Christian Gottron, André König, Ralf Steinmetz:
A Cross-Layer Approach for Increasing Robustness of Mobile Peer-to-Peer Networks. In:
Proceedings of the Security in NGNs and the Future Internet Workshop, September 2010.

A Cross-Layer Approach for Increasing Robustness of Mobile Peer-to-Peer Networks

Christian Gottron, André König, Ralf Steinmetz

TU Darmstadt, Multimedia Communications Lab - KOM,
Rundeturmstr. 10, 64283 Darmstadt, Germany
{christian.gottron,andre.koenig,ralf.steinmetz}@kom.tu-darmstadt.de
http://kom.tu-darmstadt.de

Abstract. While several Peer-to-Peer and Mobile Ad-hoc network architectures were proposed during the recent years, security is still an open problem. Combining both architectures results in an even more complex security challenge. We introduce a new cross-layer based countermeasure to increase the robustness of mobile Peer-to-Peer networks against denial of service attacks that tamper with the routing algorithms.

Keywords: Mobile Peer-to-Peer, Intrusion Detection, Intrusion Response

1 Introduction and Motivation

Mobile Ad hoc Networks (MANETs) and Peer-to-Peer (P2P) networks share the same concepts of self-organization and decentralization. Both operate without a central, coordinating entity. Combining both paradigms, MANET and P2P, results in a fully decentralized architecture for deployment in e.g. disaster relief scenarios.

Both underlying architectures of Mobile Peer-to-Peer (MP2P) are very challenging regarding network security due to their characteristics. MANETs are mobile wireless networks with permanently changing topology. The nodes are mostly battery driven and have to share the bandwidth with each node in transmission range. This results in strongly limited resources. P2P architectures as Distributed Hashtables (DHTs) on the other hand require a high effort for routing table maintenance and the maintenance of content objects. Since both architectures are completely decentralized and distributed, a node has to rely on the benign behavior during routing in both architectures. Due to this, both are vulnerable against routing attacks like the *Incorrect Lookup Routing* [3] attack. On the other hand, many security mechanisms for MANETs and P2P networks were proposed to increase the robustness of the routing algorithm.

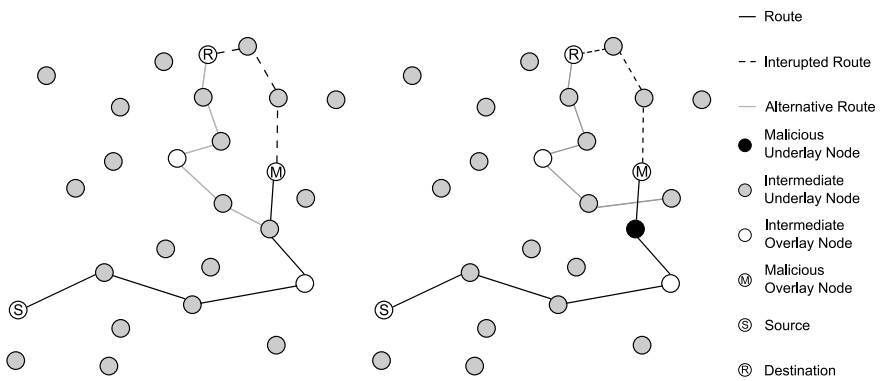
Most P2P countermeasures on routing attacks are based on redundancy. Castro et al. [1] proposed a security mechanism that is based on sending multiple requests for nodes or objects in parallel in order to increase the probability that a request is routed successfully to the destination. Other approaches as the *Iterative Routing* [3] provide feedback to the sender of the request. Those

countermeasures are efficient when sufficient bandwidth is available. Using those countermeasures in a scenario with a MANET underlay may not be efficient due to the bandwidth limitations of the MANET underlay. On the other hand, MANET countermeasures are based on different approaches as cryptography, trust-based systems and observation of neighbor nodes. These are still sufficient in MP2P networks as the overlay does not introduce new implications to underlay mechanisms. Yet, those countermeasures can be extended by providing cross-layer information to the upper layers and, thus, increase the robustness of the overlay, too. Therefore, we propose a novel cross-layer countermeasure which we explain at the example of the *Incorrect Lookup Routing* as an attack that has a high impact on network reliability. Our countermeasure is assumed to require less resources than traditional P2P security mechanisms.

2 Cross-Layer Approach

For coping with the challenging conditions in MP2P systems with respect to security, we can take an advantage of the wireless data transmission, as nodes are able to observe the behavior of other nodes in transmission range. The Watchdog [2] countermeasure is based on those observations. This security mechanism was proposed to use the promiscuous mode of wireless cards in order to overhear sent messages by neighbors. Watchdog is able to detect whenever a node in transmission range receives but does not forward a message and estimates the trustworthiness of the nodes in transmission range based on this information. Though, Watchdog considers underlay behavior only and is unaware of the application and the upper layer protocols. We are able to benefit from those observations in the overlay as well by providing cross-layer information to the upper layers.

As mentioned in the previous section, we assume that the robustness of the underlay can still be maintained by the MANET countermeasures. In order to provide robustness for the MP2P overlay, we propose a security mechanism similar to Watchdog. By observing request messages sent and received by nodes in transmission range, we should be able to identify malicious nodes. Detection of malicious behavior is based on the unique identifier of each overlay node and the recursive behavior of the DHT routing algorithm. On one hand, we are able to identify dropped requests by malicious nodes by comparing the identifier of the malicious node with the destination of the request. On the other hand, we can detect an incorrect request by comparing the identifier of the malicious node with the identifier of the proposed next overlay node. Most DHT routing algorithms provide strict rules on how the next hop overlay node has to be selected. Whenever a next hop overlay node does not comply to these rules, a malicious behavior can be assumed. To detect malicious nodes, we require on one hand information provided by the lower layers such as the overheard messages themselves and, further, we require the knowledge on the overlay routing algorithm and the overlay identifiers. Therefore, a cross-layer communication is required. To respond to an attack identified, a new routing can be initiated by the node



(a) Single malicious node (b) Colluding malicious nodes

Fig. 1. Examples for attacking a mobile P2P network and how the cross-layer approach reacts

that has detected this attack, or a reply is sent to the previous overlay node, that had forwarded the message to the malicious node, in order to redirect the request.

We have to differentiate two scenarios in order to define which node has to respond, when a malicious behavior is detected. We distinguish in our scenarios whether or not malicious nodes collude in order to increase the impact of the attack and to delude countermeasures. In scenarios without colluding malicious nodes, we assume that the malicious behavior of a node is correctly detected by the node that forwards the request to the malicious node. This intermediate underlay node is therefore able to respond to the attack as shown in Figure 1(a). However, when we assume colluding malicious nodes, also a benign behavior of the previous hop underlay node can not be assumed. Therefore, all nodes in transmission range of both nodes, the malicious overlay node and the malicious underlay node, have to detect the malicious behavior. Though, those nodes have to coordinate themselves as only a single node has to respond to the attack (as shown in Figure 1(b)) in order to avoid an increased overhead.

By harnessing cross-layer information this way, we are able to improve the robustness of the overlay routing algorithm. Further, we assume that the overhead generated by the proposed countermeasure is low compared to *traditional* P2P security mechanisms. A detailed validation in a testbed as well as by means of simulation and analytical models is part of our future work.

References

1. M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. Wallach. Secure routing for structured peer-to-peer overlay networks. In *Proc. of the OSDI '02*, 2002.
2. S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proc. of the MobiCom '00*, 2000.
3. E. Sit and R. Morris. Security considerations for peer-to-peer distributed hash tables. In *Proc of the IPTPS '01*, 2002.