Testbed E

Christian
[Christian.Gottron;Pedro.Larbig;Andre.Koenig; Ralf.Steinmetz]@KOM.TU-Darmstadt.de
Multimedia Kommunikation (KOM), Technische Universität Darmstadt
Matthias.Hollick@SEEMOO.TU-Darmstadt.de
Secure Mobile Networking Lab (SEEMOO), Technische Universität Darmstadt

Mobile Ad hoc Netze (MANET) wurden in den letzten Jahren vielfach auf Robustheit und Sicherheit untersucht. Exsistierende Arbeiten evaluierten Angriffe und Gegenmaßnahmen primär theoretisch oder analytisch. Im Rahmen dieser Arbeit wird der Aufbau eines Testbeds am Institut für Multimedia Kommunikation an der TU-Darmstadt vorgestellt. Dabei entstandene Herausforderungen und Lösungsansätze werden herausgearbeitet. Innerhalb dieses Testbeds wird der Black Hole-Angriff analysiert. Die Ergebnisse dieser Arbeit zeigen, dass das AODV Protokoll mit Hilfe eines Filters stabilisiert werden kann, der Verbindungen verhindert, die nicht eine minimale Signalqualität aufweisen. Weiterhin zeigte sich, dass der Black Hole-Angriffe in einem Testbed einen starken Einfluss auf die Verfügbarkeit von Routen innerhalb des Netzes hat.

I. Motivation und Ziele

In Katastrophenschutze Szenarien oder in der Car-to-Car-Kommunikation kann nicht von einer verfügbaren Infrastruktur ausgegangen werden. Aufgrund dessen können traditionelle Architekturen oft nicht angewandt werden. Da Mobile Ad hoc Netze (MANET) aufgrund ihrer dezentralen Eigenschaft ohne Infrastruktur operieren, bieten sich diese als Ersatz der traditionellen Architekturen in einem solchen Szenario an.

Es existieren diverse wissenschaftliche Arbeiten die sich mit MANETs befassen. Diese basieren meist auf theoretischen Modellen oder Simulationen. Dabei werden aufgrund der Komplexität Eigenschaften realer drahtloser Netze abstrahiert was zu Abweichungen zwischen theoretischen und realen Ergebnissen führen kann [1]. Bisher wurden nur wenige Aspekte der MANETs aus praktischer Sicht betrachtet. Vor allem im Gebiet der Netzwerksicherheit existieren nur wenige Testbed-basierte Analysen von Angriffen und Gegenmaßnahmen.

Um solche Angriffsszenarien zu analysieren, wurde ein MANET Testbed aufgebaut. In dieser Arbeit wird die Auswirkung des Black Hole-Angriffs betrachtet. Das Ziel dieses Angriffs auf den Routing Algorithmus des Netzes ist es, möglichst viele Routen über einen bösartigen Knoten zu leiten. Daraufhin können die an den Angreifer gesendeten Daten verworfen oder untersucht und gespeichert werden, um das Netz zu stören bzw. Daten über die anderen Teilnehmer des Netzes zu sammeln.

II. Aufbau des Testbeds

Das Testbed besteht aus 7 Lenovo Notebooks der R61 bzw. R61i Serie auf denen eine Ubuntu Distribution der Version 9.04 als Betriebssystem läuft. Das *Ad hoc on demand Distance Vector* (AODV) [2] Protokoll wurde für das Routing eingesetzt. Dieses reaktive Protokoll bietet sich aufgrund seiner weiten Verbreitung und Bekanntheit in wissenschaftlichen Kreisen für erste Versuche in einem Testbed an, da viele theoretische Arbeiten als Referenz existieren. Es wird die AODV-UU [3] Implementierung verwendet, welche an der Uppsala Universität in Schweden entwickelt wurde. Diese ist für Netzwerke basierend auf dem IEEE 802.11 Standard entwickelt worden und wurde strikt nach dem AODV RFC implementiert. Aufgrund einer Inkompatibilität zu dem neuen im Testbed verwendeten Linux Kernel 2.6.28, musste AODV-UU angepasst werden. Dadurch wurde allerdings die Funktionalität des Protokolls weder verändert noch eingeschränkt.

Die Notebooks wurden innerhalb des Instituts für Multimedia Kommunikation an der TU-Darmstadt über mehrere Büro-
räume v
che. In
einzelne

gen mit einer Qualität von über *-70 dbm* zwischen den einzelnen Teilnehmern des Netzes als Linien dargestellt. Diese Signalqualität hat sich in Vortests als zuverlässig erwiesen.

III. Evaluation des AODV Protokolls

Die ersten Versuche bezüglich der Funktionalität der AODV Implementierung zeigten Verbindungsabbrüche in einem gesteigertem Maße bei Multi-Hop-Strecken. Diese wurden durch *Gray Zones* [1] hervorgerufen. *Gray Zones* entstehen durch die unterschiedliche Reichweite von Broadcast und Unicast Nachrichten. Während Broadcast Nachrichten mit niedrigerer Übertragungsrate gesendet werden und dementsprechend eine hohe Reichweite haben, werden Unicast Nachrichten mit maximaler Übertragungsrate gesendet. Dies resultiert in einer niedrigeren Reichweite der Unicast Nachrichten in der die gesendeten Daten noch von einem Empfänger korrekt dekodiert werden können. Da die Routing Nachrichten des AODV Protokolls als Broadcast Nachrichten gesendet werden, haben sie eine höhere Reichweite als Datenpakete, die über die etablierte Route per Unicast Nachricht gesendet werden. Dadurch werden Verbindungen zwischen Knoten aufgebaut und für Routen ausgewählt, über die Daten nicht zuverlässig übertragen werden können. Weiterhin verwendet das Protokoll eine Metrik, die die kürzeste Routen (bezüglich der Anzahl der Hops) bevorzugt. Daraus ergibt sich, dass bei der Wahl des nächsten Knotens auf der Route jene Knoten bevorzugt werden, die möglichst weit vom aktuellen Knoten entfernt liegen. Aufgrund dessen ist die Wahrscheinlichkeit, dass Knoten sich in der *Gray Zone*, also der Grenzzone zwischen der Reichweite der Broadcast und der Unicast Nachrichten, befinden hoch.

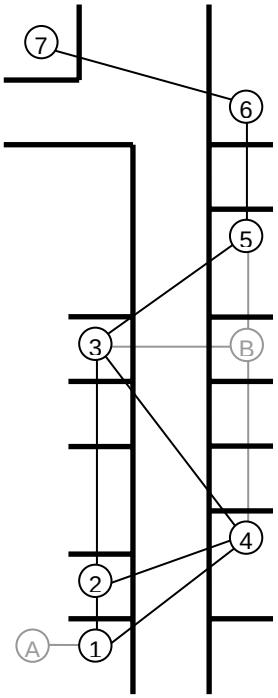

Abb.1: Aufbau des Testbeds und Verteilung der Knoten

Um die *Gray Zone*-Problematik zu vermeiden, schlagen Lundgren et al. [4] neben diversen anderen Ansätzen vor, die minimale akzeptierte Verbindungsqualität zwischen den Knoten durch einen Filter zu begrenzen. Dieser soll direkt in AODV implementiert werden. Als Folge dessen werden alle Pakete verworfen, die mit einer Signalqualität empfangen werden, die einen festgelegten Wert unterschreiten. Aufgrund des von Lundgren et al. verwendeten 802.11 Treibers
rte für
d wur-
genaue

Signalqualität zurückgreifen kann. Dieser Filter wurde nicht direkt in AODV implementiert, sondern in Form eines MAC-Filters als separates Programm eingesetzt. Dieses kann unabhängig von dem verwendeten Routing Protokoll eingesetzt werden. Mit Hilfe einer Erweiterung des aktuellen Linux Kernels, kann die Verbindungsqualität wesentlich genauer und zuverlässiger ermittelt werden. Weiterhin ist in dem hier beschriebenen Ansatz die Qualität als Durchschnittswert der *n* zuletzt empfangenen Nachrichten definiert. Dadurch werden starke Schwankungen vernachlässigt und die Routen im Allgemeinen stabiler.

Aus einem direkten Vergleich eines MANETs mit und ohne Filter ging hervor, dass Multi-Hop-Routen, die ohne Filter aufgebaut wurden, wesentlich instabiler sind als jene, die mit Hilfe des Filters ermittelt wurden. Selbst Verbindungen die lediglich über einen einzelnen zwischenliegenden Knoten geroutet werden weisen Verluste von über 50% der gesendeten Pakete auf. Wenn im gleichen Szenario ein Filter eingesetzt wird, können die Verluste auf etwa 5% reduziert werden. Passt man den Filter gezielt an das Szenario an, so reduzieren sich die Verluste auf etwa 2%. Weiterhin entstehen durch den filterlosen Einsatz von AODV Latenzen die um den Faktor zehn höher sind im Vergleich zu einem Szenario mit Filter.

IV. Evaluation des Black Hole-Angriffs

Fehlverhaltende Knoten die einen Black Hole-Angriff durchführen, leiten möglichst viel Datenverkehr über sich. Diesen können sie dann verwerfen oder umleiten um somit das Netz zu stören. Um diesen Angriff möglichst erfolgreich zu implementieren, antworten bösartige Knoten auf alle Anfragen nach Routen und geben an, eine gültige Route mit minimaler Distanz zum Zielknoten in ihrer Routingtabelle gespeichert zu haben. Sollte der anfragende Knoten näher am Zielknoten liegen als am Angreifer, so bleibt der Angriff ohne Folgen. Andernfalls wird der anfragende Knoten die vermeintlich optimale Route über den Angreifer für den Datenaustausch verwenden.

Da die Effizienz dieses Angriffs stark von der Position des Angreifers innerhalb des Netzes abhängig ist, werden im Folgenden zwei Szenarien präsentiert. In Szenario A ist der Angreifer am Rand des Netzes positioniert, während in Szenario B der Angreifer an eine für den Angriff optimierte Position innerhalb des Netzes platziert wurde. Hier ist anzunehmen, dass der zweite Angriff einen erkennbar größeren Einfluss auf das Netz hat. Die Position der Angreifer in beiden Szenarien und die Anbindung an das MANETs sind in Abbildung 1 dargestellt.

In beiden Szenarien werden die Verbindungen zwischen den Knoten des Netzes paarweise per Ping überprüft. Hierbei baut AODV-UU sowohl eine Hin- als auch eine Rückroute zwischen dem Knotenpaar auf. Da in einem realen Netz unidirektionale Verbindungen aufgrund der variierenden Übertragungsreichweiten der einzelnen Knoten entstehen können, muss auf eine solche Maßnahme zurückgegriffen werden. Daraus folgt allerdings, dass Routen nur dann erfolgreich aufgebaut werden können, wenn die Distanz zwischen beiden Knoten niedriger ist als die Distanz zwischen einem der beiden Knoten und dem Angreifer. Dadurch erhaltenen wir symmetrische Ergebnisse wie sie in Tabelle 1 und 2 zu sehen sind. Diese Tabellen zeigen die Wahrscheinlichkeit, das Knoten *X* eine Antwort auf ein Ping erhält, das er an Knoten *Y* gesendet hat ($X, Y \in M, M=\{1, 2, 3, 4, 5, 6, 7\}$). Weiterhin wurden Routen, die durch den Black Hole-Angriff betroffen sind, zur Verdeutlichung grau hinterlegt.

Das Ergebnis des Experiments in Szenario A zeigt, dass selbst ein Angreifer, der sich am Rande des Netzes befindet, dieses sehr stark beeinflussen kann. Wie in Tabelle 1 zu sehen ist, werden mehr als 50% aller Verbindungen gestört (graue hinterlegt). Im Fall der Verbindungen zwischen Knoten 2 und 5 bzw. 4 und 5 liegen Quell- und Zielknoten genau soweit von einander entfernt wie deren Entfernung zu dem Angreifer ist. Aufgrund dessen kann mit einer gewissen Wahrscheinlichkeit das Routing erfolgreich beendet werden. In diesen Fällen erhält der anfragende Knoten die Routing Nachricht des legitimen Knotens vor der Nachricht des Angreifers. Da der Angreifer allerdings vorgibt, dass seine Route aktueller ist, verwirft das AODV Protokoll die korrekte Route zugunsten der vermeintlich gleichlangen und aktuelleren Route über den Angreifer. Dies erlaubt jedoch zumindest eine kurzfristige korrekte Datenübertragung. Weiterhin kommt es nach einer gewissen Zeit, in der der sendende Knoten keine Antwort erhält zu einem Timeout und einer erneuten Routenfindung. Hier kann es folglich wieder zu einem kurzzeitigen Datenaustausch kommen, bevor der Angriff die Datenübertragung erneut stört.

	1	2	3	4	5	6	7
1		100%	0%	100%	0%	0%	0%
2	100%		100%	100%	14%	0%	0%
3	0%	100%		100%	100%	100%	0%
4	100%	100%	100%		13%	0%	0%
5	0%	15%	100%	16%		100%	100%
6	0%	0%	100%	0%	100%		100%
7	0%	0%	0%	0%	100%	100%	

Tab.1: Erfolgreiche Datenübertragung zwischen Knotenpaaren in Szenario A

Im zweiten Szenario liegen die Verlustraten höher, da hier aufgrund der zentralen Lage des Angreifers lediglich Routen zu direkten Nachbarn aufgebaut werden können. Entsprechend liegen die Verluste bei über 60% wie es der Tabelle 2 zu entnehmen ist (grau hinterlegt). Hierbei ist anzumerken, dass die Routen in Szenario B komplett gestört wurden und keinerlei Datentransfer auf den beeinträchtigten Routen mehr übertragen werden konnte. Direkte Verbindungen zwischen Nachbarn können von Black Hole-Angriffen nicht unterbrochen werden, da für diese kein Multi-Hop-Routing Anfragen benötigt werden.

	1	2	3	4	5	6	7
1		100%	0%	100%	0%	0%	0%
2	100%		100%	100%	0%	0%	0%
3	0%	100%		100%	100%	0%	0%
4	100%	100%	100%		0%	0%	0%
5	0%	0%	100%	0%		100%	0%
6	0%	0%	0%	0%	100%		100%
7	0%	0%	0%	0%	0%	100%	

Tab.2: Erfolgreiche Datenübertragung zwischen Knotenpaaren in Szenario B

V. Zusammenfassung

Im Laufe dieser Arbeit konnte ein Testbed aufgebaut werden, welches mit Hilfe der Optimierung des AODV Protokolls stabil lief. Weiterhin konnte festgestellt werden, dass Black Hole-Angriffe selbst in kleineren Netzen einen sehr großen Einfluss auf die Verfügbarkeit der Netzwerkknoten haben. So können Daten nur noch dann korrekt übertragen werden wenn (I) die Distanz zwischen den kommunizierenden Knoten kleiner ist als die Entfernung der Knoten zum Angreifer oder wenn (II) direkte Nachbarn miteinander kommunizieren.

VI. Literaturverzeichnis

[1] H. Lundgren et al. : The Gray Zone Problem in IEEE 802.11b based Ad hoc Networks; ACM SIGMOBILE 2002

[2] C. Perkins et al.: RFC 3561 Ad hoc On-Demand Distance Vector (AODV) Routing

[3] E. Nordström: AODV-UU – CoReSoftware; Uppsala University, University Basel, http://core.it.uu.se/core/index.php /AODV-UU

[4] H. Lundgren et al.: Coping with Communication Gray Zones in IEEE802.11b based Ad hoc Networks; In proc. of the 5th ACM intern. WoWMoM'02