

ADAM KUBIACZYK

Institute of Telecommunications, Warsaw University of Technology

IGOR MARGASIŃSKI

Institute of Telecommunications, Warsaw University of Technology

ON THE IMPACT OF CONTENT-BASED OVERLAY ROUTING ON PRIVACY

Abstract

In this paper we evaluate privacy information leaks via content-based overlay routing using an example of popular DHT network called KAD. Recent research has shown that content-based routing pose a significant threat for privacy and a number of improvements have been proposed. We analyse privacy of the improved content-based routing for KAD network using information entropy measurement model and show that the considered solution still can be a target of unsophisticated attacks.

Key words

Overlay networks, Overlay routing, Privacy

1. Introduction

Routing of the today's Internet becomes virtual. In the course of these changes, meta-data particularly related to privacy play a leading role as addressing information. As limitations of IP routing arise we can observe significant growth of routing strategies introduced for overlay networks, including Peer-to-Peer overlays. Currently, P2Ps—at the forefront of service overlays—represent the most part of the Internet traffic. Undoubtedly, further development of routing and localization solutions for the Internet will be focused on integration and interoperability of routing protocols coexisting on different network layers. Nevertheless, integration for today's routing is called not only in the scope of cross-layer symbiosis between different routing protocols and topologies but also within privacy enhancing technologies. As meta-data of content resources and users' digital identities become widely used addressing information possible misuses of this communications grow. Coming back to the environment of P2P overlays, the risk is increased even further as the privacy violation can come easily from any connected participant or group of participants of the P2P network.

In this paper we consider the impact of content-based routing on privacy using an example of *KAD*—a dynamically expanding overlay network of the world-wide range. A growing field of literature is studying performance and privacy of *KAD*. It was showed that this the most popular DHT overlay network of today is vulnerable to various misuses and privacy violation [1–4]. Recently, a number of corresponding improvements have been proposed [2, 4, 5]. In this position we model the considered improved version of *KAD* (referred in the rest of the paper as privacy-aware *KAD* or *PA-KAD* for simplification) and evaluate its information leaks related to users privacy in terms of associations between meta-data describing content and meta-data describing users.

2. Previous Work

In the field of overlay routing, distributed hash tables (DHT) proved to be a robust platform for scalable and fast response content-based look-up and routing. The distributed hash table concept is based on an abstract *keyspace*. Each node of a DHT system is assigned a unique ID belonging to this specific *keyspace* which is calculated to provide a uniform distribution of ID in the *keyspace*. Moreover, each of the nodes is responsible for the maintenance of a part of the *keyspace*. When a new object is published within the system it is given a key based on a result of a hash function known to all nodes. This result determines the place of the object in the *keyspace* and simultaneously points a node responsible for this object. Node trying to publish a file in the DHT structure calculates a hash function k of the file content (*data*) and publishes $(k, data)$ pair. As a result, a node responsible of the key k is found and data is stored in the node's file system. From this moment, a node trying to gain access to the content hash to retrieve the data has to know k by which responsible node is found and a data delivered to the node asking for the key. System structured like this would not be possible without an overlay network as an efficient communication platform enabling an exchange of ID information. Publication [6] resulted in several implementations of DHT systems e.g.: *CAN* [7], *Chord* [8], *Pastry* [9], and *Kademlia* [10]. Each one of these systems presents a slightly different approach to *keyspace* partitioning, routing and structure maintenance.

As far as we know *KAD* network is the widest deployed DHT based system. It is *Kademlia* protocol based system which implements all of its functionality in a distributed manner. The system does not have an official documentation, but the protocol has been well documented in [3] by analyzing a source code of *aMule* client. *KAD* uses a 128-bit one dimensional *keyspace*. Each node chooses its ID randomly during it's first join to the DHT structure. XOR metric presented by *Kademlia* protocols is crucial to all processes in the *KAD* network. In order to calculate XOR metric a binary representation of two ID are xored bit by bit. The decimal meaning of the binary result can be used to define a distance in the *Kademlia* *keyspace*. It is worth noting that differences on the more significant bits are more influential on the distance that differences on the less significant bits of XOR result. Nodes organize information about other node's IP addresses and operating ports in the tree structured routing table. The maintenance is performed during routing to continuously keep the most fresh contacts in the routing tables. Moreover, there is a "hello" message send to the contacts that are inactive for a longer period of time.

Look-up is a process of finding a node responsible for a given key. KAD performs an iterative look-up. It means that initiating node takes control of the look-up by sending request to subsequent closer to the destination with every hop nodes. To make this process more effective KAD initiates several parallel searches using only one contact list enabling an optimization of look-up process. The parallelism factor is hardcoded in the KAD client and equals 3. Research shows that this method significantly lowers routing latency in overlay networks under high churn [11]. Node performing look-up of a specific ID creates a list of nodes closest to the ID sorted by the XOR metric ascending. Only three first contacts are contacted, if they are not responsible for the key they answer with two contacts closer to the destination ID. After each reply a list of closest nodes is updated with the new contacts and used ones are marked. This process lasts until nodes responsible for the ID are found. In KAD such nodes are placed in so called tolerance zone. This is a zone defined by a set of nodes having IDs with common first 8-bits. In other words if key has at least 8-bit common with an ID of a node, it can be stored on this node. File publication process can be divided in to two stages. Meta-data is published separately to information describing content localization. This is required due to the fact that KAD enables users to search file by keyword.

We consider privacy of KAD content-based routing in a scope of possibility of tracking associations of KAD users with the particular **content downloads**. Before content download, initiator performs **content look-up** (localization of file) in a KAD network. In this process at least one keyword referring to the file is needed. Hash function is computed on the first key word and initiates a key look-up. As soon as nodes responsible for this ID are found a whole list of keywords and meta-data describing a desired content is delivered to them. Nodes filter their database of keys and respond with a list of files which fulfill the requirements. User selects specific file and a process of **source look-up** (localization of nodes which stores a particular content) is started. As a result user is presented with a list of nodes which store the looked-up content.

There has been much research done on KAD network. Long term empirical study of KAD performed by Steiner *et al.* [1] showed that KAD community consists of 3-4 million of users connecting simultaneously, but about 40% of them cannot participate in a DHT structure due to the NAT (Network Address Translation) limitations and clients tend to use KAD everyday for many hours. Weng *et al.* [2] present critical design weaknesses of KAD enabling adversary to corrupt node routing tables causing significant fraction of searches to fail. Brunner [3] shows an attack model which gives an adversary a control over a specific key. Similar strategy is presented by Steiner *et al.* [4] called *eclipse attack*. Also several DDoS strategies was introduced in [4].

3. Information Leaks via KAD content-based routing

We consider a threat model with a partial adversary who controls a colluding fraction ρ of all overlay network nodes N . These malicious nodes are able to provide both passive and active attacks. We consider static adversary unable to arbitrarily adapt the set of malicious nodes.

It has been noticed [3,4] that the adversary can easily take control over a specific key. As a consequence every specific look-up chosen by the adversary can be compromised. This gives the adversary tools efficient enough to point out initiator of chosen actions eg. downloading specific file. The adversary assigns a probability of being the initiator to each node in the network. Let p_i be probability of being the initiator of i node. Initiator is given a probability equals 1, because the initiator contacts the attacker in order to download the file, hence the attacker knows the initiator. Then, the rest of honest nodes are beyond suspicion so the adversary assigns them probability of being the initiator equal 0. According to the information theory [12,13], information entropy of KAD equals

$$\mathcal{H}_{kad} = - \sum_{i=1}^N p_i \log_2(p_i) = 0. \quad (1)$$

In other words initiator is always evident for the adversary.

3.1. Analysis of PA-KAD

Steiner *et al.* [4] proposed several centralized solution for KAD network disabling attacker to obtain an arbitrary node ID based on a central agent concept binding node ID to a cell phone number. Lightweight, but weaker mitigation techniques concerning identity authentication were introduced by Weng *et al.* [2] such as hashed IP or public key node ID generation. Whereas Castro *et al.* [5] suggest a certified node ID creation making an attack expensive in terms of money. We believe that the improvements lead to the situation, where colluding nodes are uniformly distributed in the key space. However, attacking nodes still can fill their routing tables with contacts of colluding nodes only. We assume that when a message is sent to the colluding node, it cannot go out of the adversary's "structure". To provide privacy in this environment it is crucial to ensure that an initiator does not communicate with colluding nodes during entire process of the content look-up and content download.

3.1.1. Content Look-up

Let us consider performing look-up of a keyword without contacting any of the colluding nodes. We can assign each node probability p_h that the node is honest

$$p_h = 1 - \rho. \quad (2)$$

The initiator performs an iterative look-up so it communicates with set of nodes before reaching the target. Probability p_v that during the look-up process the initia-

tor will not communicate with any of the colluding nodes is

$$p_v = p_h^r = (1 - \rho)^r, \quad (3)$$

where r is number of iteration to the target. Attacker is uniformly distributed in the keyspace, so are the look-up results. Then finally, probability p_c that the resulting target node anxiety honest is

$$p_c = p_v p_h = (1 - \rho)^{r+1}. \quad (4)$$

3.1.2. Source Look-up

Similarly, we define probability p_s of event that the result returned as a consequence of source look-up is honest as

$$p_s = p_v p_c = (1 - \rho)^{2r+1}. \quad (5)$$

Probability that the result of source look-up belongs to the adversary is $1 - p_s$. It is important to notice, that each file in KAD network is downloaded from several sources. Then, p_x probability that within x owners at least one was colluding node is defined by

$$p_x = 1 - ((1 - \rho)^{2r+1})^x. \quad (6)$$

3.1.3. Content Download

Provided the fact the initiator avoided to contact any of colluding nodes, the adversary can only state that an initiator is somewhere in the set of honest nodes D_h . The size of this set is given by

$$|D_h| = |N| (1 - \rho). \quad (7)$$

From the adversary perspective each of the honest nodes is equiprobably an initiator with a probability

$$p_d = \frac{1}{|D_h|} = (|N| (1 - \rho))^{-1}. \quad (8)$$

Then, entropy provided the fact that the file was downloaded from an honest node equals

$$\mathcal{H}_h = -p_d |D_h| \log_2(p_d) = \log_2(1 - \rho). \quad (9)$$

In the scenario when initiator communicated with colluding nodes, the attacker knows with a certainty who is the initiator. He assigns the initiator probability of 1. The situation is similar to the one in pure KAD presented in Section 3. Entropy provided the fact that the file was downloaded from an attacking node, according to the information theory will equal $\mathcal{H}_m = 0$. The adversary points the initiator without any doubt. Finally, based on conditional entropy formula, the entropy of PA-KAD equals

$$\mathcal{H}_{pakad} = (1 - p_x) \mathcal{H}_h + p_x \mathcal{H}_m = (1 - \rho)^{2r+1} \log_2(1 - \rho). \quad (10)$$

Figure 1 shows the entropy of PA-KAD system in the full spectrum of malicious nodes fraction.

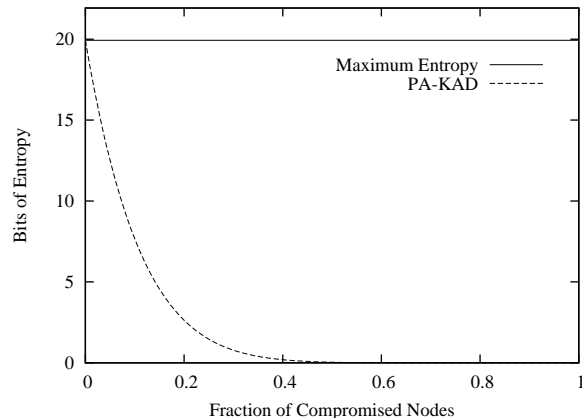


Figure 1. Entropy of PA-KAD Content-Based Routing, $|N| = 10^6$, $x = 1$, $r = 4$.

3.2. Summary of the Results

We found that even taking into consideration significant limitations of an adversary the entropy provided by the DHT structure is decreasing rapidly in function of number of colluding nodes. The diagram shown in Figure 1 was prepared with a value of $x = 1$. Even in this optimistic scenario attacker possessing a fraction $\rho = 0.2$ nodes can obtain almost all information about the initiator.

Figure 2 shows the impact of increasing the number of content sources x on entropy with a fixed $\rho = 0.1$. As a results we observe even faster decrease of entropy. It is important to remember that the characteristics of KAD and consequently PA-KAD encourages users to download from multiple sources to make the download faster and more efficient. Practically, PA-KAD users would loose about 1/3 of their already low privacy level with each content sources contacted. User downloading file from more than five sources in the network with $\rho = 0.1$ does not have any privacy. In this case DHT overlay reveals all information about the initiator.

Finally, it is important to point out, that the model of PA-KAD privacy introduced in Section 3.1 is based on the conditional entropy and describes privacy in long periods of observations. For a user it is crucial to know what is a minimum privacy level the system offers for a single action. In this case we have to take a closer look at minimum entropy, which equals zero in this situation.

4. Conclusions and Future Work

Overlay content-based routing is of crucial importance in the process of Internet virtualization. In content-based routing and localization privacy related addressing information, e.g., meta-data describing content resources and user digital identities, play a leading role. Overlay routing adjusted to specific needs of network services offers wide opportunities for deployment of new service scenarios. Still, we observe that today available overlay solutions are prone to privacy issues. It was shown that the most popular DHT overlay network of today—KAD (the implementation of *Kademlia* [10] protocol) is vulnerable

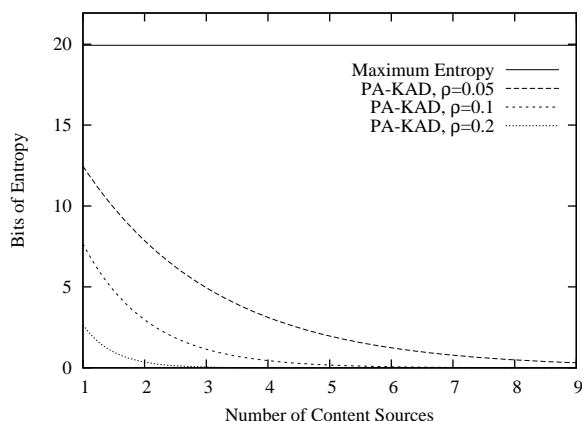


Figure 2. Entropy of PA-KAD Content-Based Routing, $|N| = 10^6$, $r = 4$.

to privacy violation [1–4]. Subsequently, corresponding improvements have been proposed [2, 4, 5]. In the paper we have analyzed the considered privacy-aware routing of KAD using information entropy measurement model and showed that the considered solution still can be a target of unsophisticated attacks. Entropy measures show that the entropy of the system is decreasing rapidly in function of fraction of compromised nodes and content sources contacted during download process. In a very probable situation ($\rho = 0.1$, $x = 5$) optimistic evaluation leads to a conclusion that nearly all information about the initiator have leaked from the system.

At the beginning, KAD network was not intended to provide privacy. Practical opportunities of KAD to operate in the Internet of today brought about an increase interest in its security and privacy issues. Still, much remains to be done. KAD DHT is an expanding overlay network of the world-wide range and a promising environment to deploy scalable content distribution services. Consequently, our future work will include research on integration of KAD DHT with privacy enhancing technologies, including its integration with the peer-to-peer direct and anonymous distribution overlay (P2PRIV) network [14, 15].

References

- [1] Steiner M., En-Najjary T., Biersack E. W.: *Long Term Study of Peer Behavior in the KAD DHT*. IEEE/ACM Transactions on Networking, 2009.
- [2] Wang P., Tyra J., Chan-Tin E., Malchow T., Kune D. F., Hopper N., Kim Y.: *Attacking the Kad network*. SecureComm '08: Proceedings of the 4th international conference on Security and privacy in communication networks, 1–10, 2008.
- [3] Brunner R.: *A performance evaluation of the Kad-protocol*. Msc thesis. University of Mannheim and Institut Eurecom; 2006.
- [4] Steiner M., En-Najjary T., Biersack E.W.: *Exploiting KAD: possible uses and misuses*. SIGCOMM Comput. Commun. Rev., 65–70, 2007.
- [5] Castro M., Druschel P., Ganesh A., Rowstron A., Wallach D. S.: *Secure routing for structured peer-to-peer overlay networks*. SIGOPS Oper. Syst. Rev., 299–314, 2002.
- [6] Karger D., Lehman E., Leighton T., Panigrahy R., Levine M, Lewin D.: *Consistent hashing and random trees: distributed caching protocols for relieving hot spots on the World Wide Web*. STOC '97: Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, 654–663, 1997.
- [7] Ratnasamy S., Francis P., Handley M., Karp R., Schenker S.: *A scalable content-addressable network*. SIGCOMM '01: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications, 161–172, 2001.
- [8] Stoica I., Morris R., Karger D., Kaashoek F.M., Balakrishnan H.: *Chord: A scalable peer-to-peer lookup service for internet applications*. SIGCOMM '01: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications, 149–160, 2001.
- [9] Rowstron A. I. T., Druschel P.: *Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems*. Middleware '01: Proceedings of the IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg, 2001.
- [10] Maymounkov P., Mazieres D.: *Kademlia: A Peer-to-Peer Information System Based on the XOR Metric*. Peer-To-Peer Systems: First International Workshop, IPTPS; 53–65, 2002.
- [11] Rhea S., Geels D., Roscoe T., Kubiawicz J.: *Handling churn in a DHT*. ATEC '04: Proceedings of the annual conference on USENIX Annual Technical Conference, 10, 2004.
- [12] Serjantov A., Danezis G.: *Towards an information theoretic metric for anonymity*. Proceedings of the Privacy Enhancing Workshop, 2002.
- [13] Diaz C., Seys S., Preneel B., Cleassens J.: *Towards measuring anonymity*. Proceedings of the Privacy Enhancing Technologies Workshop, 2002.
- [14] Margasiński I., Pioro M.: *A Concept of an Anonymous Direct P2P Distribution Overlay System*. IEEE 22nd International Conference on Advanced Information Networking and Applications (AINA), 590–597, 2008.
- [15] Margasiński I., Pioro M.: *Low-Latency Parallel Transport in Anonymous Peer-to-Peer Overlays*. IP Operations and Management, Springer LNCS 5275, 127–141, 2008.

ADAM KUBIACZYK
 A.Kubiaczyk@stud.elka.pw.edu.pl
 Nowowiejska 15/19, 00-665 Warszawa

IGOR MARGASIŃSKI
 I.Margasinski@tele.pw.edu.pl
 Nowowiejska 15/19, 00-665 Warszawa