Verteiltes Packet-Sniffing als Sicherheitswerkzeug in MANETs

Alexander Wenzel[1] · Alexander Finkenbrink[1]
Marko Jahnke[1] · Jens Tölle[1] · Stefan Karsch[2]

[1]Forschungsgesellschaft für Angewandte Naturwissenschaften e.V. (FGAN)
Forschungsinstitut für Kommunikation, Informationsverarbeitung
und Ergonomie (FKIE)
{wenzel|finkenbrink|jahnke|toelle}@fgan.de

[2]Fachhochschule Köln, Campus Gummersbach
Institut für Informatik
stefan.karsch@inf.fh-koeln.de

Zusammenfassung

Packet-Sniffing bezeichnet das Erfassen von Netzwerkverkehr in Form von Paketen bzw. Frames auf den unteren Netzwerkebenen. Es bildet die notwendige technische Grundlage für verschiedene Aufgaben im Bereich des Netzwerk-Managements und der Sicherheit. In infrastrukturbasierten (drahtgebundenen) Rechnernetzen wird Packet-Sniffing oft durch entsprechende Sensoren an zentralen Stellen des Netzwerkes realisiert, um jeglichen Verkehr erfassen zu können. Grundlegend anders gestaltet sich die Erfassung von Netzwerkverkehr in drahtlosen, mobilen Adhoc-Netzen (MANETs), in denen keine zentrale Infrastruktur existiert. Um in diesen Netzen eine umfassende Überwachung des Verkehrs erreichen zu können, muss potentiell jeder Netzwerk-Knoten in der Lage sein, Packet-Sniffing zu betreiben, was aber wegen der Überlappung der Emfangsreichweiten zu Mehrfacherfassungen (Duplikaten) führen kann und durch den zusätzlichen Aufwand auch Auswirkungen auf die Batterielebensdauer der Knoten hat. Dieser Beitrag befasst sich mit der Beschreibung eines realisierten Sensors für die verteilte Datenerfassung.

1 Einführung

Viele Aufgaben im Bereich des Netzwerk-Managements und bei der Sicherstellung des ordnungsgemäßen Betriebs von Rechnernetzen basieren auf dem sog. *Packet-Sniffing*, dem Mitschneiden von Paketen. Viele Kenndaten von Netzwerken sind erst durch Beobachtung der über die Leitungen übertragenen Informationen bestimmbar.

Die Erkennung potentieller Angriffe gegen Rechnernetze anhand bestimmter, für missbräuchliches Verhalten repräsentativer Signaturen durch so genannte netzwerkbasierte Intrusion-Detection-Systeme (kurz *NIDS*) erfolgt auf dieser Basis. Verfahren, die auf der Ermittlung einer vollständigen Verkehrsstatistik beruhen, sind konkrete Anwendungsfelder des Packet-Sniffings.

In den meisten Fällen ist eine vollständige Überdeckung des Netzwerkverkehrs mit entsprechender Sensorik notwendig, um hinreichend sichere Aussagen treffen zu können; dies ist ins-

P. Horster (Hrsg.) · D•A•CH Security 2007 · syssec (2007) 1-12.

besondere in mobilen Adhoc-Netzwerken (*MANETs*) zunächst nicht immer möglich, weil ein Netzwerkknoten nur denjenigen Netzwerkverkehr erfassen kann, der das Funkmedium innerhalb seiner Empfangsreichweite nutzt.

2 Packet-Sniffing: Prinzip und Anwendungen

In diesem Abschnitt werden die Prinzipien des Packet-Sniffings und deren Eigenschaften erläutert. Zudem werden Anwendungen beschrieben, die sich dieses Verfahren zu nutze machen.

2.1 Prinzip und Funktionsweise

Der aktuell am weitesten verbreitete Standard zur Kommunikation in drahtgebundenen lokalen Netzen ist IEEE 802.3 (Ethernet). Dem ursprünglich eingesetzten Verfahren liegt die Idee zugrunde, dass mehrere Netzstationen das gleiche Übertragungsmedium im Zeitmultiplex nutzen. Damit ist prinzipiell von jeder Netzstation aus ein lesender Zugriff auf alle im Netz übertragenen Pakete möglich. Diesen Lesevorgang bezeichnet man als Packet-Sniffing. Das Prinzip des Packet-Sniffing ist grundsätzlich auch auf andere „Broadcast-Netze“, wie bspw. IEEE 802.11-basierende Funknetze übertragbar. Diese arbeiten nach dem CSMA/CA-Verfahren (Carrier Sense Multiple Access / Collision Avoidance), welches einen jederzeit möglichen Lesezugriff zum Erkennen der Belegung des Netzes voraussetzt. Eine Eigenschaft von Funknetzen ist die begrenzte Funkreichweite der Stationen. Deshalb muss davon ausgegangen werden, dass ein einzelner Knoten im allgemeinen nicht den gesamten Datenfluss des Netzes erfassen kann. Auch der zeitgleiche Datenfluß in räumlich getrennten Bereichen ist eine zu beachtende Eigenschaft eines Funknetzes.

Bei IP-basierten Netzen besitzt jeder der an das Netz angeschlossenen Rechner einen Netzadapter, der für die Umsetzung der rechnerinternen Datendarstellung in ein netzprotokollkonformes Format auf OSI-Layer 2 sorgt. Beim Empfang von Nachrichten übergibt der Netzadapter alle an einen Rechner gerichteten Pakete an das Betriebssystem zur weiteren Verarbeitung. Hierbei werden zunächst nur an diesen Rechner gerichtete Pakete weitergereicht. Das Verwerfen der übrigen Pakete erfolgt unter anderem aus Effizienzgründen Hardware-basiert durch den Netzadapter. Packet-Sniffing erfordert ein anderes Verhalten des Netzadapters: Anwendungen, die Packet-Sniffing nutzen sollen, erfordern die Verfügbarkeit aller über das Netz übertragenen Pakete für das Anwendungsprogramm. Die meisten der aktuellen Netzadapter für IP-basierte Netze besitzen die Möglichkeit, sie in den *Promiscuous Mode* zu versetzen. Hierbei werden alle über das Netz übertragenen Pakete an das Betriebssystem bzw. eine Anwendung weitergeleitet. Auch für die IEEE 802.11-Protokollfamilie sind Netzadapter verfügbar, die dies ermöglichen.

Die frei verfügbare Funktionsbibliothek *Libpcap* [1] ermöglicht auf Unix-basierten Systemen eine transparente Umschaltung des Netzadapters auf den Promiscuous Mode und liefert den Anwendungen alle über das entsprechende Netzsegment übertragenen Pakete.

2.2 Anwendung: Signaturbasierte Netzwerk-IDS

Eine verbreitete Anwendung des Packet-Sniffing sind Systeme zur netzbasierten Erkennung von Angriffen (Network Intrusion Detection Systems - NIDS). Diese Systeme erfassen den gesamten Netzverkehr und analysieren ihn im Hinblick auf typische Angriffsmuster. Wird ein Muster erkannt, so erfolgt eine Alarmierung, etwa, um entsprechende Gegenmaßnahmen einzuleiten. Ein Beispiel für ein Werkzeug zur netzbasierten Angriffserkennung ist *Snort* [2]. Snort

nutzt Libpcap und setzt zur Analyse Mustererkennung (Pattern-Matching) ein. Die im System hinterlegten Angriffsmuster werden nach dem Konzept der regulären Ausdrücke in einer systemspezifischen Syntax formuliert.

2.3 Anwendung: IP-Verkehrsstatistik

RMON bedeutet *Remote Monitoring* und ist ein in [3] festgelegter Standard zur Erfassung und Speicherung von statistischen Netzwerkkenndaten. Erfasste Daten werden in der MIB (*Management Information Base*) gespeichert. Diese Einträge können durch SNMP-Requests (*Simple Network Management Protocol*) abgefragt werden und dienen der Überwachung von Rechnernetzen im Rahmen von Wartung und Diagnose.

Mit den dadurch gewonnenen Daten und auch den durch Packet-Sniffing erhaltenen Informationen über den geflossenen Verkehr können in einem weiteren Verarbeitungsschritt detailliertere Kenntnisse über den aktuellen Zustand des Netzes gewonnen werden. Ein Beispiel hierfür ist die in [11] durchgeführte automatische Erkennung von typischen Verkehrsstrukturen sowie die Erkennung von plötzlichen Veränderungen dieser Strukturen. Diese Anwendung kann sowohl als Anomalieerkennung dem Bereich der Intrusion-Detection als auch dem Bereich des Netzwerkmanagements zugeordnet werden.

3 Routing und Packet-Sniffing in MANETs

Es werden im weiteren einige Routing-Protokolle für MANETs grundlegend beschrieben und die Auswirkungen der MANET-Eigenschaften auf das Packet-Sniffing erläutert. Anschließend werden Anwendungsfälle geschildert, bei denen das Packet-Sniffing als Sicherheitswerkzeug in MANETs eingesetzt wird.

3.1 Routing-Protokolle

Im Folgenden werden zwei unterschiedliche Herangehensweisen zum Routing in MANETs genannt.

- *Proaktive Routingprotokolle*
  Unter Verwendung der so genannten proaktiven Protokolle unterhält jeder Knoten eine Tabelle von Routen zu jeweils allen anderen Knoten des MANETs und aktualisiert diese Tabelle – meist in regelmäßigen Abständen – durch den Austausch entsprechender Management-Informationen. Der Bestimmung der jeweiligen Routen liegen die aus dem “klassischen” drahtgebundenen Routingprotokollen bekannten Techniken des Link State Routing bzw. des Distance Vector Routing zugrunde.

  Die bekanntesten Vertreter proaktiver Protokolle sind das Optimized Link State Routing (*OLSR* [6]) sowie das Destination-Sequenced Distance Vector Routing (*DSDV* [7]).

  Durch den Austausch von Management-Nachrichten ist generell von einem Kommunikationsoverhead auszugehen; der Vorteil besteht jedoch in der Tatsache, dass keine Verzögerungen durch Bestimmung einer Route vor dem Versand eines Paketes entstehen.
- *Reaktive Routingprotokolle*
  Bei reaktiven Protokollen werden die Routen, die ein Paket durch das Netzwerk nimmt, erst unmittelbar vor dem Versand bestimmt. Dies geschieht durch das so genannte *Fluten* (engl. Flooding) des Netzes mit Anfragenachrichten, bis der entsprechend vorgesehene Empfänger des Paketes unter Angabe des ermittelten Weges antwortet.

Zu den prominentesten Vertretern reaktiver Protokolle gehören Dynamic Source Routing (*DSR* [4]) sowie das Adhoc On-Demand Distance Vector Routing (*AODV* [5]).

Reaktive Protokolle besitzen keinen ständigen Kommunikationsoverhead; allerdings ist vor dem Versand eines neuen Paketes erst der Routenaufbau abzuwarten, was zu entsprechenden Verzögerungen führt.

Es sind auch hybride Verfahren bekannt, wie etwa das *Zone Routing Protocol* (ZRP [8]), bei dem jeder Knoten die Routen zu seinen unmittelbaren Nachbarn proaktiv verwaltet und nur Routen zu weiter entfernt liegenden Empfängern beim Paketversand ermittelt werden müssen.

3.2 Auswirkungen auf das Packet-Sniffing

Das für den hier beschriebenen Kontext wesentliche Charakteristikum eines MANETs ist die Tatsache, dass es keine definierten Orte im Netzwerk gibt, an dem der Fluss aller Netzpakete vollständig und verlässlich beobachtet werden kann. Wegen potentiell instabiler Funkverbindungen und vor dem Hintergrund potentiell hoher Mobilität der Knoten ist außerhalb des Netzwerkes nicht bekannt, welche Route ein Paket auf seinem Weg vom Sender zum Empfänger nimmt, sodass kein Hinweis auf die Stelle gegeben ist, an der ein Paket erfasst werden muss.

Damit müsste, um jederzeit eine vollständige Erfassung aller Netzwerkverbindungen zu garantieren, auf jedem einzelnen Netzwerkknoten eine entsprechende Sensoreinheit installiert sein. Dies ist aus zwei Gründen nicht praktikabel:

1. *Energie* (Promiscuous Mode)
   Da die Netzwerkpakete aller in der Empfangsreichweite befindlichen Knoten nur im o.g. Promiscuous Mode erfolgen kann, ist die Verwendung des Energiesparmodus eines WLAN-Funkadapters, der eine Abschaltung des Empfangs nach Lesen der IEEE 802.11-Präambel bewirkt, um Batteriekapazität zu sparen, nicht möglich. Der Energieaspekt beim System-Monitoring wurde bereits 2001 in einem Papier von Ko et al. [12] aufgeworfen.
2. *Überlappung* (Duplikate)
   Durch sich überlappende Empfangsreichweiten der einzelnen Knoten ist es sehr wahrscheinlich, dass Pakete von mehreren Knoten simultan erfasst werden. Auch ein erneutes Erfassen auf dem weiteren Weg des Paketes ist denkbar. Dies hätte zur Folge, dass die erfassten Netzwerkpakete bei der zentralen Sammlung von Duplikaten befreit werden müssten, was insbesondere vor dem Hintergrund der nur begrenzt exakten zeitlichen Synchronisierung der einzelnen Knoten eine aufwändige Aufgabe darstellt.

Wie von Anjum et al. [13] bereits 2003 diskutiert, stellen insbesondere reaktive Routing-Protokolle eine Hürde für die konventionelle Netzwerkbeobachtung dar. In dieser Arbeit wurden verschiedene Routingprotokolle (darunter DSDV, AODV und DSR) hinsichtlich der Wahrscheinlichkeit untersucht, dass ein durchgeführter Angriff durch Überwachung mit einem einzigen, zufällig ausgewählten MANET-Knoten erkannt werden kann.

3.3 Anwendung: Watchdog für Blackhole-Angriffe

Das so genannte Watchdog-Prinzip (vgl. [20], [19]) beschreibt ein auf Packet-Sniffing basierendes Verfahren in einer Multihop-Umgebung, um Knoten zu erkennen, die Pakete verwerfen oder deren Inhalt manipulieren. Hierzu zeichnet der Watchdog-Knoten die wesentlichen Eigenschaften der von ihm weitergegebenen Pakete auf und vergleicht diese mit denjenigen, die er von dem weiterleitenden Knoten bei der Weitergabe zum nächsten Knoten empfängt. Wird

innerhalb einer geeigneten Zeitspanne kein Paket mit Eigenschaften empfangen, das den zuvor aufgezeichneten entspricht, so wird dies unter Abwägung mit den potentiell vorhandenen Fehlerquellen (s.u.) mit einer gewissen Wahrscheinlichkeit als mutmaßlich nicht weitergeleitetes Paket interpretiert. Bei Überschreitung eines geeigneten Schwellwertes wird dieser Vorfall an die entsprechenden IDS-Komponenten gemeldet. Da diese Methode auf optimale Bedingungen (ausreichende Funkausbreitung mit geringen Interferenzen) angewiesen ist, die zwangläufig nicht immer gegeben sind, sollte das Verfahren mit weiteren Erkennungsmechanismen kombiniert werden.

Ein weiteres Beispiel (vgl. [18]) für eine Situation unter nicht optimalen Bedingungen stellt der Fall dar, in dem der weiterleitende Knoten das entsprechende Paket aufgrund von Energiesparoptionen mit geringerer Sendeleistung zum Empfänger leitet, so das der Watchdog-Knoten das Paket nicht mehr empfangen kann. Dies würde nach Überschreitung des Schwellwertes einen Alarm auslösen. Dieser Effekt lässt sich aber auch von einem Angreifer ausnutzen, indem er das Paket genau dann weiterleitet, wenn der Empfängerknoten sich in einem Sendevorgang befindet. Dadruch ist aus der Sicht des Watchdog-Knotens das Paket korrekt weitergeleitet, da dieser die Kollision der Pakete nicht bemerkt. Der Angreifer schickt in diesem Fall trotz Kollision das entsprechende Paket kein zweites mal. In einem weiteren Angriffszenario mit zwei kooperierenden Angreifern besteht die Möglichkeit, dass der erste Angreifer das weiterzuleitende Paket zum zweiten Angreifer sendet und dann dieser das Paket verwirft. Somit hat der Watchdog-Knoten den ersten Angreifer nicht detektiert, obwohl im zweiten Schritt das ursprüngliche Paket verworfen wurde.

3.4 Anwendung: Routing-Integritätsprüfung

Die Plausibilitätsprüfung von Routingpaketen ist ein weiteres sinnvolles Mittel zur Erkennung von Angreifern in einem MANET. Einen möglichen Angriffspunkt stellen beispielsweise die aus OLSR bekannten HELLO-Pakete dar, mit denen Links zu gefälschten oder praktisch nicht erreichtbaren Knoten vorgetäuscht werden. Damit verändert sich dann das Routing der anderen Knoten im Netz, womit verschiedenen Effekte (z.B. Blackhole) erzielt werden können.

Wie auch in [9] diskutiert, gibt es unterschiedliche Möglichkeiten, diese und andere Störungen in einem OLSR-Netz zu entdecken. Hierbei werden zum Beispiel die eintreffenden TC-Pakete auf plausible, d.H. topologisch mögliche Veränderungen im Sinne des Routings hin geprüft. Wenn ein Routing-Paket verschickt wird, welches eine Veränderung der Routing-Struktur verursacht, muss sich diese Tatsache in den darauf folgenden empfangenen Paketen widerspiegeln. Wenn dies nicht der Fall ist, kann hier möglicherweise ein Angriff stattgefunden haben. Auch ein Abgleich der Informationen aus HELLO- und TC-Paketen dient der Plausibilitätsüberprüfung der eingehenden Routing-Pakete. Ein anderer Ansatz der Absicherung gegen das Verändern der Routing-Paket ist die in [10] beschriebene Erweiterung um eine Kontroll-Nachricht, die ein authentifiziertes Antwortpaket veranlasst.

3.5 Sicherstellung der Netzüberdeckung im MANET

Anomalieerkennungen in MANETs stellen Verfahren dar, mit denen beispielsweise durch einen zentralen Ansatz Bedrohungen erkannt werden können. Das so genannte *Cluster Based Anomaly Detection* Verfahren (CBAD, vgl. [11]) wurde ursprünglich als Anomalieerkennung für kabelgebundene Netzwerke entworfen, bei der verschiedene statische Flussparameter der Verkehrsstruktur als Graph aufgezeichnet werden und signifikante Veränderungen dieser Struktur als potentieller Angriff gemeldet werden.

Routing-Angriffe gegen OLSR in MANETs stellen Bedrohungen dar, die beispielsweise durch einen zentralen Ansatz zur Anomalieerkennung, bei der die Topologie des Netzes als Graph dargestellt wird, erkannt werden können. Dieser zur Zeit in einem Forschungsprojekt untersuchte Ansatz wird als Topology-Graph based Anomaly Detection (TOGBAD) bezeichnet und stellt eine Erweiterung zu CBAD dar. Hierbei wird versucht manipulierte HELLO-Nachrichten zu detektieren, indem Plausibilitätstests auf einer zentralen Knoten-Instanz durchgeführt werden. Die Verwendung von TOGBAD und CBAD setzen voraus, dass eine netzüberdeckende Überwachung aller im MANET befindlichen Knoten vorhanden ist.

Wie von Subhadrabandhu et al. [14], [15] dargelegt, stellt die Bestimmung einer minimalen, das gesamte MANET überdeckenden Untermenge der Knoten zur Überwachung mittels eines NIDS ein NP-vollständiges Problem in der Anzahl der Überwachungsknoten dar. Die Autoren stellen als Lösung des genannten Problems zwei approximative Algorithmen vor, die die Auswahl der Überwachungsknoten in polynomieller Zeit vornehmen können. Diese vergleichen sie mit der o.g. optimalen Lösung und der zufälligen Wahl von Knoten. Der erste Algorithmus (*Greedy-MC*, “Gierige” Maximum Coverage) sieht zwischen allen Knoten des Netzes allerdings eine zusätzliche Kommunikation vor, während der zweite Algorithmus (*MUNEN-MC*, Maximum Unsatisfied Neighbours in Extended Neighbourhood) den zusätzlichen Nachrichtenverkehr nur innerhalb der Knotennachbarschaft voraussetzt. Darüber hinaus wird eine Heuristik vorgeschlagen, die sehr effizient arbeitet, aber auf geometrischen Annahmen (insbesondere einer kreisförmigen Funkausbreitung) basiert.

4 Verteilte Sensoren für MANET-Verkehrsstatistiken

Ein Ansatz, der sich die Eigenschaften eines proaktiven Routingprotokolls zu nutze macht, um eine Menge von netzüberdeckenden Überwachungsknoten zu bestimmen, wird in diesem Abschnitt dargestellt.

4.1 Szenario

Im hier betrachteten Fall geht man von einem MANET mit einer Knotenanzahl von 5-15 Knoten aus, in dem mobile Kleingeräte (High-Performance-PDAs bzw. Ultra-Mobile-PCs) miteinander infrastrukturlos vernetzt sind. Die Geräte stellen ihren Benutzern verschiedene Dienste (z.B. VoIP, Geo-Informationssystem) zur Verfügung. Da die mobilen Geräte über aufladbare Batterien betrieben werden, ist bei der Implementierung von Betriebsystemen wie Dienstprogrammen eine unnötige Belastung von CPU, Speicher sowie Übertragungsmedium zu vermeiden.

Trotz der genannten Einschränkungen bezüglich der zur Verfügung stehenden Ressourcen wird als Routing-Protokoll das proaktive OLSR eingesetzt.

4.2 Verwendung von MPRs als Überwachungsknoten

Wegen der Verwendung von OLSR erscheint es denkbar, die so genannten MPRs des OLSR-Protokolls für die Überwachung einzusetzen. Sie dienen zur effizienten Verteilung der Routing-Nachrichten im Netz und sollen ein Fluten des Netzes verhindern. Sie stellen im optimalen Fall eine minimale Überdeckung des Netzes bezüglich der Funkreichweite (Sende- und Empfangsüberdeckung) dar und würden somit auch die Filterung der Duplikate erleichtern.

Jeder Knoten wählt einen oder mehrere Knoten als ”seine” MPRs aus, von dem oder denen er weiß, dass diese Kontakte zu weiter Entfernten Knoten unterhälten. Im allgemeinen konvergiert

dieses Verfahren recht schnell und benötigt keine aufwändigen Rechen- oder Speicheroperationen, um den gewünschten Effekt zu erzielen.

Zwar setzt die im Folgenden vorgestellte Verfahrensweise auf OLSR auf; der Einsatz des Verfahrens ist jedoch bei jedem proaktiven sowie hybriden MANET-Routingprotokoll möglich, das zur Verringerung von Flutungsvorgängen MPRs oder MPR-ähnliche Techniken verwendet. Bei reaktiven Protokollen sind den Knoten ihre jeweiligen Nachbarn a priori nicht bekannt, und so kann auch der beschriebene Ansatz nicht unmodifiziert eingesetzt werden.

4.3 Sonderfälle bei der Erfassung

Es gibt einige Sonderfälle, in denen das vorgestellte Konzept nicht problemlos anwendbar ist. In manchen Szenarien, in denen sich das mehrfache Erfassen der Pakete von zwei MPR-Knoten zwangsweise durch ihre Position ergibt (siehe Abb. 1).

Knoten A und B wurden als MPR gewählt. Die Knoten A, B und D befinden sich in einem gemeinsamen Funkradius und können direkt miteinander kommunizieren. Da nun aber Knoten A und B MPR und somit aufzeichnende Knoten sind, würden beide Knoten die Pakete verarbeiten, die von Knoten D gesendet werden.

Eine Lösungsmöglichkeit besteht darin, dass MPR-Knoten die Pakete verwerfen, die bereits von anderen MPR-Knoten in der direkten Nachbarschaft aufgezeichnet wurden. Dazu wird die Netztopologie aus dem OLSRd zu Hilfe genommen, um zu erkennen, welche anderen MPR-Knoten die gleichen Nachbarn aufweisen und dementsprechend auch identische Pakete aufzeichnen. Die Entscheidung, wer Pakete des Knotens aufzeichnet, der sich in der Funkreichweite von zwei oder mehr MPR-Knoten befindet, könnte an statischen Kriterien, wie zum Beispiel der Wertigkeit des letzten Blockes einer IP-Adresse, ausgemacht werden. Eine Regel für die Auswahl würde dann so aussehen: MPR_A (`10.0.0.1`) hat eine höhere Priorität als MPR_B (`10.0.0.2`) und wird zum Aufzeichnen der Duplikate ausgewählt.

Dieser Lösungsansatz könnte das Problem der doppelt aufgezeichneten Pakete deutlich reduzieren. Da allerdings dieses Verfahren auf den Daten des OLSRd aufbaut, diese aber aufgrund der Paketlaufzeiten nicht auf jedem Knoten im Netz und zu jeder Zeit synchron sind, tritt auch hier ein Problem auf. Es handelt sich um die Problematik der Zeitdifferenz zwischen MPR-Knoten-Auswahl und dem Aufzeichnungsbeginn der Pakete.

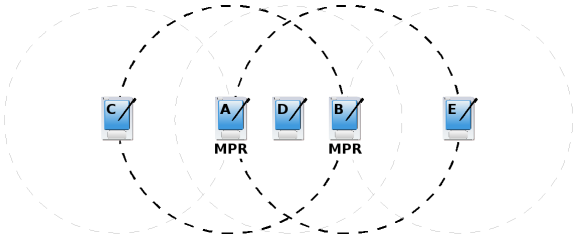

Abb. 1: Schematische Darstellung einer Situation, in der eine doppelte Paketaufzeichnung durch MPRs stattfindet

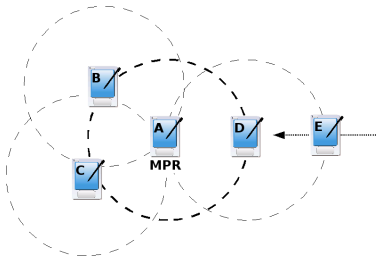

Abb. 2: Schematische Darstellung eines Paketverlustszenarios

In Abbildung 2 wird gezeigt, dass Knoten A von Knoten B, C und D als MPR ausgewählt wurde. Knoten E ist anfangs außerhalb der Reichweite aller Knoten, nähert sich aber Knoten D. Sobald Knoten D und E in Funkreichweite sind, wird auch Knoten D zum MPR. In der

Zeitdifferenz zwischen dem Erkennen des neuen Knotens E und dem Beginn der Aufzeichnung können Pakete verloren gehen, die von Knoten E ausgehen. Dieses Szenario wird hier nur rein theoretisch vorgestellt. Es ist bislang noch keine Aussage über die Häufigkeit des Auftretens solcher Situationen und damit dem Stellenwert des Problems getätigt. Hierzu sind weitergehende Simulationen unterschiedlicher Szenarien notwendig.

Die oben erwähnte Zeitdifferenz würde sich nur einschränken lassen, wenn die einzelnen Knoten die eingehenden Management-Pakete untersuchten, da über diese die Bekanntmachung ausgewählter MPR-Knoten stattfindet. Zwischen einer solchen Management-Paketauswertung und dem Beginn der Aufzeichnung können jedoch weiterhin Pakete verloren gehen. Diese Tatsache würde sich nur umgehen lassen, indem sämtliche Knoten Pakete aufzeichneten; dies ist aber hinsichtlich des Ressourcenaufwandes nicht erwünscht.

4.4 Implementierung und Funktionsweise eines Sensors auf Basis von OLSR

Im Folgenden wird die Arbeitsweise des konzipierten und realisierten Sensors für die verteilte Datenerfassung beschrieben. Hierbei ist zu erwähnen, dass die Sensoren auf den verschiedenen Knoten unabhängig voneinander, also ohne direkte Kommunikation miteinander, operieren.

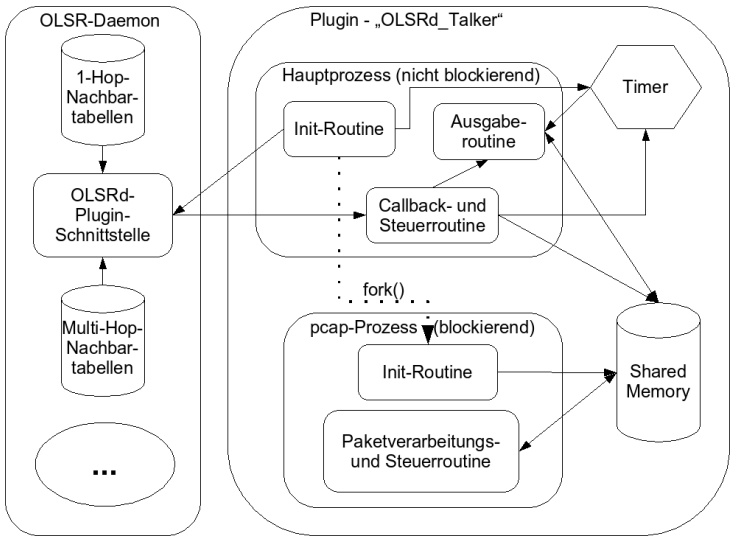

Abb. 3: Schematische Darstellung der Prozessstruktur des Sensors

Abbildung 3 zeigt neben dem OLSR-Daemon den groben Ablauf der Prozessstruktur des Sensors (Plugin). Die Initialisierungs-Routine des Hauptprozesses meldet das Plugin beim OLSRd an, registriert eine Callback-Routine und initialisiert den Timer. Die Callback- und Steuerroutine wird bei Änderungen in der Netztopologie aufgerufen. Sobald dem Knoten der MPR-Status zugewiesen wird (siehe Abschnitt 4.2), welches er wiederum aus den Topologiedaten entnehmen kann, weist der Hauptprozess den Nebenprozess (pcap-Prozess) an, mit der Paketaufzeichnung zu beginnen. Wenn dies geschehen ist, werden die Datenpakete auf Sonderfälle hin überprüft (siehe Abschnitt 4.3) und in den internen Datenstrukturen für das spätere Versenden abgelegt. Außerdem wird mit Hilfe der durch den Timer in vorgegebenen Zeitintervalle (vergl. [23]) eine Übertragung der Verbindungsstatistiken samt Topologiedaten zu den zentralen IDS-Komponenten veranlasst.

Die Absicherung der Informationspakete kann beispielsweise zukünftig mit einem symmetrischen Verschlüsselungsverfahren, wie es in Version 3 von SNMP (siehe [25]) zu finden ist, sichergestellt werden. Ein weiterer möglicher Ansatz zur Absicherung ist der Einsatz einer so genannten *Plausible-deniability*-Technik (glaubwürdiges Abstreiten), deren Eigenschaften sich *TrueCrypt* (siehe [24]), ein freies Open-Source-Programm zur Verschlüsselung von Festplatten, zu nutze macht. Ein besonderes Sicherheitsmerkmal von TrueCrypt ist die Eigenschaft, dass es einen äußeren und inneren Container für die Datenhaltung verwenden kann. Wird der Besitzer eines Knotens beispielsweise psychisch oder physisch bedroht und gezwungen, sich gegenüber dem System zu authentizieren, so gewährt er nur Zugang in den äußeren Container. Der versteckte und mit anderen Authentifikationsmerkmalen geschützte innere Container, welcher in diesem Fall die Informationspakete selbst wären, bleibt unentdeckt. Weitere Details der Implementierung der Sensorik finden sich in [16].

5 Testumgebung und Testergebnisse

Für die durchgeführten Tests am Sensor wurde eine spezielle Testumgebung aufgebaut, die aus einer Kombination von realen und virtuellen Knoten besteht. Sie verfügt über eine automatisierte Emulation von Bewegungseffekten auf das Netz unter Berücksichtigung eines beliebigen Funkausbreitungsmodells und vordefinierter Bewegungsdaten. Es können dadurch reproduzierbare Änderungen in der Netztopologie dargestellt werden und zudem über entsprechende Schnittstellen den laufenden Anwendungen (z.B. Navigationskomponenten) synchrone Geokoordinaten zur Verfügung gestellt werden. Außerdem wurden zwei Knoten mit einem Crossoverkabel verbunden, um so zeitlich exakte Messergebnisse zu erhalten. Die auftretenden Steuerbefehle der Testprogramme konnten über das drahtgebundene Netz versandt werden und haben das Funkmedium somit nicht belastet.

Mithilfe des Paket-Generators [21] aus dem Netzwerk-Subsystem des Linux-Systemkerns, wurden bei diesem Test UDP-Pakete ohne Nutzdaten mit stetig steigendem Ziel-Port im LAN verschickt. Um zudem einen genauen Überblick über die verschickten Pakete und den darauf wirklich gezählten Verbindungen zu erlangen, wurden mit Hilfe des Tools „netcat“ [17] alle verwendeten Ports zum Empfang geöffnet, da sonst jedes UDP-Paket, welches an einen nicht verwendeten Port gesendet wird, eine ICMP-Meldung auslöst. Bei einer Übertragungsrate von 2500 Pkt/s wurde die Verarbeitungsgeschwindigkeit des Sensors getestet. In der Abbildung 4 ist zu erkennen, dass der Sensor erst ab ca. 4000 Verbindungen mit der Verarbeitung aller neu eintreffenden Verbindungen überfordert ist und diese somit teilweise verwirft. Eine wesentliche Ursache ist die nicht optimierte, lineare Datenhaltung der Verbindungsstatistikpakete im Speicher. Hier liegt Potential für weitere Verbesserungen der Leistungsfähigkeit des Sensors.

Weiterhin wurde das in Abschnitt 4.3 beschriebene Problem der zeitlichen Differenz zwischen MPR-Knoten-Auswahl und dem Aufzeichnungsbeginn näher untersucht. Hierzu wurde ein Szenario gewählt, in dem einem bestimmten Knoten der MPR-Status manuell zugewiesen werden kann. Während der Tests wurden parallel zu der Paketaufzeichnung im OLSRd-Plugin alle Pakete in einem weiteren Programm (Wireshark, [22]) aufgezeichnet. Anschließend wurden Datenpakete mit unterschiedlichen Intervallen verschickt. Zur eindeutigen Bestimmung der verlorenen Pakete wurde die fortlaufende so genannte IP-Identifikationsnummer verwendet. Hierzu wurden nach der Testdurchführung die Log-Dateien des OLSRd-Plugins mit der Wireshark-Aufnahme verglichen, um so nach der MPR-Auswahl des Knotens durch die HELLO-Pakete die Anzahl der nicht aufgezeichneten Pakete zu bestimmen. Das Ergebnis ist in Abbildung 5

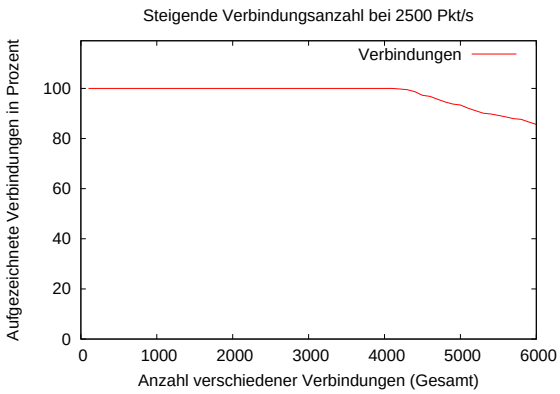

Abb. 4: Paketverluste bei hoher Verbindungsanzahl

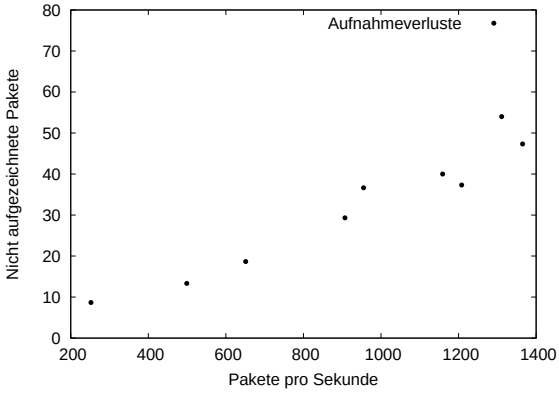

Abb. 5: Aufnahmeverluste durch verzögerte MPR-Knotenerkennung

dargestellt. Hier ist zu erkennen, dass mit ansteigender Paketanzahl pro Sekunde auch die Aufzeichnungsverluste ansteigen. Diese und weitere Aspekte werden in [16] näher ausgeführt.

6 Diskussion

Unter Verwendung eines Routing-Protokolls, das über einen MPR-Mechanismus verfügt, ist der Nutzen des hier vorgestellten Verfahrens zur verteilten Verkehrsstatistikerfassung in MANETs vor allem bei der Einsparung von Batterieleistung zu sehen. Die Verwendung der in Abschnitt 3.5 genannten Ansätze würde eine erhebliche Redundanz in den Management-Prozess einbringen und somit die Batterie über Gebühr belasten.

Um sowohl eine höhere Reduktion des Batterieverbrauches, als auch eine größere Detektierbarkeit von Angriffen zu ermöglichen, wird derzeit ein rollenbasiertes Sicherheitsmodell analysiert. Hierbei übernimmt jeder Knoten z.B. zu randomisierten Zeiten andere Überwachungsaufgaben. Dadurch kommt es zum einen zusätzlich zur Energieeinsparung und zum anderen wird es einem Angreifer erschwert, zu bemerken, wer ihn momentan überwacht. Davon unbeeinträchtig muss die Verkehrsstatistikerfassung sein, da diese zu jederzeit vollständig benötigt wird.

Verfahren, die auf geometrischen Annahmen bezüglich der Funkausbreitung basieren, können darüber hinaus in realen Umgebungen auf Schwierigkeiten stoßen, etwa durch Dämpfung, Reflexion und Beugung. Diese Schwierigkeiten können durch einen steigenden Grad an Mobilität noch einmal verstärkt werden. Daher basiert der vorgestellt Ansatz auf der Nutzung der MPRs, wodurch zwar eine Minimalität an Sensor Knoten nicht gegeben ist, wohl aber eine vollständige Abdeckung des Netzes erreicht wird.

Ein nicht zu vernachlässigender Nachteil des MPR-Ansatzes besteht in den Sonderfällen, die bei bestimmten Konfigurationen bezüglich der relativen Positionen und der Funkausbreitung entstehen können. Insbesondere bei plötzlichen Topologieänderungen kann beispielsweise der Fall eintreten, dass mehrere Knoten als MPR von einem weiteren ausgewählt wurden, sodass für einen gewissen Zeitraum Duplikate nicht zu vermeiden sind.

Einigen dieser Sonderfälle kann man durch pragmatische Methoden begegnen, so etwa die A-Posteriori-Elimination von Duplikaten an zentraler Stelle, sofern der Auswerteeinheit außer den Paketen die MPR-Rollen zum jeweiligen Erfassungszeitpunkt bekannt sind.

7 Zusammenfassung und Ausblick

Das vorliegende Papier stellte die Grundlagen und Einsatzbereiche des so genannten Packet-Sniffing in Rechnernetzen vor. Häufig eingesetzte Bibliotheken wurden ebenso beschrieben wie Anwendungen, die davon Gebrauch machen. Darauf folgend wurden die Grundzüge von mobilen Adhoc-Netzwerken (MANETs) unter besonderer Berücksichtigung der dort verwendeten Routing-Protokolle vorgestellt. Der typische Aufbau von Adhoc-Netzen erschwert die umfassende Sammlung von versendeten Datenpaketen zum Zwecke der Netzwerküberwachung und Problemerkennung erheblich.

Nachdem einige existierende Arbeiten zur Lösung der durch den Einsatz in MANETs entstehenden Herausforderungen vorgestellt wurden, folgte die Präsentation eines Ansatzes, der sich bestimmte Mechanismen so genannter proaktiver Routingprotokolle zu Eigen macht. Diese Verfahren besitzen dynamisch bestimmte, herausgehobene Knoten (MPRs), deren eigentlicher Zweck die effiziente Verteilung von Informationen an alle Teilnehmer des Netzes ist, ohne dass alle Knoten die Nachricht durch Fluten weiterleiten müssen. Die dazu notwendige Überdeckung des gesamten Netzes kann im Gegenzug auch zu einer Überwachung aller Netzteilnehmer genutzt werden.

Dieser Ansatz wurde implementiert und untersucht. Auftretende Probleme durch Nicht- oder Mehrfacherfassung einzelner Datenpakete wurden vorgestellt und Lösungsansätze dazu aufgezeigt. Zu den anstehenden Arbeiten bei der Weiterentwicklug der Sensorik zählt die Abstraktion vom verwendeten Routingprotokoll durch Verwendung festgelegter Schnittstellen. Eine weitere Beurteilung zur Weiterentwicklung der Verfahren folgt durch den Einsatz in Adhoc-Testnetzen, sowohl im praktischen Einsatz als auch zur reproduzierbaren Untersuchung besonderer Szenarien durch eine Bewegungsemulation der dem Adhoc-Netz zugehörigen Geräte.

Literatur

[1] Libpcap - Packet Capture Library - Libpcap. http://www.tcpdump.org/.

[2] M. Roesch. *Snort – Lightweight Intrusion Detection for Networks.* In: Proc. of USENIX LISA ’99 conference, 1999.

[3] S. Waldbusser. *Remote Network Monitoring Management Information Base.* RFC2819, 2000.

[4] D. Johnson, D. Maltz, Y. Hu. *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR).* Internet Draft, 2003.

[5] C. Perkins, E. Belding-Royer, S. Das. *Ad hoc On-Demand Distance Vector (AODV) Routing.* RFC3561, 2003.

[6] T. Clausen, P. Jacquet. *Optimized Link State Routing Protocol (OLSR).* RFC3626, 2003.

[7] C. Perkins, P. Bhagwat. *Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers.* In: Proc. of the conference on Communications architectures, protocols and applications (SIGCOMM’94), London, UK, 1994.

[8] Z. Haas, M. Pearlman, P. Samar. *The Zone Routing Protocol (ZRP) for Ad Hoc Networks.* IETF Internet Draft, http://www.ietf.org/proceedings/02nov/I-D/draft-ietf-manet-zone-zrp-04.txt, 2002.

[9] D. Dhillon, J. Zhu, J. Richards, T. Randhawa. *Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs.* In: Proc. of International Conference On Communications And Mobile Computing, Canada, 2006.

[10] F. Hong, L. Hong, C. Fu. *Secure OLSR.* In: Proc. 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1, Califonia, USA, 2005.

[11] J. Tölle, C. de Waal. *A Simple Traffic Model Using Graph Clustering For Anomaly Detection.* In: Proc. of Applied Simulation and Modelling (ASM) Crete, Greece, 2002.

[12] C. Ko, P. Brutch, J. Rowe, G. Tsafnat, K. Levitt. *System Health and Intrusion Monitoring Using a Hierarchy of Constraints.* In: Proc. of the Conference on Recent Advances in Intrusion Detection (RAID), 2001.

[13] F. Anjum, D. Subhadrabandhu, S. Sarkar. *Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols.* In: Proc. of IEEE Vehicular Technology Conference (VTC), 2003.

[14] D. Subhadrabandhu, S. Sarkar, F. Anjum. *A Framework for Misuse Detection in Ad Hoc Networks – Part I.* In: IEEE Journal on Selected Areas Of Communication, 2006.

[15] D. Subhadrabandhu, S. Sarkar, F. Anjum. *A Framework for Misuse Detection in Ad Hoc Networks – Part II.* In: IEEE Journal on Selected Areas Of Communication, 2006.

[16] A. Wenzel. *Sensorik für Intrusion-Detection Systeme in mobilen Ad-Hoc-Netzwerken.* Diplomarbeit, Fachhochschule Köln, Campus Gummersbach, Institut für Informatik, 2006.

[17] The GNU Netcat – Official homepage. http://netcat.sourceforge.net/

[18] D. Djenouri, N. Badache. *New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks.* In: Security and Privacy for Emerging Areas in Communication Networks, 2005.

[19] F. Kargl, A. Klenk, S. Schlott, M. Weber. *Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks* In: Proc. of 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004). Springer Lecture Notes in Computer Science, Heidelberg, 2004.

[20] S. Marti, T.J. Giuli, K. Lai, M. Baker. *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks.* In: Proc. of MOBICOM 2000, August 2000.

[21] Linux Packet Generator Howto. http://linux-net.osdl.org/index.php/Pktgen

[22] Wireshark – The world's most popular network protocol analyzer. http://www.wireshark.org/

[23] S. Lettgen. *Simulation und Bewertung einer ressourcenschonenden Intrusion-Detection-System-Architektur für Mobile Ad-Hoc Netze.* Diplomarbeit, Universität Bonn, Informatik IV, 2006.

[24] TrueCrypt, Free open-source disk encryption software for Windows Vista/XP/2000 and Linux http://www.truecrypt.org/

[25] J. Case, R. Mundy, D. Partain, B. Stewart. *Introduction and Applicability Statements for Internet-Standard Management Framework.* RFC3410, 2002.