at the network layer. In: CCS 15. ACM; 2015. p. 1441–54. ISBN 978-1-4503-3832-5.
Antunez-Veas A, Navarro-Arribas G. Onion routing in deterministic delay tolerant networks. In: Lecture Notes in Computer Science. Springer, Cham; 2015. p. 303–10. ISBN 978-3-319-30302-4.
Baek S., Seo S.-H., Kim S. Preserving biosensor users anonymity over wireless cellular network. 2015, p. 470–475. doi:10.1109/ICUFN.2015.7182588.
Borges F, Santos RAM, Marquezino FL. Preserving privacy in a smart grid scenario using quantum mechanics. Secur Commun Netw 2015;8(12):2061– 9. doi:10.1002/sec.1152.
Ogah CPA, Cruickshank H, Sun Z, Chandrasekaran G, Cao Y, Asuquo PM, et al. Privacy-enhanced group communication for vehicular delay tolerant networks; 2015. p. 193–8. doi:10.1109/NGMAST.2015.67.
Papapetrou E, Bourgos VF, Voyiatzis AG. Privacy-preserving routing in delay tolerant networks based on Bloom filters; 2015. p. 1–9. doi:10.1109/ WoWMoM.2015.7158148.
Hermoni O, Gilboa N, Felstaine E, Dolev S. Rendezvous tunnel for anonymous publishing. Peer-to-Peer Netw Appl 2015;8(3):352–66. doi:10.1007/ s12083-014- 0254- 6.
Arya KV, Saxena R. S-ALERT: secure anonymous location-based efficient routing protocol; 2014. p. 1–6. doi:10.1109/ICIINFS.2014.7036496.
Gagneja KK. Secure communication scheme for wireless sensor networks to maintain anonymity; 2015. p. 1142–7. doi:10.1109/ICCNC.2015.7069511.
Movahedi M, Saia J, Zamani M. Secure multi-party shuffling. In: Lecture Notes in Computer Science. Springer, Cham; 2015. p. 459–73. ISBN 978-3-319-25257-5.
Tao F, Fei X, Ye L, Li FJ. Secure network coding-based named data network mutual anonymity communication protocol;

2015.
Zeng T, Shen M, Wang M, Zhu L, Li F. Self-adaptive anonymous communication scheme under SDN architecture; 2015. p. 1–8. doi:10.1109/PCCC.2015. 7410337.
Tan Q, Shi J, Fang B, Zhang W, Wang X. StegoP2P: oblivious user-driven unobservable communications; 2015. p. 7126–31. doi:10.1109/ICC.2015. 7249463.
Chakravarty S, Naik V, Acharya HB, Tanwar CS. Towards practical infrastructure for decoy routing (positional paper); 2015. p. 1–6.
Ekhtiarabadi MA, Yajam HA, Mohajeri J, Salmasizadeh M. Verifiable identity-based mix network; 2015. p. 406–9. doi:10.1109/IranianCEE.2015.7146249.
Safaka I, Czap L, Argyraki K, Fragouli C. Towards unconditional tor-like anonymity; 2015. p. 66–70. doi:10.1109/NETCOD.2015.7176791.
Ike M, Sarac K. PPEP: a deployable privacy preserving E-Commerce protocol for electronic goods. In: ICCNS 16. ACM; 2016. p. 104–12. ISBN 978-1-4503-4783-9.
Madhusudhan R, Shashidhara. An efficient and secure authentication scheme with user anonymity for roaming service in global mobile networks.In: ICCNS 16. ACM; 2016. p. 119–26. ISBN 978-1-4503-4783-9.
Bultel X, Gambs S, Grault D, Lafourcade P, Onete C, Robert J-M. A prover-anonymous and terrorist-fraud resistant distance-bounding protocol. In: WiSec 16. ACM; 2016. p. 121–33. ISBN 978-1-4503-4270-4.
Piao C, Li X, Pan X, Zhang C. User privacy protection for a mobile commerce alliance. Electron Commer Res Appl 2016;18:58–70. doi:10.1016/j.elerap. 2016.03.005.
Florian M, Pieper F, Baumgart I. Establishing location-privacy in decentralized long-distance geocast services. Ad Hoc Netw 2016;37:110–21. doi:10. 1016/j.adhoc.2015.07.015.
Caballero-Gil C, Molina-Gil J, Hernndez-Serrano J, Len O, Soriano-Ibaez M. Providing k-anonymity and revocation in ubiquitous vanets. Ad Hoc Netw 2016;36:482–94. doi:10.1016/j.adhoc.2015.05.016.
Qian C, Shi J, Yu Z, Yu Y, Zhong S. Garlic cast: lightweight and decentralized anonymous content sharing; 2016. p. 216–23. doi:10.1109/ICPADS.2016. 0037.
Yu H, Lee E, Lee SB. Symbiosis: anti-censorship and anonymous web-browsing ecosystem. IEEE Access 2016;4:3547–56. doi:10.1109/ACCESS.2016. 2585163.
Li D, Liu J, Liu W. Secure and anonymous data transmission system for cluster organised space information network; 2016. p. 228–33. doi:10.1109/ SmartCloud.2016.12.
Zhu T, Feng D, Hua Y, Wang F, Shi Q, Liu J. MIC: an efficient anonymous communication system in data center networks; 2016. p. 11–20. doi:10.1109/ ICPP.2016.9.
Wang Q, Yu C, Gao F, Qi H, Wen Q. Self-tallying quantum anonymous voting. Phys Rev A 2016;94(2):022333. doi:10.1103/PhysRevA.94.022333.
Ren J, Li Y, Jiang T, Li T. Anonymous communication in overlay networks. Secur Commun Netw 2016;9(3):229–40. doi:10.1002/sec.539.
Emura K, Kanaoka A, Ohta S, Omote K, Takahashi T. Secure and anonymous communication technique: formal model and its prototype implementa- tion. IEEE Trans Emerg Top Comput 2016;4(1):88–101. doi:10.1109/TETC.2015.2400131.
Sabra Z, Artail H. Using group anonymity to hide the identity of voip mobile users communicating over hybrid networks while preserving quality of service. Wirel Commun Mob Comput 2016;16(17):2792–808. doi:10.1002/wcm.2725.
Baek S, Seo S-H, Kim S. Preserving patients anonymity for mobile healthcare system in iot environment. Int J Distrib Sens Netw 2016;12(7):2171642. doi:10.1177/155014772171642.
Tsudik G, Uzun E, Wood CA. AC3N: anonymous communication in content-centric networking; 2016. p. 988–91. doi:10.1109/CCNC.2016.7444924.
Lu T, Zhang X, Du X, Li Y. F-Crowds: an anonymity scheme for p2p file-sharing. Int J Secur Applb 2016;10(6):1–12.
Zhao X, Li L, Xue G, Ahn GJ. Efficient anonymous message submission. IEEE Trans Dependable Secure Comput 2016;PP(99). doi:10.1109/TDSC.2016. 2556659. 1–1
Lin D, Sherr M, Loo BT. Scalable and anonymous group communication with mtor. Proc Privacy Enhancing Technol 2015;2016(2):22–39. doi:10.1515/ popets-2016-0003.
Palmieri P, Pouwelse J. Paying the guard: an entry-guard-based payment system for tor. In: Lecture Notes in Computer Science. Springer, Berlin, Heidelberg; 2015. p. 437–44. ISBN 978-3-662-47853-0.
Hofheinz D, Kiltz E. Secure hybrid encryption from weakened key encapsulation. In: CRYPTO07. Springer-Verlag; 2007. p. 553–71. ISBN 978-3-540-74142-8.
Li C-T, Hwang M-S. A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks. Inf Sci (Ny) 2011;181(23):5333–47.
Taheri S, Hartung S, Hogrefe D. Anonymity and privacy in multicast mobile ad hoc networks. In: SIN'13. ACM; 2013. p. 241–50. ISBN 978-1-4503-2498-4.
Chen J, Zhang H, Fang B, Du X, Yin L, Yu X. Towards efficient anonymous communications in sensor networks; 2011. p. 1–5. doi:10.1109/GLOCOM. 2011.6133560.
Zou X., Qi M., Li F., Sui Y., Wang K. A new scheme for anonymous secure group communication. 2011, p. 1–9. doi:10.1109/HICSS.2011.19.
Pereniguez F, Marin-Lopez R, Kambourakis G, Gritzalis S, Gomez A. Privakerb: a user privacy framework for kerberos. Comput Secur 2011;30(6– 7):446–63. doi:10.1016/j.cose.2011.04.001.
Arnedo-Moreno J., Domingo-Prieto M., Pérez Gilabert N. Anonymous communications for jxta peer-to-peer services: a multi-protocol approach. IN3Working Paper Series2013b; 0(0).
Tian G, Duan Z, Baumeister T, Dong Y. Reroute on loop in anonymous peer-to-peer content sharing networks; 2014. p. 409–17. doi:10.1109/CNS.2014. 6997510.
Girry KT, Ohzahata S, Wu C, Kato T. Reducing congestion in the tor network with circuit switching. J Inf Process 2015;23(5):589–602. doi:10.2197/ ipsjjip.23.589.
Wittayasatiankul S, Chumjai S, Tuaycharoen N. Tors API on iOS. In: Advances in Intelligent Systems and Computing. Springer, Cham; 2015. p. 267–74. ISBN 978-3-319-19023-5.
Le Blond S, Choffnes D, Zhou W, Druschel P, Ballani H, Francis P. Towards efficient traffic-analysis resistant anonymity networks. In: SIGCOMM 13. ACM; 2013. p. 303–14. ISBN 978-1-4503-2056-6.

Sujatha G, Azeem MA. UOSHR: unobservable secure hybrid routing protocol for fast transmission in MANET. In: Advances in Intelligent Systems and Computing. Springer, Cham; 2015. p. 467–74. ISBN 978-3-319-13730-8.
Frster D, Kargl F, Lhr H. Puca: a pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks. Ad Hoc Netw 2016;37:122–32. doi:10.1016/j.adhoc.2015.09.011.
Miao J, Hasan O, Mokhtar SB, Brunie L, Hasan A. 4pr: Privacy preserving routing in mobile delay tolerant networks. Comput Netw 2016;111:17–28. doi:10.1016/j.comnet.2016.08.005.
Chang CS, Ho T, Effros M. Peer-to-peer anonymous networking using coding; 2012. p. 525–32. doi:10.1109/Allerton.2012.6483263.
Bouzid Z, Travers C. Anonymity-preserving failure detectors. In: Lecture Notes in Computer Science. Springer, Berlin, Heidelberg; 2016. p. 173–86. ISBN 978-3-662-53425-0.
Finster S, Baumgart I. Pseudonymous smart metering without a trusted third party; 2013. p. 1723–8. doi:10.1109/TrustCom.2013.234.
Yu M, Liu W, Xing T. A new trust model for trustworthiness-based routing protocols in sensor networks; 2012. p. 56–61.
Liu W, Yu M. Aasr: authenticated anonymous secure routing for manets in adversarial environments. IEEE Trans Veh Technol 2014;63(9):4585–93. doi:10.1109/TVT.2014.2313180.
Florian M, Finster S, Baumgart I. Privacy-preserving cooperative route planning. IEEE Internet Things J 2014;1(6):590–9. doi:10.1109/JIOT.2014.2361016.
Patel M, Rao S, Mothkur R. An efficient anonymous secure routing (easr) protocol for manets in adversial environment. Adv Comput Sci Inf Technol (ACSIT) 2015;2(11):69–73.
Taheri S, Hartung S, Hogrefe D. Anonymous group-based routing in manets. J Inf Secur Appl 2015;22:87–98. doi:10.1016/j.jisa.2014.09.002.
Basu A, Corena JC, Vaidya J, Crowcroft J, Kiyomoto S, Marsh S, et al. Lightweight practical private one-way anonymous messaging. In: IFIP Advances in Information and Communication Technology. Springer, Cham; 2015. p. 76–91. ISBN 978-3-319-18490-6.
Karthick SA, Sudhakar K. Secure neighbor discovery system for ad-hoc through aasr protocol. Int J Comput Sci Inf Technol Secur (IJCSITS) 2014;4(6):145–8.
Pham DV, Kesdogan D. Towards relations between the hitting-set attack and the statistical disclosure attack. In: IFIP Advances in Information and Communication Technology. Springer, Cham; 2015. p. 35–50. ISBN 978-3-319-18466-1.
de Sales TBM, Perkusich A, de Sales LM, de Almeida HO, Soares G, de Sales M. Asap-v: a privacy-preserving authentication and sybil detection protocol for vanets. Inf Sci (Ny) 2016;372:208–24. doi:10.1016/j.ins.2016.08.024.
Snchez-Carmona A, Robles S, Borrego C. Privhab: a privacy preserving georouting protocol based on a multiagent system for podcast distribution on disconnected areas. Ad Hoc Netw 2016;53:110–22. doi:10.1016/j.adhoc.2016.09.019.
R S, M D. Enhanced bio-trusted anonymous authentication routing technique of wireless body area network. Biomed Res 2016;0(0).
Pan J, Ma L, Yu K. FASRP: a fully anonymous security routing protocol in MANETs. In: Lecture Notes in Computer Science. Springer, Cham; 2016. p. 292–304. ISBN 978-3-319-49147-9.