Robust Overlay Routing in Structured, Location Aware Mobile Peer-to-Peer Systems

Christian Gottron(✉), Sonja Bergsträßer, and Ralf Steinmetz

Multimedia Communications Lab, TU Darmstadt, Darmstadt, Germany
{cgottron,bergstr,ralf.steinmetz}@kom.tu-darmstadt.de

Abstract. Mobile Peer-to-Peer architectures provide object and service lookup functionality in absence of a preexisting communication infrastructure. Therefore, those architectures can be harnessed in several application scenarios like disaster relief scenarios where no infrastructure can be assumed and mobility is required. Yet, Mobile Peer-to-Peer architectures inherit the vulnerability to routing attacks from the underlying communication technologies. Further, even though many security mechanisms were developed for traditional Peer-to-Peer architectures, those mechanisms cannot be applied without adaptations to Mobile Peer-to-Peer architectures due to the wireless, mobile underlay network. In this paper, we analyze the vulnerability of the overlays routing algorithm of structured, location aware Mobile Peer-to-Peer architectures against a prominent routing attack. Therefore, we discuss and analyze existing security mechanisms that were developed to ensure a reliable routing process of these architectures. Moreover, we validate and adapt analytic models for the routing algorithm and those previously mentioned security mechanisms.

Keywords: Mobile Peer-to-Peer · Security · Routing

1 Introduction

Mobile Peer-to-Peer (MP2P) networks combine the benefits of Peer-to-Peer (P2P) systems and Mobile Ad hoc networks (MANET). The resulting architecture provides storage and retrieval services without a predefined infrastructure in a decentralized way. Furthermore, MP2P networks are resilient to single node failures. Due to these features, they meet the requirements of application scenarios like disaster relief, development aid, and military operations.

In MP2P networks, data objects as pictures, text, or other media files can be stored in a decentralized way. Structured P2P systems as distributed hash tables (DHTs) and, therefore, structured MP2P systems are based on unique overlay identifiers. These overlay identifiers are used by the routing mechanism of the overlay to perform lookup operations for objects and to initially map objects on nodes. In most cases, the network address of the node that stores and maintains an object, henceforth called the root node, is unknown to the sender of

I. Stojmenovic et al. (Eds.): MOBIQUITOUS 2013, LNICST 131, pp. 155–167, 2014.
DOI: 10.1007/978-3-319-11569-6_13

the lookup request. Therefore, the lookup message is sent to a node that is numerically closer to the root according to the overlay identifier. These intermediate nodes are used to forward the message to a node with an identifier that is numerically closer to the destination, until the lookup request is received by the root.

However, even though multiple MP2P architectures were proposed in the recent years, providing security in terms of robustness (as increasing the availability of stored objects) was mostly neglected. Due to their decentralized architecture, MP2P networks are highly vulnerable to routing attacks. Further, new challenges arose due to the combination of a P2P network with a MANET. Those challenges include a strongly limited bandwidth, an increased packet loss due to the characteristics of the wireless channel and a highly dynamic topology due to node mobility. As a result, existing security mechanisms for traditional P2P architectures that are based on the Internet as underlay cannot be directly applied without adaptations in an MP2P scenario.

In the scope of this paper, we analyze attacks performed by maliciously behaving intermediate nodes that do not forward lookup requests correctly but drop them. Thus, we survey the effects of this *Incorrect Lookup Routing Attack* on the reliability of a location aware MP2P systems lookup mechanism in the following sections. Moreover, we evaluate and compare the most promising, existing security mechanism for DHTs and the Overlay WatchDog, an approach developed for a structured, location aware MP2P architecture [1]. Based on these results we validate and optimize our analytic models for these security mechanisms, which have been proposed in [1].

The rest of the paper is structured as follows, in the next section we introduce related work that has motivated our work. In Sect. 3 we provide background information on MP2P systems. Section 4 focuses on the validation and adoption of the analytic models for the *Incorrect Lookup Routing Attack*. In Sect. 5, we discuss and evaluate security mechanisms that have been developed to increase the robustness of the overlay's lookup algorithm. Moreover, we validate the analytic models of these mechanisms in the light of MP2P systems. In the last section we conclude this paper and discuss future work.

2 Related Work

The *Incorrect Lookup Routing Attack* has initially been introduced by Sit and Morris [2] in the context of DHTs. This attack is based on maliciously behaving intermediate nodes that do not forward received lookup requests but misroute or drop them. As a result, an increased fraction of lookup requests fails. Several security mechanisms were proposed for traditional DHT architectures to increase the robustness against this attack. However, existing mechanisms for DHTs are mostly based on the following three basic concepts.

The first concept harnesses an iterative routing mechanism. During routing, feedback is provided to the source node of the lookup request on each step. Thus, misdirected or dropped lookup messages can be detected by the source node based on this feedback or whenever no feedback is received. This concept

has been initially introduced by Sit and Morris [2]. However, other mechanisms as Myrmic [3] or Sechord [4] are also based on an iterative lookup algorithm.

Another mechanism to increase the network's robustness against the *Incorrect Lookup Routing Attack* is based on introducing redundancy. Here, instead of sending a single lookup message, multiple messages are sent over different routes. Thus, the probability that at least a single lookup request is received by the destination is increased. This redundant routing has been initially proposed by Castro et al. [5]. However, other approaches are also based on a redundant routing algorithm, such as Cyclone [6] or HALO [7].

The third kind of security mechanisms harnesses the reputation of the nodes in the network to detect malicious behavior. Due to these mechanisms, messages are routed via reliable nodes only. Artigas et al. [6] introduced a reputation based system that is combined with a redundant routing algorithm. The Exclusion Routing Protocol [8] or the Higher-Reputated Neighbor Selection [9] are other examples for reputation based security mechanisms.

Also MANET routing mechanisms have to rely on the benign behavior of intermediate nodes. Thus, the underlay routing can also be attacked by malicious intermediate nodes that drop messages. Marti et al. [10] proposed WatchDog, an intrusion detection system (IDS) for MANETs. Messages sent via the wireless channel can be overheard by all nodes within transmission range of the sender of the message. This IDS uses those overheard message to detect malicious behavior. Whenever an intermediate node has to forward a message, WatchDog analyzes overheard messages to detect whether the message was forwarded correctly. If the message has not been forwarded within a specific amount of time, a malicious behavior is assumed. In [1] we proposed an Overlay WatchDog that can also be used to monitor the overlay of an MP2P System.

3 Clustered Pastry Mobile Peer-to-Peer System

MP2P architectures, as considered in this paper, combine a MANET underlay with a P2P overlay. Thus, a completely decentralized storage and retrieval of data objects can be ensured. Yet, multiple challenges are introduced by these architectures due to the characteristics of the underlying systems. This includes a strongly limited bandwidth and an increased fraction of dropped messages due to the wireless channel. The Clustered Pastry MP2P [11] system combines a MANET underlay with a DHT overlay to meet these requirements. The DHT overlay of this MP2P system is based on the Pastry [12] DHT and is used to store and manage objects in a decentralized manner.

We differentiate between overlay lookups and underlay routing. A lookup is initiated whenever an application requests or stores an object from or in the network, respectively. In order to determine the root node of an object, a lookup request is sent. In most cases intermediate nodes are required to forward lookup requests. To deliver this lookup request to the next intermediate overlay node, an underlay route is required. An example for a lookup request is shown in Fig. 1. The black node is the sender of the lookup request. The dark gray nodes are

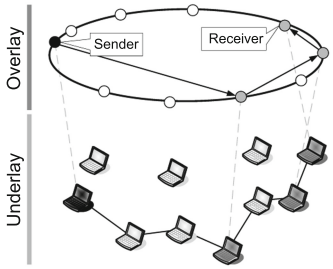


Fig. 1. Schematic representation of a lookup process in an MP2P network

intermediate overlay nodes and the root of the requested object. As shown in the figure, most overlay hops consist of multiple underlay hops. For example, the first overlay hop consists of three underlay hops. Therefore, this first overlay hop requires a complete underlay route (from the black node to the first dark gray node).

In order to combine the underlay with the overlay efficiently, both architectures, the MANET as well as the DHT have to be adapted. We harness location awareness of the mobile nodes in order to optimize the lookup mechanism. For this, the operation area, in which the MP2P network is established, is clustered. Each cluster defines the prefix of the overlay identifier of all nodes that are located in this cluster. As the lookup mechanism of Pastry is based on forwarding the lookup message to a node that is logically closer to destination with each hop, we are able to reduce not only the virtual distance but also the physical distance to the destination with each hop. This results in a reduced overhead caused by routing. Also the average number of hops required for an overlay route is affected by our location-aware architecture. In traditional DHTs, the average number of hops is a logarithmic function of the network size. In our clustered Pastry architecture, the average overlay hops is a function of the number of clusters as shown in Eq. 1 [13].

$$h_{CP} = 1 + log_{(2^b)}(C) * (1 - \frac{1}{2^b}) \tag{1}$$

3.1 Implementation, Assumptions, and Setting

We implemented the previously introduced MP2P architecture for the OMNeT++ [14] simulator. Moreover, we integrated security mechanisms that have been discussed in Sect. 2 into this implementation of the Clustered Pastry MP2P system.

In the underlay we assume bidirectional links. Furthermore, all nodes participate in the MP2P network. The fraction of malicious nodes f is defined by $0 \leq f \leq 0.5$. Malicious nodes may initiate insider attacks. We assume that security mechanisms are in use to harden the underlay against MANET related attacks. Furthermore, we assume that a public key infrastructure is available and that nodes are able to sign sent messages. Using identity based cryptography [15] would be a promising approach as, otherwise, every node has to know

the public keys of each node in the network. Yet, in the interest of simplification we assume pre-shared keys.

We assume a disaster relief scenario where the first responders are equipped with mobile nodes. Due to this fact, a rather low number of nodes participate in our MP2P network compared to traditional static P2P file-sharing scenarios. Therefore, we simulated our scenarios with 100 nodes. Each node was mobile using the random waypoint model. As we assume that all nodes were carried by pedestrians, the node speed was randomly chosen between 0 m/s and 1 m/s. The transmission range was according to WiFi in an open field up to 200 m. Further, all nodes were placed randomly in a field with a total size of 1100 m * 1100 m. The field size was chosen such that a connected network is typically achieved. We used 4 clusters in our scenarios as proposed by [11] for scenarios with 100 nodes.

4 Incorrect Lookup Routing Attack

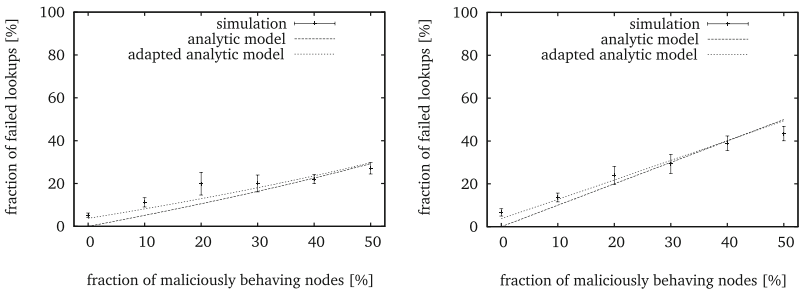
DHTs and, therefore, MP2P architectures that are based on a structured overlay have to rely on the benign behavior of intermediate nodes during a lookup. Those intermediate nodes have to forward received lookup requests correctly toward the destination node. Yet, benign behavior cannot always be assumed. Malicious nodes that perform the *Incorrect Lookup Routing Attack* drop or misroute incoming lookup requests.

According to Castro et al. [5], the impact of the *Incorrect Lookup Routing Attack* on a recursive lookup request depends on the fraction of maliciously behaving nodes (f) and the overall number of hops (h). The resulting model that displays the fraction of successfully completed lookups is shown in Eq. 2.

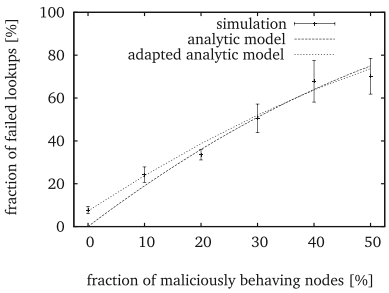
$$\sigma = (1 - f)^{h-1} \tag{2}$$

4.1 Validation of Castro et al.'s Model in MP2P Scenarios

The analytic model proposed by Castro et al. has been developed in the light of traditional static DHTs. Thus, characteristics of MP2P systems have been neglected. Therefore, we simulated Clustered Pastry in scenarios with maliciously behaving intermediate nodes that drop incoming lookup messages. As the model proposed by Castro et al. [5] predicted a strong impact of the number of average overlay hops required for a lookup, scenarios have been simulated with 2, 4 and, 16 clusters. Thus, on average a lookup has to be forwarded 1.5, 2 and 3 times, respectively. As shown in Fig. 2, the outcome of the simulation of these scenarios with a fraction of up to 50 % of maliciously behaving nodes matches quite good with the analytic model. Yet, the analytic prediction fails in scenarios with a small fraction or high fraction of malicious nodes. On one hand, this is the result of neglecting the impact of the lossy wireless channel. Therefore, we proposed an adapted model that considers the fraction of lost messages



(a) Scenario with 2 clusters (b) Scenario with 4 clusters



(c) Scenario with 16 clusters

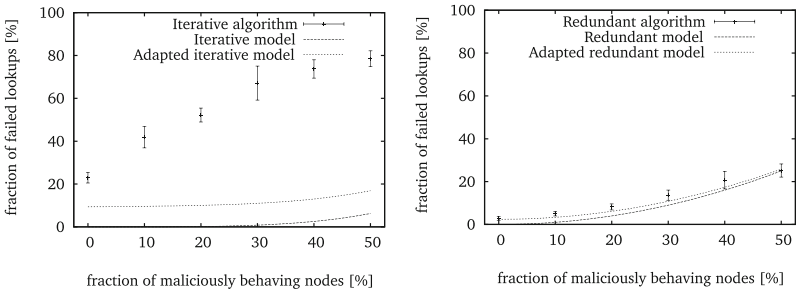
Fig. 2. Impact of the *Incorrect Lookup Routing Attack* on a recursive, unsecured lookup algorithm

due to, e.g., the collisions of sent packets. This can be seen in settings without maliciously behaving nodes. Moreover, Clustered Pastry harnesses a basic replication mechanism in order to ensure the availability of objects even in scenarios with a churn. However, these replicas are not used during a lookup, but only to redistribute whenever a root node leaves a cluster or the network. Yet, whenever lookup is initiated, locally stored objects and replicas are used if available. As a result, we developed an optimized Equation as shown in Eq. 3. The probability p_{loss} represents the fraction of lost lookup messages per overlay hop. Moreover, the number of nodes in the Network (N) and the average number of root nodes of an object (N_{rep}) are used to cover the impact of the basic replication mechanism. As shown in Fig. 2, this adapted analytic model matches the simulation results better than the analytic model proposed by the related work.

$$\sigma_{Optimized} = \sigma * \frac{N - N_{rep}}{N} * p_{loss}^{h} + \frac{N_{rep}}{N} \tag{3}$$

5 Security Mechanisms

In Sect. 2, different security mechanisms were introduced that were developed for DHTs to reduce the impact of the *Incorrect Lookup Routing Attack*. In this section



(a) Iterative algorithm (b) Replication/redundant algorithm

Fig. 3. Comparison of the analytic models with the simulation results of a redundant and iterative routing algorithm

we evaluate the most promising approaches in the context of MP2P systems. This includes the adapted WatchDog approach, the iterative and redundant routing algorithm. Reputation based mechanisms are neglected as we assume that the lossy wireless channel would result in a high fraction of false positives. In [1], analytic models for the iterative, the redundant and the Overlay Watchdog security mechanism have been introduced. However, these models have not been validated by now and consider failed lookups due to malicious behavior only.

5.1 Iterative Routing Algorithm

The iterative routing mechanism ensures reliable lookup services due to the feedback provided to the source of the lookup as discussed in [2]. Yet, the source node is only able to respond to incorrectly routed or dropped lookup requests as long as sufficient addresses of nodes are available, that may be used as next hop intermediate nodes. Therefore, the number of routes per routing table entries (r) limits the efficiency of the iterative security mechanism regarding the fraction of successful lookups ($\sigma_{Iterative}$). Moreover the number of intermediate nodes that are required to forward the lookup request (h) also affects the probability of a successfully completed lookup as shown in Eq. 4 [1].

$$\sigma_{Iterative} = (1 - f^r)^{h-1} \tag{4}$$

To validate this analytic model, we simulated scenarios with 4 clusters, 100 nodes, and maliciously behaving intermediate nodes. The efficiency of the iterative lookup mechanism is evaluated by measuring the fraction of the failed lookups. As shown in Fig. 3(a), the fraction of failed lookups is displayed as a function of the fraction of malicious nodes in the network. The simulation results indicate that the iterative lookup mechanism introduces a high fraction of failed lookups. This is a result of the increased traffic due to the feedback provided to the source of the request. As network congestion is neither considered by the basic nor the adapted models, analytical models can not be used to predict the fraction of failed lookups due to the iterative lookup mechanism.

5.2 Replication and Redundant Routing

As multiple orthogonal routing paths to a single root node are hard to ensure, we harness replicas to deploy a robust routing mechanism. In [13] we proposed multiple replication mechanisms for Clustered Pastry that harness the location awareness to distribute the replicas efficiently. The *Optimized Cyclic Replica Allocation* (OCRA) mechanism has been shown to be the most efficient scheme to distribute replicas in our location aware MP2P system. OCRA allocates replicas to opposing geographical areas (clusters) in the MP2P system. Due to this geographical diversity of the replicas and the location aware structure of the routing table of Clustered Pastry, orthogonal routes to each replica are ensured [13]. Thus, a redundant routing mechanism is enabled.

The resulting fraction of successfully completed lookups is described by Eq. 5 [1] and is a function of the fraction of maliciously behaving nodes (f), the number of parallel requests that have been sent (s), and the average number of required overlay hops per lookup (h). However, the number of sent requests is limited by the number of distributed replicas, in order to ensure orthogonal routing paths. Contrary to sending the requests in parallel as proposed by [5], redundant lookups are only initiated when a lookup fails. Moreover, the replica that is located geographically closest is routed first. Due to this adoptions, the traffic overhead can be reduced.

$$\sigma_{Redundant} = 1 - (1 - (1 - f)^{h-1})^{s} \tag{5}$$

We simulated this redundant routing algorithm in settings with 100 nodes, 4 clusters, and maliciously behaving intermediate nodes. Moreover, a replica is stored for each object that has been stored in the network using the OCRA replication mechanism. A comparison between the outcome of these simulations and the analytical model of Eq. 5 is shown in Fig. 3(b). The analytical model of the fraction of failed lookups is quite similar to the simulation results. Yet, the basic replication mechanism as well as the characteristics of the wireless transmission channel have been neglected. Therefore, we harness Eq. 3 to derive an adapted analytical model. By considering the increased amount of replicas, the adapted analytical model matches the outcomes of the simulations.

5.3 Overlay WatchDog

In [1] we introduced a theoretical approach on how to improve the robustness of the lookup mechanism while keeping the overhead on a reasonable level. This approach is based on an adapted WatchDog mechanism. In the following paragraphs, we discuss this adapted approach.

Mostly, multiple overlay hops are required for a single lookup. For each of those overlay hops an underlay route is required. The traditional WatchDog is only capable of detecting malicious behavior on the network layer and, therefore, can only detect malicious behavior on the underlay route between two overlay nodes. Thus, further information is required in order to detect malicious overlay behavior. In Fig. 4 an example for a lookup is shown. Nodes marked with

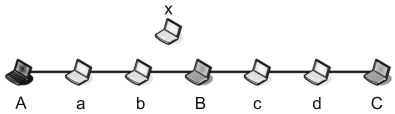


Fig. 4. An example of an MP2P lookup

uppercase letters are involved in the lookup and, therefore, are either overlay intermediate nodes (B), the source (A), or the destination of the lookup (C). All other nodes are either intermediate underlay nodes (a, b, c, d) or nodes that are not involved in the overlay or the underlay routing (x). Two overlay hops are required in order to forward the request from the source node to the destination node. Therefore, two underlay routes are required to perform the lookup. Route one from node A to B and route two from node B to C. The traditional WatchDog mechanism is capable of detecting malicious behavior within any of those underlay routes. Yet, a maliciously behaving node B that performs the *Incorrect Lookup Routing Attack* within the P2P overlay can not be detected. Therefore, the WatchDog mechanism has to be adapted in order to also detect malicious behavior in the overlay.

Whenever a lookup request is received by a node, this node has to determine whether the next hop node is part of the overlay route. Therefore, the intermediate nodes have to be aware of the overlay identifier of the physical neighbors as well as of the destination identifier of the request. Furthermore, basic information about the lookup mechanism is required. The lookup mechanism is well defined in DHTs and, therefore, malicious behavior that violates this algorithm can be detected by an adapted WatchDog with little effort. The overlay identifier of the destination node can be determined by cross-layer information. The destination identifier has to be extracted from the lookup request message. Therefore, overlay messages have to be identified and processed by the underlay. In our example, only two nodes (b and d) have an overlay node as next hop. Both nodes have to compare the node identifier of the next hop node with the destination identifier extracted from the lookup message. As a result, node b identifies node B as intermediate overlay node. Therefore, node B has to forward the message to a node that is logically closer to the destination identifier. As node b is aware of this, messages sent by node B have to be overheard in order to detect a message that includes the lookup request with a next hop overlay node that satisfies the constrains of the overlay routing algorithm. In the example, the next hop overlay node is the destination. Therefore, a benign behavior is assumed by the adapted WatchDog mechanism at node b. Node d on the other hand identifies the next hop node C as destination of the lookup request. A benign behavior is detected when a reply message is sent, to the sender of the request.

Whenever a node detects malicious behavior, the node has to respond in order to increase the network's robustness. The node, that has detected the malicious behavior has to be within transmission range of the malicious node and, therefore, has to be physically close to this node. Due to this, the probability

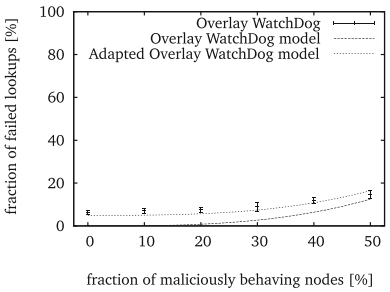


Fig. 5. Robustness provided by the *Overlay WatchDog* to the *Incorrect Lookup Routing Attack*

that the node that has detected the malicious behavior is within the same cluster as the malicious node is high. Due to this, both nodes have similar routing table entries and the node that has detected the malicious behavior is able to provide the same routing functionality as the malicious node should provide. This results in a reduced overhead as no notification message is required.

As shown in Eq. 6 [1], the fraction of successful lookups ($\sigma_{OverlayWatchdog}$) strongly depends on the number of overlay hops. Yet, also the number of physical neighbors (n) and the number of routes per routing table entries (r) affects the impact of maliciously behaving intermediate nodes.

$$\sigma_{OverlayWatchdog} = (\sum_{i=1}^{r}(\sum_{j=1}^{n} f^j * (1-f))^i * (1-f) + (1-f))^{h-1} \qquad (6)$$

Again, we simulated a scenario with 100 nodes and 4 clusters. As shown in Fig. 5, these simulation results of the Overlay WatchDog mechanism match the prediction of the previously discussed analytic model, especially when considering the adaption of Eq. 3.

5.4 Comparison of the Security Mechanisms

By now we have simulated a unsecured recursive routing algorithm and three different security mechanisms in the context with the *Incorrect Lookup Routing Attack*. In Fig. 6 the fraction of failed lookups of these mechanisms is shown as a function of the fraction of malicious nodes in the network. As the recursive lookup mechanism does not provide any robustness against this attack, a high fraction of lookup messages is dropped. The Overlay WatchDog approach and the redundant routing mechanism provide better results compared to the recursive mechanism, while the iterative algorithm performs worse, even in scenarios without maliciously behaving nodes.

The WatchDog mechanism benefits from the structure of the geographically clustered architecture, as mentioned in the previous subsection, and, therefore, introduces a minimal overhead. Whenever a maliciously behaving intermediate

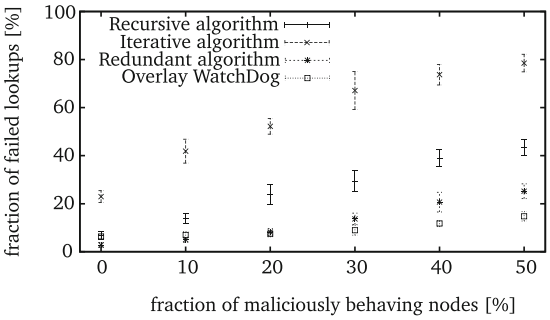


Fig. 6. A comparison between the different security mechanisms

node drops a lookup message, the Overlay Watchdog defines another node in the physical neighborhood that provides the lookup services that have been denied by the malicious node. Thus, only a minor overhead of about 5 % of the overall overlay traffic is introduced by this security mechanism.

The iterative mechanism on the other hand requires feedback at the sender side whenever a lookup message is received by an intermediate node (no matter whether this node behaves maliciously or benignly). Therefore, an increased number of control messages is required. This results in a highly increased fraction of collisions in the wireless channel and, therefore, in the highly degraded reliability of the lookup mechanism, as discussed previously.

The redundant routing mechanisms also introduces replicas. Thus, excellent results are achieved in scenarios with a small fraction of maliciously behaving intermediate nodes. This is the result of the adapted lookup mechanism that always requests the physically closest replica. Therefore, the probability of a dropped lookup message due to the lossy wireless channel is reduced. Yet, due to the distribution of the replicas, the overall traffic is increased by 10 %.

To sum it up, the redundant, replication based mechanism provides the most reliable lookup services in scenario with only a small fraction of maliciously behaving intermediate nodes. Yet, this mechanism introduces the highest traffic overhead. However, the Overlay Watchdog provides the best results in scenario with an increased fraction of malicious nodes. The iterative routing algorithm results in a congested network and, therefore, performs worse than the unsecured recursive routing algorithm.

6 Conclusions and Future Work

Multiple MP2P architectures have been proposed in the recent years. Those architectures benefit from the underlying decentralized architectures. Yet, the robustness of the lookup mechanism against maliciously behaving intermediate nodes during a lookup was neglected by now. Therefore, we discussed the impact of the *Incorrect Lookup Routing Attack* attacks on a structured, location aware MP2P architecture in this paper. As shown, the *Incorrect Lookup Routing Attack*

is able to decrease the efficiency of the lookup algorithm strongly. We have evaluated mechanisms to increase the robustness of the routing mechanism. It has been shown that the Overlay WatchDog and the redundant routing mechanism provide the best results in such a scenario. Moreover, we were able to validate and optimize analytic models that describe the reliability of the unsecured and secured overlay's lookup algorithm.

In future work we plan to improve the Overlay WatchDog mechanism by including a redundant replication mechanism in order to increase the robustness of the overlay's routing algorithm. We assume that such a hybrid mechanism provides even better results. Further we have to reduce the resulting traffic overhead that is introduced by such a hybrid mechanism to avoid network congestion.

References

1. Gottron, C., et al.: A cross-layer approach towards robustness of mobile Peer-to-Peer networks. In: 7th IEEE International Workshop on Wireless and Sensor Networks Security (2011)
2. Sit, E., Morris, R.: Security considerations for Peer-to-Peer distributed hash tables. In: Druschel, P., Kaashoek, M.F., Rowstron, A. (eds.) IPTPS 2002. LNCS, vol. 2429, pp. 261–269. Springer, Heidelberg (2002)
3. Wang, P., et al.: Myrmic: secure and robust DHT routing. Technical report, University of Minnesota (2006)
4. Needels, K., Kwon, M.: Secure routing in Peer-to-Peer distributed hash tables. In: 24th ACM Symposium on Applied Computing (2009)
5. Castro, M., et al.: Secure routing for structured Peer-to-Peer overlay networks. In: Proceedings of 5th Symposium on Operating Systems Design and Implementation (2002)
6. Artigas, M.S., et al.: A novel methodology for constructing secure multipath overlays. IEEE Internet Comput. **9**(6), 50–57 (2005). (IEEE Press, New York)
7. Kapadia, A., Triandopoulos, N.: Halo: high-assurance locate for distributed hash tables. In: 15th Annual Network and Distributed System Security Symposium (2008)
8. Roh, B.-S., Kwon, O.-H., Je Hong, S., Kim, J.: The exclusion of malicious routing peers in structured P2P systems. In: Joseph, S., Despotovic, Z., Moro, G., Bergamaschi, S. (eds.) AP2PC 2006. LNCS (LNAI), vol. 4461, pp. 43–50. Springer, Heidelberg (2008)
9. Sànchez-Artigas, M., García-López, P., Skarmeta, A.F.G.: Secure forwarding in DHTs - is redundancy the key to robustness? In: Luque, E., Margalef, T., Benítez, D. (eds.) Euro-Par 2008. LNCS, vol. 5168, pp. 611–621. Springer, Heidelberg (2008)
10. Marti, S., et al.: Mitigating routing misbehavior in mobile ad hoc networks. In: 6th International Conference on Mobile Computing and Networking (2000)
11. Gottron, C., et al.: A cluster-based locality-aware mobile Peer-to-Peer architecture. In: 8th International Workshop on Mobile Peer-to-Peer Computing (2012)
12. Rowstron, A.I.T., Druschel, P.: Pastry: scalable, decentralized object location and routing for large-scale peer-to-peer systems. In: IFIP/ACM International Conference on Distributed Systems Platforms (2001)
13. Gottron, C.: Security in mobile Peer-to-Peer architectures - introducing mechanisms to increase the robustness of overlay routing algorithms of Mobile-Peer-to-Peer architectures. Dissertation, Technische Universität Darmstadt (2013)

14. Varga, A.: OMNeT++. In: Wehrle, K., Günes, M.M., Gross, J. (eds.) Modeling and Tools for Network Simulation. Springer, Heidelberg (2010)
15. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)