Validierung von Antworten auf Objektanfragen in Mobilen Peer-to-Peer Architekturen

Christian Gottron, André König, Ralf Steinmetz:
Validierung von Antworten auf Objektanfragen in Mobilen Peer-to-Peer Architekturen. In: 6. Essener Workshop "Neue Herausforderungen in der Netzsicherheit", March 2012.

Mobile Peer-to-Peer-Architekturen als eine Kombination von einem Mobile Ad hoc Netz mit einem strukturierten Peer-to-Peer-Netz ermöglichen ein komplett dezentrales und mobiles Speichern sowie Auffinden von Objekten. Bösartige Knoten können sich die vollständige Dezentralität allerdings auch zunutze machen, um die Verfügbarkeit solcher dezentral gespeicherten Objekte anzugreifen. Ein Angreifer kann so inkorrekte Antwortnachrichten generieren wenn er eine Anfrage nach einem gespeicherten Objekt erhält, selbst wenn er nicht der eigentliche Zielknoten für diese Anfrage ist. Existierende Ansätze zur Reaktion auf solche Angriffe für traditionelle Peer-to-Peer-Netze basieren hier zumeist auf Annahmen, die im Kontext einer Mobilen Peer-to-Peer-Architektur, wie sie hier betrachtet wird, nicht zulässig sind. In diesem Beitrag wird ein neuer Ansatz vorgestellt der für die beschriebenen Szenarien angepasst wurde.

I. Motivation und Ziele

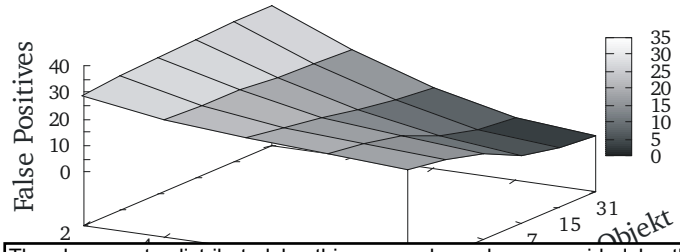
Distributed Hashtables (DHTs) sind strukturierte Peer-to-Peer-Architekturen. Sie ermöglichen ein effizientes Speichern, Verwalten und Abrufen von Objekten. Kombiniert man eine solche DHT mit einem Mobilen Ad hoc Netz (MANET) als Underlay, so erhält man eine dezentrale und mobile Architektur. Diese kann in Szenarien eingesetzt werden, in denen die Mobilität der Knoten als eine Grundvoraussetzung angesehen wird, und in denen nicht von einer funktionierenden Infrastruktur ausgegangen werden kann. Beispiele sind Katastrophenschutz, Entwicklungshilfe oder militärische Szenarien.

Die Effizienz der DHTs lässt sich durch ihre Strukturierung erklären. Die Routingtabellen sind so aufgebaut, dass jeder Knoten nur Routen zu einem kleinen Teil der Knoten des Netzes speichert. Als Folge dessen sind der Verwaltungsaufwand sowie die Kosten für die Aktualisierung der Routingtabellen gering. Da jedoch in den meisten Fällen ein Knoten die Route zu seinem Ziel nicht kennt, muss er sich auf meist mehrere zwischenliegende Knoten verlassen, die seine Anfragen für den Abruf gespeicherter Objekte weiterleiten. Durch die Strukturierung der Routingtabelle wird allerdings die Anzahl der benötigten zwischenliegenden Knoten minimiert.

Diese zwischenliegenden Knoten können verwendet werden um einen Angriff auf eine Anfrage durchzuführen. So kann sich ein Knoten als Zielknoten ausgeben und eine Antwortnachricht fälschen. Im Kontext von DHTs wurde hier von Castro et al. [1] ein möglicher Sicherheitsmechanismus vorgestellt. Dieser trifft allerdings Annahmen die in einer Mobilen Peer-to-Peer-(MP2P) Architektur nicht gültig sind. Entsprechend wird im Folgenden der Ansatz von Castro et al. im Rahmen einer MP2P Anwendung betrachtet. Weiterhin wird ein neuer Ansatz vorgestellt, der für MP2P Architekturen entwickelt wurde.

II. Annahmen und Hintergrundinformationen

Jedem Knoten, der einer DHT beitritt, wird eine virtuelle Identität (ID) zugewiesen. Diese bestimmt, wie der Knoten in der DHT adressiert wird. Aufgrund dieser IDs entstehen virtuelle Nachbarschaften zwischen Knoten, deren ID die größte Ähnlichkeit aufweisen. Dies entspricht bei numerischen IDs den Knoten, deren Differenz der IDs niedrig ist. Weiterhin erhält ebenfalls jedes gespeicherte Objekt eine ID. In den meisten Fällen wird ein Objekt von jenem Knoten verwaltet, dessen ID die geringste Differenz zur ID des Objektes aufweist.



Die Effizienz, mit der ein Fehlverhalten detektiert werden kann, wird mit Hilfe zweier Metriken ermittelt. Zum einen werden durch die *False Positives* jene Knoten bezeichnet, die als bösartig identifiziert wurden, obwohl sie sich gutartig verhalten. Zum anderen geben die *True Positives* den Anteil der korrekt erkannten Angriffe an.

III. Routing Failure Test

Der von Castro et al. vorgestellte *Routing Failure Test* wird verwendet um fehlerhafte Antwortnachrichten zu identifizieren. Castro trifft dafür die folgenden Annahmen: (I) Die IDs der Knoten werden zufällig verteilt. (II) Jeder Knoten speichert die Adressen seiner L virtuellen Nachbarn. (III) Es werden zu jedem Objekt jeweils Kopien auf den virtuellen Nachbarn des für das Objekt verantwortlichen Knotens gespeichert. Dadurch werden R Versionen von jedem Objekt generiert. (IV) Die Anzahl der Knoten im Netz wird als hoch angenommen. Evaluiert wurde Castro‘s Ansatz mit 100.000 Knoten und 32 virtuellen Nachbarn und Versionen je Objekt ($R=L=32$).

Aufgrund von Annahme (III) können inkorrekte Antwortnachrichten von Knoten, die alleine agieren, leicht identifiziert werden. Hier müssen lediglich die anderen Knoten kontaktiert werden, deren Adresse in der Antwortnachricht enthalten ist. Diese liefern entweder eine Kopie des Objektes oder geben an, dass diese nicht für das Objekt verantwortlich sind. In beiden Fällen kann Fehlverhalten detektiert werden. Sollten jedoch bösartige Knoten zusammenarbeiten, so kann ein Angreifer in der Antwortnachricht Adressen von anderen bösartigen Knoten verwenden. So würde jeder der vermeintlichen Zielknoten das gleiche fehlerhafte Objekt liefern. Hier ermittelt Castro‘s Ansatz die Knotendichte in seiner virtuellen Nachbarschaft und vergleicht diese mit der Dichte der Zielknoten. Da die Knoten im Netz gleichverteilt sind, müsste die durchschnittliche virtuelle Distanz zwischen den Knoten-Gruppen ähnlich sein. Da sich jedoch nur eine begrenzte Anzahl der Knoten im Netz bösartig verhält, ist deren Dichte wesentlich geringer. Entsprechend lässt sich so mit einer ausreichend hohen Wahrscheinlichkeit ermitteln, ob die Menge der Antwortknoten korrekt ist.

Castro‘s Ansätze sind für Internet basierte Peer-to-Peer-P2P Architekturen basieren

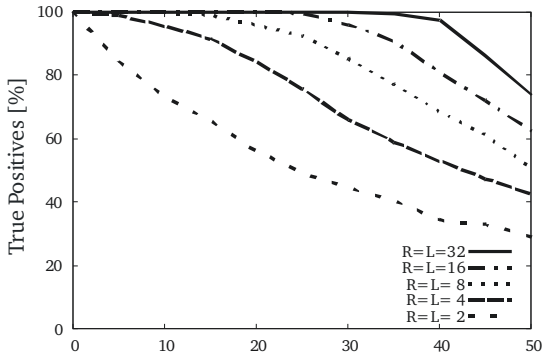


Abbildung 2: True Positives von Castro's Ansatz

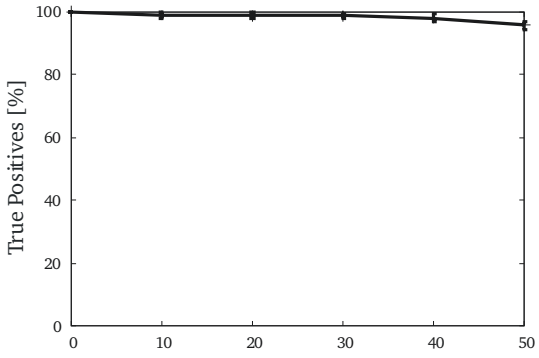


Abbildung 4: True Positives des Cross Layer Ansatzes

darauf, dass IDs nicht zufällig, sondern als Funktion der physikalischen Lokation des Peers generiert werden (z.B. [2], [3]). (II) Die meisten Ansätze verwenden zwar virtuelle Nachbarn, meist wird die Anzahl jedoch massiv reduziert im Vergleich zu Internet-basierten Architekturen ($L<32$). (III) Da das Erstellen oder Modifizieren von Objekten Datenverkehr erzeugt, kann in einem mobilen Szenario aufgrund der limitierten Bandbreite nur eine stark begrenzte Anzahl an Kopien von Objekten erstellt werden ($R<<32$). (IV) Zuletzt ist die Anzahl der Knoten wesentlich niedriger in den für MP2P-Systeme relevanten Szenarien.

Berücksichtigt man dies, sinkt die Effizienz des *Routing Failure Tests* massiv. In Abbildung 1 ist die Rate der False Positives zu sehen in einem Szenario mit 100 Knoten und einer variablen Anzahl von virtuellen Nachbarn (L) und Versionen eines Objektes (R). Hier sieht man, dass die *False Positives* massiv ansteigen wenn entweder die Anzahl der virtuellen Nachbarn oder die Anzahl der Versionen eines Objektes reduziert werden. Auch die *True Positives* sind von diesen beiden Parametern abhängig. Abbildung 2 zeigt, dass die Zuverlässigkeit stark von der Anzahl der Kopien der Objekte und der virtuellen Nachbarn abhängig ist.

IV. Cross Layer-Ansatz

Einige MP2P-Architekturen basieren auf einer geografischen Verteilung der IDs. Dies bewirkt ein effizienteres Routen und somit eine optimierte Nutzung der Ressourcen. Auf Basis dieses Szenarios wird in diesem Beitrag ein effizienter Mechanismus zur Erkennung inkorrekter Antwortnachrichten vorgestellt.

Da MP2P-Architekturen auf drahtloser Kommunikation aufbauen, kann eine Nachricht nicht nur von dem entsprechenden Zielknoten mitgehört werden, sondern auch von jedem anderen Knoten in Übertragungsreichweite. Wenn ein Knoten also eine Nachricht sendet, kann diese auch von seinen physikalischen Nachbarn empfangen werden. Wenn diese nun auch die virtuellen Nachbarn des antwortenden Knotens sind, so verfügen diese über eine ähnliche Routing-Tabelle. Mit Hilfe derer kann leicht überprüft werden, ob der antwortende Knoten wirklich jener Knoten ist, der sich virtuell am nähesten zu dem angefragten Knoten befindet. Entsprechend kann einer der virtuellen Nachbarn den anfragenden Knoten über das Fehlverhalten informieren und dabei auch gleich Informationen bereitstellen, welcher Knoten näher am Zielobjekt liegt.

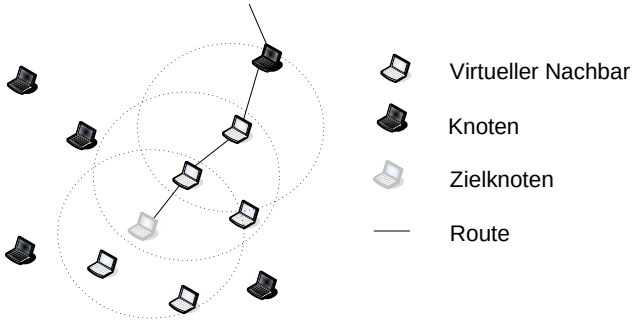


Abbildung 3: Beispiel für den Cross Layer-Ansatz

Ein Beispiel hierzu ist in Abbildung 3 zu sehen. Der hellgraue Knoten ist der Zielknoten bzw. der Knoten der sich als Zielknoten ausgibt. Die dunkelgrauen Knoten stellen die virtuellen Nachbarn da, die sich entweder in Empfangsreichweite befinden, oder direkt auf der Route zum anfragenden Knoten liegen. Jeder dieser dunkelgrauen Knoten kann ein Fehlverhalten identifizieren. Solange zumindest einer dieser Knoten sich gutartig verhält, kann die Antwort validiert werden.

Dieser Mechanismus wurde simulativ evaluiert. Hier wurde eine geobasierte MP2P-Architektur verwendet wie sie in [3] vorgestellt wurde. Unabhängig von der Anzahl der bösartigen Knoten lagen die *False Positives* permanent unter 0,5%. Dies ist vergleichbar mit den besten Ergebnissen von Castro's Ansatz, jedoch ohne dabei auf Kopien von Objekten zurückgreifen zu müssen. Weiterhin, wie in Abbildung 4 zu sehen, kann eine *True Positive* Rate erzielt werden, die bei weitem nicht so stark von der prozentualen Anzahl der bösartigen Knoten abhängig ist. Selbst in Szenarien mit einem hohen prozentualen Anzahl von bösartigen Knoten liegt diese bei etwa 95%. Vor allem im Vergleich mit Szenarien mit einer niedrigen Anzahl von Objektkopien können hier wesentlich bessere Ergebnisse erzielt werden.

V. Zusammenfassung

In diesem Beitrag konnte gezeigt werden, dass Castro's Ansatz zum Validieren von Objektanfragen in einem MP2P Szenario nicht effizient ist, da viele von Castro's Annahmen hier nicht mehr zutreffen. Vor allem in Kombination mit Architekturen, die Knoten-IDs anhand der physikalischen Lokation der Knoten definieren, kann dieser Ansatz nicht verwendet werden. Für diese Szenarien wurde ein neuer Ansatz vorgestellt. Dieser nutzt die Einheit der virtuellen und physikalischen Nachbarschaften um Fehlverhalten effizient zu detektieren. Dabei erhält der anfragende Knoten nicht nur Informationen über das Fehlverhalten eines Knotens, sondern zusätzlich einen Vorschlag für einen weiterführenden Routing-Schritt.

VI. Literaturverzeichnis

[1] M. Castro, P. Druschel, A. Ganesh und A. Rowstron and D. Wallach: "Secure routing for structured peer-to-peer overlay networks"; OSDI , 2002

[2] T. Zahn und J. Schiller: "MADPastry: A DHT Substrate for Practicably Sized MANETs"; ASWN, 2005

[3] Christian Gottron, André König und Ralf Steinmetz: "A Cluster-Based Locality-Aware Mobile Peer-to-Peer Architecture". MP2P, 2012.