Accepted for Kommunikation in Verteilten Systemen (KiVS) 2007
26. Februar - 2. März 2007 in Bern, Schweiz

Verhaltensbeobachtung und -bewertung zur Vertrauensbildung in offenen Ad-hoc-Netzen

Daniel Kraft[1] und Günter Schäfer[2]

[1] Institut für Telematik, Universität Karlsruhe
[2] Fachgebiet Telematik/Rechnernetze, Technische Universität Ilmenau

Zusammenfassung. Die Beobachtung des Verhaltens anderer Teilnehmer anhand mitgehörten Netzverkehrs ist in offenen Ad-hoc-Netzen die einzige ohne Vorwissen anwendbare Methode, durch welche Einschätzungen über die Kooperationsbereitschaft und Vertrauenswürdigkeit Anderer gewonnen werden können. Dieser Beitrag beschreibt die Problematik der Verhaltensbeobachtung und entwickelt auf der Basis einer grundlegenden Bedrohungsanalyse ein konkretes Verfahren für die zuverlässige Bewertung des Weiterleitungsverhaltens teilnehmender Knoten in Ad-hoc-Netzwerken. Anhand von Simulationsergebnissen wird nachgewiesen, dass mit dem Verfahren eine ausreichende Anzahl an Bewertungsereignissen gewonnen werden kann.

1 Einleitung

Vertrauen in andere Teilnehmer ist eine grundlegende Voraussetzung für die Funktionsfähigkeit jedes verteilten Systems, in dem Dienstleistungen erbracht und in Anspruch genommen werden. Bei existierenden verteilten Systemen wird häufig einfach generell in korrektes Verhalten aller Teilnehmer vertraut – eine Annahme, die bei großen offenen Systemen ggf. nicht mehr gerechtfertigt ist, wenn die Nutzer die Systeme lediglich als Werkzeug für die Verfolgung ihrer eigentlichen Interessen sehen.

In offenen Ad-hoc-Netzen gibt es im Wesentlichen zwei Möglichkeiten, Vertrauen in andere Teilnehmer zu gewinnen: Entweder muss existierendes Vertrauen aus der realen Welt in die virtuelle des Netzwerks übertragen werden (was neben der Existenz solchen Vertrauens eine sichere Verknüpfung zwischen realen Benutzern und Identitäten im Netz agierender Rechner voraussetzt und aktive Mitarbeit des Benutzers erfordert) oder neues Vertrauen muss innerhalb der Netzwerkwelt aufgebaut werden, indem das Verhalten der anderen Knoten automatisch beobachtet und bewertet wird und somit Erfahrungen gesammelt werden, ähnlich wie dies Menschen beim Aufbau sozialer Beziehungen und Netzwerke tun. Benachbarte Netzknoten können hierbei dank der Rundrufcharakteristik drahtloser Übertragungstechniken anhand mitgehörten Netzverkehrs beobachtet werden. Da die Möglichkeiten automatischer Beobachtung in der virtuellen Welt gegenüber der realen damit allerdings recht eingeschränkt sind (im Allgemeinen kann nur die Einhaltung von Protokollen und die Reaktion auf Dienstleistungsanforderungen automatisch beurteilt werden), ist es besonders wichtig, möglichst viel der zur Verfügung stehenden Information zu nutzen. Insbesondere sollte sowohl *beobachtetes korrektes Verhalten* als auch *beobachtetes inkorrektes Verhalten* explizit registriert

werden und in die ermittelte Einschätzung einfließen: Korrektes Verhalten erzeugt Vertrauen beim Beobachter, inkorrektes Misstrauen. Liegen gar keine Beobachtungen vor, so ist weder Vertrauen noch Misstrauen angebracht. Die verwendete Vertrauensmetrik muss geeignet sein, dies auszudrücken.

Die Beobachtung des Verhaltens anderer Knoten in Bezug auf die Erbringung der Paketweiterleitung in der Netzwerkschicht erscheint aufgrund der häufigen Nutzung dieses Dienstes als besonders geeignet für die Einschätzung der Kooperationsbereitschaft anderer Knoten. Die Verhaltensbeobachtung enthält hierbei jedoch grundsätzlich gewisse Unsicherheiten. Beispielsweise kann sich der zur Weiterleitung verpflichtete Knoten zwischen Empfang und Weiterleitung eines Pakets aus der Reichweite des Beobachters bewegen oder auf andere Weise von ihm abgeschirmt werden, so dass der Beobachter die Weiterleitung nicht beobachten kann und fälschlich annimmt, dass sie unterlassen wurde. Sind die Bedingungen für eine richtige Bewertung aber im Großteil der Fälle erfüllt und führen einzelne Beobachtungen immer nur zu graduellen Anpassungen von Einschätzungen, können wenige „falsche“ Beobachtungen i. d. R. ohne wesentliche Verfälschungen der Gesamteinschätzungen verkraftet werden.

Der vorliegende Beitrag stellt ein Verfahren zur Beobachtung und Bewertung des Weiterleitungsverhaltens in Ad-hoc-Netzen vor, das nicht von einem bestimmten Routing-Protokoll abhängig ist und alle beobachtbaren Übertragungen einbezieht. Der folgende Abschnitt beschreibt zunächst verwandte Ansätze. Abschnitt 3 beschreibt unseren Ansatz, dessen wesentliche Neuerungen anhand einer systematischen Bedrohungsanalyse begründet werden. Die Leistungsfähigkeit des Verfahrens wird in Abschnitt 4 in einer Simulationsstudie untersucht. Abschnitt 5 fasst die Ergebnisse des Beitrags kurz zusammen und gibt einen Ausblick auf weiterführende Arbeiten.

2 Stand der Technik

Marti, Giuli, Lai und Baker beschreiben [MGLM00] den ersten Ansatz zur Beobachtung des Weiterleitungsverhaltens in Ad-hoc-Netzen, der speziell für das reaktive Routing-Verfahren Dynamic Source Routing (DSR)entworfen wurde. Dabei bewahrt eine „Watchdog“ genannte Komponente eine Kopie eines jeden in der Weiterleitungsphase selbst gesendeten Pakets auf, das noch der Weiterleitung bedarf, und startet mit der Aussendung einen Zeitgeber. Wird in der Folge beobachtet, wie das Paket weitergeleitet wird, so werden Kopie und Zeitgeber gelöscht. Läuft der Zeitgeber aber ab, ohne dass die Weiterleitung beobachtet wurde, so erfolgt eine Meldung über unterlassene Weiterleitung an die Quelle des Pakets; sie führt zum Ausschluss von Wegen über den unzuverlässigen Knoten bei der Wegewahl. In der Routing-Phase selbst erfolgt keine Überwachung. Durch die Beschränkung auf ein Source-Routing-Protokoll kann der Beobachter leicht erkennen, ob und wohin ein Paket noch weitergeleitet werden muss.

Dieser Ansatz wurde häufig in ähnlicher Form aufgegriffen. Beim CONFIDANT-Ansatz [BuBo02] etwa wird ein ähnliches Beobachtungsverfahren verwendet, um negative Bewertungen zu ermitteln, die bei gehäuftem Auftreten zum Ausschluss des Verursachers aus dem Netz führen. In einer Weiterentwicklung [BuBo04,BuTLB04] wird auch korrektes Verhalten registriert und aus positiven und negativen Beobachtungen eine Einschätzung ermittelt.

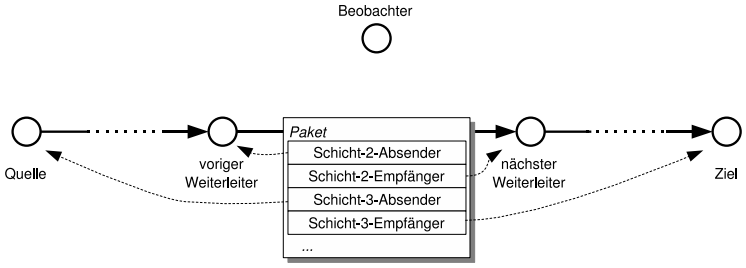

Abb. 1. An der Übertragung eines Pakets beteiligte Knoten und Adressangaben in Paketen

Auch bei SORI [HeWK04] und OCEAN [BaBa03] gibt es jeweils eine Watchdog-Komponente, welche positive und negative Beobachtungen bezüglich der selbst versendeten Pakete erfassen. Pakete, die von anderen Teilnehmern versendet worden sind, werden aber auch hier nicht beobachtet. In [BaBa03] wird dies dadurch begründet, dass solche Beobachtungen zu anfällig gegen Angriffe seien.

3 Beobachtung des Weiterleitungsverhaltens

Zur Klärung der Begriffe in den weiteren Ausführungen sind in Abbildung 1 einige an der Übertragung eines Pakets beteiligte Knoten dargestellt und aus der Sicht eines Beobachters bezeichnet. Ein allgemeiner Grundsatz für die Verfahren zur Beobachtung und Bewertung ist, dass durch sie möglichst wenig zusätzlicher Energieaufwand und keine zusätzliche Netzbelastung entstehen sollten.

3.1 Grundidee

Jeder Knoten hält für jeden seiner Nachbarn ein Paar von Zählern, mit denen er Beobachtungen korrekten bzw. unkorrekten Weiterleitungsverhaltens registriert. Aus den Zählerständen kann jederzeit eine Vertrauensmaßzahl berechnet werden, die eine Einschätzung des Weiterleitungsverhaltens des jeweiligen Nachbarn darstellt.

Beobachtet ein Knoten, wie ein anderer Knoten ein Paket weiterleitet, erhöht er den diesem weiterleitenden Knoten zugeordneten Zähler für positive Beobachtungen um eins. Um auch erfassen zu können, dass ein Knoten die Weiterleitung verweigert, wird außerdem für jedes beobachtete oder selbst ausgesandte Paket, das noch von einem Nachbarn weitergeleitet werden muss, ein Eintrag in einer Liste derzeit beobachteter Pakete angelegt. Zu jedem solchen Eintrag wird ein Zeitgeber gestartet. Wird während der Laufzeit des Zeitgebers die erwartete Weiterleitung beobachtet, so werden der Zeitgeber und der zugehörige Eintrag gelöscht. Läuft der Zeitgeber aber ab, ohne dass die erwartete Weiterleitung beobachtet werden konnte, so wird dem säumigen Weiterleiter eine negative Beobachtung angerechnet.

Führen die einzelnen Knoten eine Zugangskontrolle in dem Sinne durch, dass Pakete nur dann weitergeleitet werden, wenn sie von einem vertrauenswürdigen Knoten stammen [Kraf06], so ist für Beobachter zunächst nicht vorhersehbar oder erkennbar,

wie die aufgrund lokaler Information getroffenen Zugangsentscheidungen ausfallen. In Fällen unterlassener Weiterleitung kann somit nicht entschieden werden, ob die Weiterleitung berechtigterweise aufgrund einer Zugangsentscheidung oder unberechtigterweise unterlassen wurde. Daher muss jeder Knoten, der eine negative Zugangsentscheidung trifft, dies durch Aussenden einer entsprechenden Fehlermeldung bekanntgeben. Wenn eine solche Fehlermeldung beim Beobachter eintrifft, wird das zugehörige Paket aus der Liste beobachteter Pakete gelöscht.

Als Teilnehmerkennungen, denen positive und negative Beobachtungen zugeordnet werden, dienen die öffentlichen Teile asymmetrischer Schlüsselpaare [Kraf06]. Ein Teilnehmer kann und darf sich mehrere solcher Kennungen zulegen. Aus dem Vorliegen unterschiedlicher Kennungen etwa als Absender zweier Nachrichten kann somit nicht geschlossenen werden, dass diese von unterschiedlichen Teilnehmern stammen. Andererseits kann aber ausschließlich der tatsächliche Inhaber einer Teilnehmerkennung Signaturen mit dem privaten Teil des asymmetrischen Schlüsselpaars erzeugen, die dann mit Hilfe des öffentlichen Teils verifizierbar sind. Fremde Teilnehmerkennungen können somit nicht für eigene Zwecke missbraucht werden. Die Teilnehmerkennungen seiner Nachbarn sind jedem Knoten stets bekannt, da jeweils beim ersten Kontakt mit neuen Nachbarn ein Schlüsselaustausch durchgeführt wird, bei welchem jede Seite auch den Besitz des privaten Schlüssels nachweist (Challenge-Response-Verfahren).

Bei dem beschriebenen Beobachtungs- und Bewertungsverfahren werden an zwei Stellen Informationen über die Zuordnung zwischen Schicht-2- und Schicht-3-Adressen benötigt, die nicht aus dem beobachteten Paket entnommen werden können und daher durch eine entsprechende Abbildungsfunktion (bzw. Routing-Information) ermittelt werden müssen. Gemeint sind die beiden folgenden Entscheidungen:

- Wenn ein Sendevorgang beobachtet wird, muss zunächst entschieden werden, ob es sich um einen Weiterleitungsvorgang handelt, oder ob die beobachtete Nachricht von ihrem ursprünglichen Erzeuger (also ihrer Quelle) ausgesandt wurde.
- Weiterhin muss ein Beobachter erkennen, ob ein beobachtetes Paket nochmals weitergeleitet werden muss, oder ob es am Ziel angekommen ist.

3.2 Bedrohungsanalyse

Angriffsziele und -motivation Bei dem Versuch, die Resultate des Verfahrens zur Verhaltensbeobachtung und -bewertung zu verfälschen, kommen für Angreifer folgende Ziele in Frage:

1. Beschaffung positiver Bewertungen für den Angreifer bzw. für „Komplizen“, wobei
   (a) der für reguläre positive Bewertung zu erbringende Aufwand (Dienstleistung an der Allgemeinheit) entfällt oder
   (b) die sich durch mangelnde Nachfrage nach zu erbringenden Dienstleistungen ergebende Einschränkung (etwa dadurch, dass keine Pakete zur Weiterleitung zur Verfügung stehen) wegfällt.

   Eine Art natürlicher Beschränkung für die Beschaffung ungerechtfertigter positiver Bewertungen der erstgenannten Art besteht dadurch, dass immer nur bei Beobachtung eines tatsächlich gesendeten Pakets eine positive Bewertung erfolgt. Dass positive Bewertungen völlig ohne Aufwand (d. h. ohne Energieverbrauch durch Senden) massenhaft erzeugt werden können, ist damit schon ausgeschlossen. Es kann

also höchstens erreicht werden, dass ein normalerweise nicht positiv bewerteter Sendevorgang (wie die Erzeugung eines eigenen Pakets) als Dienstleistung an der Allgemeinheit (z. B. Weiterleitung) erscheint.
2. Verhindern negativer Bewertung des Angreifers oder eines „Komplizen“ (darf nicht mehr Aufwand erfordern, als durch unterlassene Weiterleitung eingespart wird).
3. Erzeugung negativer Bewertungen oder Verhindern positiver Bewertung für andere Knoten, entweder
   (a) um die Verfügbarkeit des Netzes zu beeinträchtigen oder
   (b) um eine eigene schlechte Bewertung durch andere Knoten zu relativieren.

   Angriffe gegen die Verfügbarkeit sind in Ad-hoc-Netzen schwierig zu bekämpfen, weil mit genügend hohem Aufwand ohnehin jede Kommunikation zumindest in der Nachbarschaft des Angreifers durch Störsignale unterbunden werden kann. Ob der Angriffsversuch (b) Erfolg haben kann, hängt vom Zugangskontrollverfahren ab.

Die unter 1. und 2. genannten Angriffsmotivationen dürften die größte Gruppe potentiell interessierter Angreifer anziehen, da Möglichkeiten, sich selbst Vorteile zu verschaffen, ohne dabei durch allzu offensichtliche Benachteiligung anderer auffällig zu werden, erfahrungsgemäß gerne genutzt werden.

Angriffsanalyse Die prinzipiellen Möglichkeiten eines Angreifers umfassen die *Unterschlagung, Zerstörung* oder *Verfälschung bewertungsrelevanter Information* in den Nachrichten anderer, die *Wiedereinspielung fremder Nachrichten* sowie die *Angabe falscher bewertungsrelevanter Information* in eigenen Nachrichten. Einige dieser Möglichkeiten werden durch das vorgeschlagene Verfahren von vornherein ausgeschlossen:

- Da nur Nachrichten von Nachbarn für die Beobachtung herangezogen werden, entfällt die Unterschlagung (die nur bei erforderlicher Weiterleitung möglich wäre).
- Die gezielte Zerstörung oder Verfälschung bestimmter bewertungsrelevanter Informationen innerhalb fremder Nachrichten ist technisch aufgrund der Eigenschaften der Signalausbreitung nur in den seltensten Fällen realisierbar. Eine Mindestvoraussetzung hierfür ist, dass sich der Angreifer in einer geeigneten Position zwischen Sender und Empfänger befindet. Normalerweise gibt es aber mehrere benachbarte Knoten, die ebenfalls Beobachtungen durchführen, und der Angreifer kann eine Übertragung nicht für alle Beobachter in gleicher Weise manipulieren.
- Die Falschangabe bewertungsrelevanter Information ist dann sinnlos, wenn der einzige Zweck der unversehrten Information darin liegt, dem Sender eine positive Bewertung zuzuordnen.

Es bleiben die Möglichkeiten der Zerstörung fremder Nachrichten, der Wiedereinspielung fremder Nachrichten und der Falschangabe bewertungsrelevanter Information in eigenen Nachrichten (ggf. um eine Nachricht so erscheinen zu lassen, als sei sie von einem anderen Knoten erzeugt worden):

1. *Fälschung der Identität des Weiterleiters:* Für positive Bewertungen kann die Identität des zu bewertenden Teilnehmers an der (ungesicherten) Schicht-2-Absenderadresse des beobachteten Pakets abgelesen werden. Durch Falschangabe könnte der

Absender nur sich selbst schaden. Für negative Bewertung unterlassener Weiterleitung muss die Identität des zu Bewertenden aus der Schicht-2-Zieladdresse des weiterzuleitenden Pakets ermittelt werden. Diese Angabe könnte also nur vom vorigen Weiterleiter gefälscht werden (abgesehen von technisch schwierig zu realisierender Überlagerung der Übertragung durch den Empfänger, die allenfalls einen Teil der Beobachter täuschen könnte). Die Fälschungsmotivation für diesen ist gering, da er keinen direkten eigenen Vorteil hätte, sondern höchstens versuchen könnte, die Einschätzungen eines Anderen in den Augen Dritter zu verschlechtern. Dazu könnte der Angreifer absichtlich Schicht-2-Empfänger angeben, die die jeweiligen Pakete gar nicht empfangen und deshalb auch nicht weiterleiten können.

2. *Erfinden angeblich weiterzuleitender Pakete:* Erzeugt ein „Weiterleiter" ein angeblich weiterzuleitendes Paket selbst oder wiederholt er ein früher bereits übertragenes Paket noch einmal, erbringt er keine positiv zu bewertende Dienstleistung. Varianten dieses Angriffs sind:
   (a) Das „Weiterleiten" erfundener bzw. Wiederholen eines Pakets führt zwar zu positiven Bewertungen, ergibt für den Angreifer jedoch keinen Energievorteil.
   (b) Unterhält ein Knoten mehrere Identitäten und tritt er unter einer Identität als Weiterleiter der unter einer anderen Identität erzeugten Pakete auf, kann er positiven Bewertungen für eigene Pakete erhalten (attraktiver Angriff!).
3. *Weiterleitung über nicht erreichbare Knoten:* Dieser Angriff kann dazu verwendet werden, selbst eine positive Bewertung zu erhalten (auf Kosten eines Sendevorgangs) oder anderen Knoten negative Bewertungen zu verursachen.
4. *Senden an einen falschen nächsten Weiterleiter:* Der Angreifer kann evtl. den Aufwand der Teilnahme an einem Routing-Protokoll einsparen und z. B. immer an einen zufällig gewählten Nachbarn weiterleiten, oder an einen bestimmten, besonders zu strapazierenden Nachbarn, um diesem zu schaden. Solche Weiterleitung ist keine vollwertige Leistung.
5. *Vortäuschen, ein weiterzuleitendes Paket nicht erhalten zu haben:* Dieser Angriff kann dazu verwendet werden, negative Bewertung für Nichtweiterleitung zu vermeiden, ist jedoch nur durchführbar, wenn die negative Bewertung noch davon abhängig ist, ob der Beobachter eine im verwendeten Schicht-2-Protokoll vorgesehene Empfangsbestätigung beobachtet, die der Angreifer dann absichtlich unterschlagen kann; in diesem Fall handelt es sich um einen attraktiven Angriff.
6. *Vorschieben einer negativen Zugangsentscheidung als Begründung für Nichtweiterleitung:* Damit Beobachter nicht von böswillig unterlassener Weiterleitung ausgehen, werden negative Zugangsentscheidungen bekannt gemacht. Unkooperative Knoten könnten ausschließlich negative Entscheidungen treffen.

Gegenmaßnahmen Gegen Angriffe, durch welche der Angreifer sich einen Vorteil verschaffen kann, werden die folgenden Maßnahmen vorgeschlagen. Rein destruktive Angriffe ohne umfassende Auswirkungen werden nicht betrachtet.

- *Werte nur dann positiv, wenn der vorige Weiterleitungsschritt beobachtet wurde:* Anhand der Beobachtung des vorigen Weiterleitungsschrittes kann erkannt werden, dass ein Paket weder erfunden noch wiederholt wurde. Jeder Knoten speichert

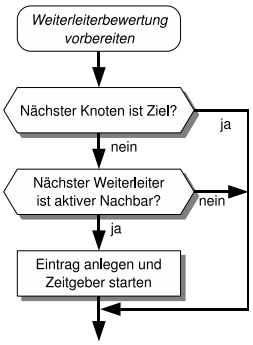

Abb. 2. Vorbereitung der Weiterleitungsbeobachtung

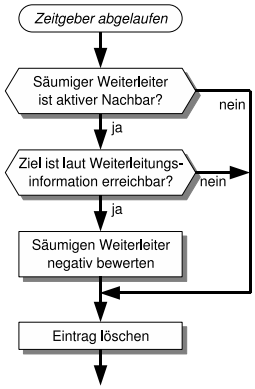

Abb. 3. Negative Bewertung bei Ablauf des Zeitgebers

dafür zu jedem beobachteten Paket für kurze Zeit einen Hash-Wert, anhand dessen er wiedererkennen kann, ob es vom nächsten Weiterleiter erneut ausgesendet wird. Für die Bewertung fallen Beobachter weg, die den vorigen Weiterleitungsschritt nicht beobachten konnten, so dass insgesamt weniger positive Bewertungen vergeben werden können (richtet sich gegen Angriff 2).

- *Werte nur dann negativ, wenn der Knoten, der weiterleiten soll, in der Nachbarschaft des Beobachters ist:* Diese Maßnahme richtet sich gegen die Angriffe 1 und 3 bzgl. negativer Bewertung und stellt weiterhin sicher, dass Knoten nur dann negativ bewertet werden, wenn eine potentielle Weiterleitung überhaupt vom bewertenden Knoten beobachtet werden könnte.
- *Werte bei ausbleibender Weiterleitung auch dann negativ, wenn der Empfang des weiterzuleitenden Pakets vom säumigen Weiterleiter nicht bestätigt wurde:* Diese Maßnahme hilft bei im Schicht-2-Protokoll vorgesehenen Empfangsbestätigungen gegen Vortäuschen von Empfangsproblemen (Angriff 5).
- *Übertrage in Fehlermeldungen aufgrund von Zugangsentscheidungen auch die abgelehnten Pakete:* Negative Zugangsentscheidungen sind somit mindestens so umfangreich wie die eigentlich weiterzuleitenden Pakete so dass Angriff 6 keinen Energievorteil mehr ergibt. Weiterhin kann dadurch jeder Beobachter nach Empfang der Fehlermeldung das abgelehnte Paket in seiner Liste löschen.

3.3 Detaillierte Verfahrensbeschreibung

Beim Absenden selbst erzeugter Pakete sowie bei der Weiterleitung fremder Pakete wird kurz vor der Aussendung zum nächsten Weiterleiter die Beobachtung vorbereitet (siehe Abbildung 2). Dazu wird das Paket in die Liste beobachteter Pakete aufgenommen, falls es erstens nach der selbst durchzuführenden Weiterleitung tatsächlich nochmal weitergeleitet werden muss (nächster Knoten $\neq$ Zielknoten) und sich zweitens der nächste Weiterleiter in der Nachbarschaft des Beobachters befindet. Der angelegte Eintrag enthält einen Hashwert über alle Bestandteile des Pakets, die bei der Weiterleitung

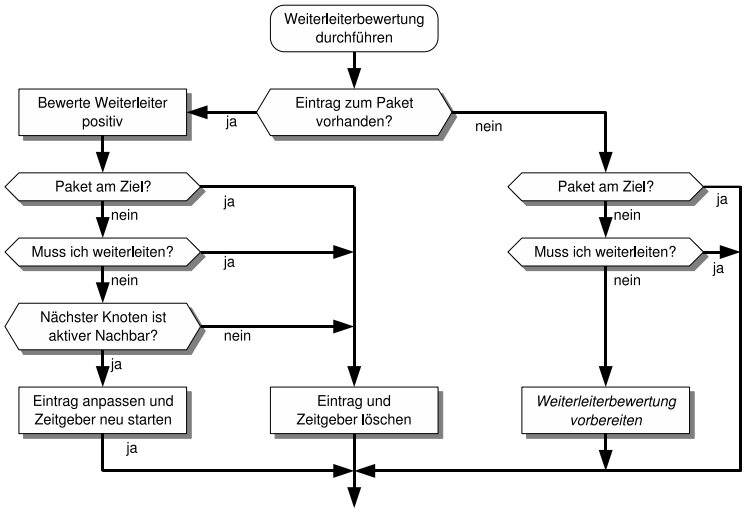

Abb. 4. Ablauf der Weiterleitungsbeobachtung

nicht verändert werden, sowie die Adresse des Schicht-2-Empfängers. Dem Eintrag ist ein Zeitgeber zugeordnet, bis wann die nächste Weiterleitung erfolgt sein sollte.

Abbildung 4 stellt die Abläufe dar, die für jedes empfangene oder mitgehörte Paket stattfinden. Anhand der Liste beobachteter Pakete wird festgestellt, ob das Paket bereits früher beobachtet bzw. selbst gesendet wurde. Hierzu wird der über das beobachtete Paket berechnete Hash-Wert in der Liste gesucht und geprüft, ob der Schicht-2-Absender des beobachteten Pakets mit dem im Eintrag gespeicherten Schicht-2-Empfänger übereinstimmt. In diesem Fall wird eine positive Beobachtung in dem Vertrauensprofil des Weiterleiters registriert. Unabhängig davon, ob eine positive Bewertung stattgefunden hat, ist das Ziel der nachfolgenden Schritte, die weitere Beobachtung des Pakets vorzubereiten, falls es nochmals weitergeleitet werden muss. Die Bearbeitung ähnelt deshalb der aus Abbildung 2, mit zwei Unterschieden: Muss der bearbeitende Knoten das Paket selbst weiterleiten, wird der Eintrag in der Liste beobachteter Pakete gelöscht, da das eigene Verhalten ja nicht bewertet wird. Weiterhin ist in manchen Fällen ggf. schon ein Eintrag vorhanden, der nur noch angepasst werden muss.

Schließlich muss noch der Fall eines ablaufenden Zeitgebers behandelt werden (Abbildung 3). Eine negative Bewertung wird in diesem Fall nur dann durchgeführt, wenn angenommen werden kann, dass der säumige Weiterleiter sich noch in der Nachbarschaft des Beobachters aufhält und das Ziel des Pakets erreichbar ist. Diese beiden Fragen werden anhand der lokalen Nachbarschaftsinformation und Routing-Tabelle geklärt. Sind die Bedingungen für eine negative Bewertung erfüllt, so wird aus der im Eintrag gespeicherten Schicht-2-Empfängeradresse die zugehörige Teilnehmerkennung ermittelt und für diese eine negative Beobachtung registriert. Der Eintrag in der Liste beobachteter Pakete wird abschließend gelöscht, da davon ausgegangen wird, dass das Paket entweder verloren gegangen ist oder den vom Beobachter wahrnehmbaren Bereich des Netzes verlassen hat.

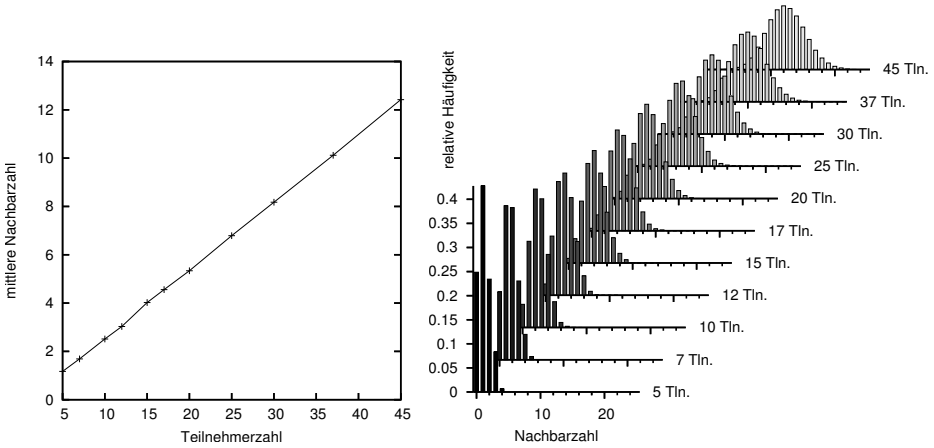

Abb. 5. Mittlere Nachbarzahl (links) und relative Häufigkeiten bestimmter Nachbarzahlen (rechts) in Abhängigkeit von der Teilnehmerzahl bei gleichbleibend großem Simulationsgebiet

4 Evaluation

Im Folgenden wird untersucht, ob und unter welchen Bedingungen die beschriebene Methode zur Beobachtung des Weiterleitungsverhaltens benachbarter Knoten ihre Funktion erfüllen und möglichst schnell eine ausreichende Menge an Information über das Verhalten der Nachbarn liefern kann. Hierfür wurde ein Netzknotenmodell innerhalb der Simulationsumgebung OMNeT++implementiert, wobei in der Schicht 2 zunächst ein idealisiertes Medienzugangsverfahren verwendet wurde, welches Kollisionen vermeidet und die verfügbare Bandbreite möglichst gut ausnutzt.

Zunächst wird die Verteilung von Nachbarzahl und Dauer von Nachbarschaftsverhältnissen in simulierten Szenarien betrachtet, da die Zahl der Nachbarn eines Knotens bestimmt, wie oft eine erbrachte Leistung oder ihre Verweigerung maximal beobachtet werden kann, und gegenseitige in Beobachtungen gewonnene Einschätzungen umso sicherer werden, je länger zwei Knoten Nachbarn sind.

Abbildung 5 zeigt links die per Simulation ermittelte Abhängigkeit zwischen Teilnehmerzahl und mittlerer Nachbarzahl bei gleichbleibender Gebietsgröße, rechts sind die relativen Häufigkeiten bestimmter Nachbarzahlen für Teilnehmerzahlen zwischen 5 und 45 aufgezeichnet. Dabei bewegten sich die Teilnehmer zufällig nach dem Random-Waypoint-Modell mit gleichverteilter Geschwindigkeit zwischen 1 und 10 m/s sowie gleichverteilter Wartezeit zwischen 1 und 30 s in einem torusförmigen Simulationsgebiet von 600 m Länge und 600 m Breite; als maximale Sendereichweite wurden 180 m angenommen. Es ist eine lineare Abhängigkeit zwischen Teilnehmerzahl und mittlerer Nachbarzahl zu erkennen. Theoretische Überlegungen zum Zusammenhang zwischen Gesamtteilnehmerzahl N_T, Gebietsgröße A, Übertragungsreichweite r und mittlerer Nachbarzahl N_N bestätigen dieses Ergebnis:

$$N_N = \frac{N_T - 1}{A} \cdot \pi \cdot r^2. \tag{1}$$

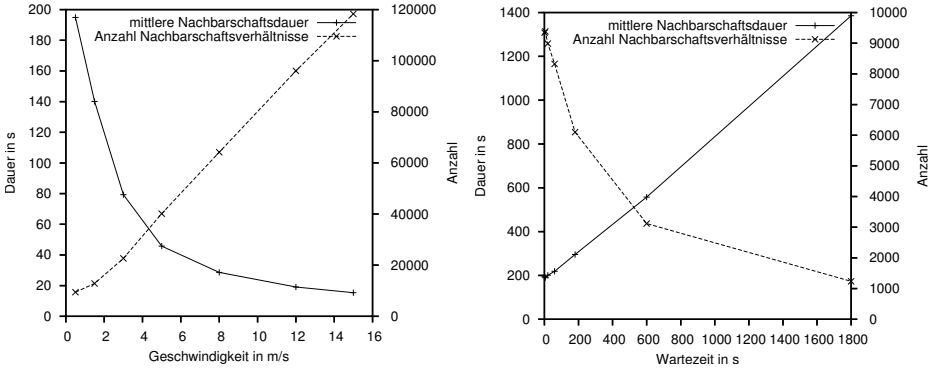

Abb. 6. Mittlere Dauer von Nachbarschaftsverhältnissen in Abhängigkeit von der Geschwindigkeit (Aufenthaltsdauer 1 s; links) bzw. Aufenthaltsdauer (Geschwindigkeit um 0,5 m/s; rechts)

Die maximale Übertragungsreichweite r, die in der Realität aufgrund unterschiedlicher Sendeleistung und Emfangsempfindlichkeit sowie von Störeinflüssen für jede Knotenpaarung verschieden sein kann, wird hierbei vereinfachend als eine scharfe, für alle Knotenpaarungen gleiche Entfernung angenommen. Fehlerfreie Signalübertragung sei genau bei jeder kürzeren Distanz zwischen zwei Knoten möglich.

Versuche mit unterschiedlicher Parametrisierung des Random-Waypoint-Modells zeigen, dass die mittlere Nachbarzahl stets dem rechnerisch ermittelten Wert entspricht.

Bei sehr kurzer Aufenthaltszeit (Mittelwert 1 s) ergibt sich ein regelmäßiger Zusammenhang zwischen Knotengeschwindigkeit und Dauer von Nachbarschaftsverhältnissen. Abbildung 6 stellt hierzu die mittlere Nachbarschaftsdauer und die dazu umgekehrt proportionale Anzahl von Nachbarschaftsverhältnissen über der gewählten mittleren Knotengeschwindigkeit dar. Bei längeren Aufenthaltszeiten streut die Dauer von Nachbarschaftsverhältnissen stärker und ist im Mittel größer. Variiert man statt der Geschwindigkeit die Aufenthaltsdauer, so erhält man den rechts dargestellten Verlauf der mittleren Nachbarschaftsdauer. Man sieht, dass der Mittelwert nahezu linear mit der Aufenthaltsdauer ansteigt. Zusammenfassend führen beim Random-Waypoint-Bewegungsmodell größere Geschwindigkeiten zu einer Häufung kurzer Nachbarschaftsdauern und größere Aufenthaltszeiten zu einer stärkeren Streuung.

Damit eine erbrachte Weiterleitungsleistung auch bewertet werden kann, müssen nicht nur Beobachter vorhanden sein, sondern es muss auch jeweils die Zusatzbedingung erfüllt sein, dass der Beobachter auch den vorigen Weiterleitungsschritt beobachtet hat, damit er sicher sein kann, dass es sich um eine Weiterleitung und nicht um die Aussendung einer eigenen Nachricht handelt (erste Gegenmaßname in Abschnitt 3.2). Um empirisch zu untersuchen, ob die Zusatzbedingung die Bewertungsmöglichkeiten zu stark einschränkt, wurde im Versuch zunächst die Anzahl aller vergebenen positiven Weiterleitungsbewertungen erfasst und in Verhältnis zur Zahl der insgesamt durchgeführten Weiterleitungsvorgänge gesetzt. Abbildung 7 zeigt links das Ergebnis, aufgetragen über der Teilnehmerzahl des verwendeten Netzes; zum Vergleich ist dort außerdem die ermittelte mittlere Nachbarzahl eingetragen. Man sieht, dass die mittlere

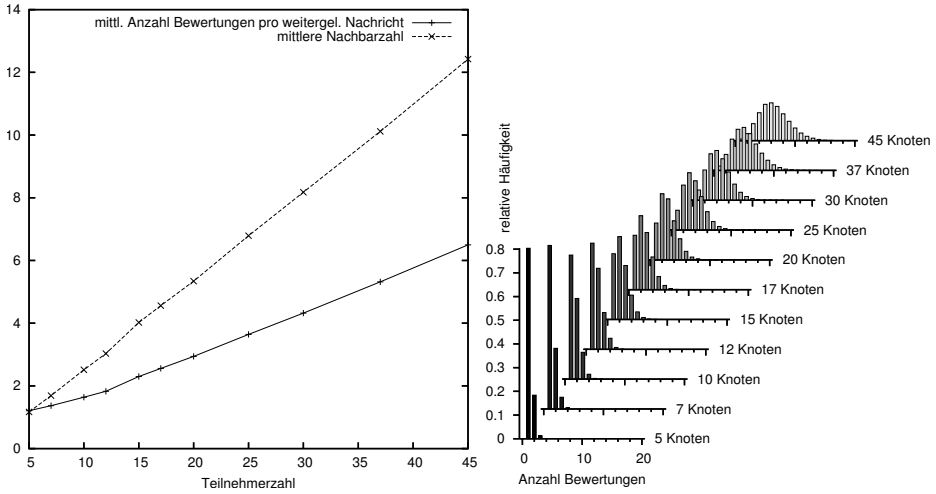

Abb. 7. Anzahl (positiver) Bewertungen pro weitergeleiteter Nachricht (links) sowie Häufigkeiten bestimmter Anzahlen positiver Bewertungen bei weitergeleiteten Nachrichten (rechts)

Zahl der Bewertungen pro weitergeleiteter Nachricht näherungsweise proportional zur Teilnehmer- und etwa halb so groß wie die mittlere Nachbarzahl ist, abgesehen vom unteren Teilnehmerzahlbereich, wo sie etwas höher ist. Bei der Anzahl von 25 Teilnehmern wurden immerhin 3,64 positive Bewertungen pro erfolgter Weiterleitung vergeben. Es erscheint somit durchaus plausibel, dass aufgrund der bewerteten Beobachtungen zügig Einschätzungen zur Kooperationsbereitschaft der beobachteten Teilnehmer gewonnen werden können. Bei diesen Experimenten wurden nur positive Bewertungen betrachtet, und die verwendeten Modellteilnehmer verweigerten niemals absichtlich Leistungen; andernfalls käme jeweils eine ähnliche Zahl an Negativbewertungen zustande. Eine Differenzierung wurde für eine erste Evaluierung nicht vorgenommen, da hierfür nur die Gesamtzahl verwertbarer Beobachtungen eingeschätzt werden muss.

Bezüglich des Einflusses der Teilnehmermobilität auf die in diesem Abschnitt beschriebenen Zusammenhänge ist festzustellen, dass sie lediglich von der Teilnehmerdichte des betrachteten Netzwerks abhängen. Da diese bei Verwendung des Random-Waypoint-Modell homogen ist, ergeben sich auch durch Variation der Verteilungen für Geschwindigkeiten und Aufenthaltsdauern keine Änderungen. Realitätsnähere Bewegungsmodelle bewirken stärkere Häufungen der Teilnehmer, was auch zu einer höheren mittleren Nachbarzahl führt. Versuche mit solchen Mobilitätsmodellen mit inhomogeneren Teilnehmerdichten ergeben regelmäßig eine höhere Bewertungsquote, da hier mehr Nachbarschaftsbeziehungen bestehen und somit mehr Beobachtungen bewertet werden können.

5 Zusammenfassung und Ausblick

Der vorliegende Beitrag stellt ein Verfahren zur Beobachtung und Bewertung des Weiterleitungsverhaltens von Ad-hoc-Netz-Teilnehmern vor, welches im Unterschied zu

existierenden Verfahren erstens nicht von einem bestimmten Routing-Protokoll abhängig ist und zweitens auch Beobachter erlaubt, die selbst nicht am beobachteten Weiterleitungsvorgang beteiligt sind. Gezielte Täuschungen des Verfahrens, durch welche Angreifer sich Vorteile durch falsche Bewertungen verschaffen könnten, wurden dabei nach einer detaillierten Analyse der Angriffsmöglichkeiten durch Gegenmaßnahmen ausgeschlossen.

Dadurch, dass Beobachtungen auch durch Teilnehmer erfolgen können, die an dem Weiterleitungsvorgang selbst nicht beteiligt sind, entstehen wesentlich mehr Beobachtungen pro Weiterleitungsvorgang als bei existierenden Verfahren, wo nur jeweils eine Beobachtung anfallen kann. Die simulative Evaluation des Verfahrens zeigt, dass die Anzahl verwertbarer Beobachtungen etwa halb so groß ist wie die Zahl der Nachbarn des weiterleitenden Knotens. Diese höhere Beobachtungszahl führt insgesamt dazu, dass in kürzerer Zeit bessere Einschätzungen ermittelt werden können.

Einschätzungen beliebiger entfernter Netzknoten, wie sie etwa für eine Zugangskontrolle aufgrund der Einschätzung der Quellknoten weiterzuleitender Pakete benötigt werden, kann die Beobachtung von Nachbarn nur allmählich durch mobilitätsbedingte Durchmischung der Teilnehmer liefern. Wesentlich schneller erhält man Einschätzungen entfernter Teilnehmer, wenn lokal ermittelte Einschätzungen im Netz verteilt und von anderen Teilnehmern in geeigneter Weise einbezogen werden. Ein entsprechendes, auf dem hier vorgestellten Ansatz aufbauendes Verfahren wird in [Kraf06] beschrieben.

In den hier vorgestellten Simulationen wurde ein idealisiertes Medienzugangsverfahren verwendet. Bei realen Verfahren können durch gleichzeitiges Senden von Knoten, die sich außerhalb ihrer gegenseitigen Sendereichweite befinden, bei Beobachtern Überlagerungen entstehen, durch welche Beobachtungen verhindert werden. Die Untersuchung der Auswirkungen solcher Effekte ist Gegenstand zukünftiger Arbeiten.

Literaturverzeichnis

[BaBa03] S. Bansal und M. Baker. Observation-based cooperation enforcement in ad hoc networks. Technischer Bericht, Stanford University, 2003.

[BuBo02] S. Buchegger und J.-Y. Le Boudec. Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks). In *Proc. ACM Symp. on Mobile Ad Hoc Networking & Computing (MobiHoc)*, Juni 2002.

[BuBo04] S. Buchegger und J.-Y. Le Boudec. A Robust Reputation System for P2P and Mobile Ad-hoc Networks. In *Proc. 2nd Workshop on the Economics of Peer-to-Peer Systems*, Juni 2004.

[BuTLB04] S. Buchegger, C. Tissieres und J. Y. Le Boudec. A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks - How Much Can Watchdogs Really Do? In *Proc. IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, English Lake District, UK, Dezember 2004.

[HeWK04] Q. He, D. Wu und P. Khosla. SORI: A secure and objective reputation-based incentive scheme for ad hoc networks. In *Proc. IEEE Wireless Communications and Networking Conference*, Atlanta, GA, USA, März 2004.

[Kraf06] D. Kraft. *Verteilte Zugangskontrolle in offenen Ad-hoc-Netzen*. Dissertation, Universität Karlsruhe (TH), 2006.

[MGLM00] S. Marti, T. J. Giuli, K. Lai und M.Baker. Mitigating Routing Misbehaviour in Mobile Ad hoc Networks. In *Proc. 6th International Conf. on Mob. Comp. and Networking (MOBICOM)*, August 2000, S. 255–265.