Sicherheit in Mobilen Ad-hoc Netzwerken

Frank Kargl
Abteilung Medieninformatik
Universität Ulm

Abstract: In jüngster Zeit entwickeln Forscher in aller Welt eine Vision von Netzwerken, welche anders aufgebaut sind als bisherige drahtlose Netze. So genannte Mobile Ad-Hoc Netzwerke (MANETs) sind vollkommen dezentral aufgebaut und kommen ohne feste Infrastruktur aus. Damit ermöglichen sie den Einsatz an Orten oder in Situationen, in denen der vorherige Aufbau einer Infrastruktur zur Vernetzung von Computern oder anderen elektronischen Geräten nicht möglich oder wünschenswert ist.

Während der Aufbau solcher MANETs bereits recht gut verstanden ist, wurde ein Aspekt bisher eher vernachlässigt: der Schutz der entstehenden Netzwerke und seiner Teilnehmer vor den vielfältigen Angriffen, die hier möglich sind. So können Knoten beispielsweise den Routingprozess empfindlich stören oder Knoten können schlicht die Kooperation im Netz verweigern. Im Vergleich zu klassischen Netzwerken ermöglicht die Selbstorganisation also einige weitergehende Angriffe, so dass hier auch zusätzliche Schutzmaßnahmen nötig werden.

Im Rahmen meiner Dissertation habe ich die besonderen Sicherheitsprobleme bei MANETs analysiert und eine integrierte Sicherheitsarchitektur für Mobile Ad-hoc Netzwerke mit dem Namen „*SAM*“ entwickelt.

1 Einleitung

Klassische Netzwerke zur Funkkommunikation wie das *Global System for Mobile Communication* (*GSM*) oder *IEEE 802.11 Wireless LAN* benötigen meist eine mehr oder weniger umfangreiche Infrastruktur im Hintergrund.

In jüngster Zeit entwickeln Forscher in aller Welt jedoch eine Vision von Netzwerken, welche ganz anders aufgebaut sind. So genannte *Mobile Ad-hoc Netzwerke (MANETs)* sind vollkommen dezentral organisiert. Es gibt keine ausgezeichneten Knoten, deren Ausfall das Netzwerk zum Stillstand bringen könnte. Damit ermöglichen MANETs den Einsatz an Orten oder in Situationen, in denen der vorherige Aufbau einer Infrastruktur zur Vernetzung von Computern oder anderen elektronischen Geräten nicht möglich oder wünschenswert ist. Typische Beispiele sind Besprechungen, in denen die Notebooks der Teilnehmer vernetzt werden sollen, Einsätze von Rettungskräften in Katastrophengebieten, militärische Einheiten auf dem Schlachtfeld oder fahrende Pkws auf einer Autobahn. Zwangsläufig ergeben sich hieraus auch neue Formen von Anwendungen, welche diese spontan gebildeten Netze nutzen.

Eine zentrale Fragestellung bei Ad-hoc Netzen ist die Wegefindung. Jeder Knoten leitet

Datenpakete für andere Knoten an entferntere weiter. Hierzu muss aber die Netzwerktopologie bekannt sein (entweder in jedem Knoten oder verteilt im Netz). Zur Topologieerkennung wird ein Routingprotokoll eingesetzt. Eines der bekanntesten, auf welchem ich auch im Rahmen meiner Arbeit aufgebaut habe, ist das *Dynamic Source Routing* Protokoll (*DSR*). Die (vereinfachte) Funktionsweise: jeder Knoten, der ein Datenpaket zu einem anderen Knoten versenden will, zu dem er noch keine Route kennt, flutet einen *Route Request* im Netz. Jeder Knoten, der den Route Request weiterleitet, hängt seine eigene Adresse an eine Wegeliste an, die im Paket mitgeführt wird. Erreicht ein Route Request den Zielknoten, so schickt dieser entlang der Wegeliste einen *Route Reply* an den Ursprungsknoten zurück. Aus dem Route Reply ersieht dieser den Weg zum Ziel, den er für weitere Datenpakete verwenden kann. Hierzu wird die Wegeliste jedem Datenpaket als *Source Route* beigefügt.

In [KRSW03] ist eine Anwendung von MANETs dargestellt, bei der sich Mobiltelefone mittels Bluetooth-Funk unter Verwendung eines anderen Routing-Protokolls (dem *Bluetooth Scatternet Routing* (*BSR*)) selbständig zu einem Netz zusammenschließen, so dass beispielsweise zwei Teilnehmer in einem Bürogebäude unter Nutzung dazwischenliegender Mobiltelefone ein Gespräch führen können, ohne hierzu einen Mobilfunkprovider in Anspruch nehmen zu müssen.

Bisher konzentrierten sich die Anstrengungen primär auf die Entwicklung geeigneter Routingprotokolle, welche die Verkehrslenkung in MANETs organisieren. Zu den Neuerungen gehören Protokolle, die erst bei Bedarf (on-demand) tätig werden, oder solche, welche die geographische Position oder die Signalstärke mit in Betracht ziehen. Für weitere Informationen zu Ad-hoc Routing sei auf die einschlägige Literatur verwiesen (z.B. [Pe01]).

Ein Aspekt, der bisher nur teilweise untersucht wurde, ist die Absicherung solcher Netze. Dabei treten eine Reihe von neuen Fragestellungen auf, die ich im Rahmen meiner Arbeit behandelt habe:

- Wie werden Knoten oder deren Benutzer identifiziert? Wie wird das Vertrauen in solchen Netzen organisiert, wenn sich die Teilnehmer zu Anfang nicht kennen und auch kein vertrauenswürdiger Dritter online verfügbar ist? Wie geschieht die Authentisierung von Knoten oder Benutzern?
- Können Knoten oder deren Benutzer genau lokalisiert werden? Lassen sich Bewegungsprofile erstellen? Wie kann man dies verhindern?
- Wenn alle Knoten gleichzeitig auch Router sind, tragen auch alle Knoten zum Topologieaufbau und zur Routenfindung bei. Wie kann man verhindern, dass böswillige Knoten diesen Prozess stören und somit die Funktionsfähigkeit des Netzwerks beeinträchtigen?
- Wie geht man mit egoistischen Knoten um, welche zwar die Leistung des MANETs nutzen, selbst aber nicht bereit sind, zum Aufbau des Netzes eigene Ressourcen beizutragen?
- Können die Sicherheitsmechanismen den dynamischen Strukturen im MANET Rechnung tragen und sich daran anpassen? Lassen sich die Sicherheitsmechanismen auch

auf stark ressourcenbeschränkten Geräten wie PDAs oder Mobiltelefonen betreiben?

Wegen der besonderen Struktur von MANETs lassen sich die Security Lösungen aus dem Bereich herkömmlicher Netze nicht einfach auf MANETs übertragen. So wird eine klassische „Public Key Infrastructure“ (PKI) Lösung in MANETs nicht ohne weiteres funktionieren, da zentrale „Certification Authority“ (CA) Server meist nicht online erreichbar sind. Auch kann man Router nicht einfach durch „Message Authentication Codes“ (MAC) vor den normalen Knoten schützen, wie dies im Internet Üblich ist - in einem MANET ist jeder Knoten gleichzeitig auch Router.

Im obigen Telefoniebeispiel will ein Anwender beispielsweise nicht, dass einer der Zwischenknoten das Gespräch abhört oder manipuliert. Natürlich kann man die Sprachdaten verschlüsseln. Da jedoch beliebige Anwender miteinander kommunizieren, die sich eventuell nie vorher gesehen haben und auch ein Zugriff auf PKI Server nicht möglich ist, ist die Authentifizierung der Knoten schwierig, was Man-in-the-Middle Angriffe erleichtert.

Neben bösartigen Knoten (*Malicious Nodes*), die das Netz aus Eigeninteresse schädigen wollen, haben alle Knoten auch eine starke Motivationen, sich nicht an der gemeinsamen Routing-Infrastruktur zu beteiligen, um eigene Ressourcen zu schonen. In einem MANET erbringen alle Knoten gemeinsam eine Leistung, von der wiederum alle profitieren. Das Ergebnis dieser Leistung ist die Konnektivität, zu welcher alle beitragen und die alle benutzen. Dabei wendet ein Knoten einen Teil seiner Ressourcen (CPU, Bandbreite, Batterie) auf, um den Verkehr von anderen weiterzuleiten, immer in der Hoffnung, dass diese einen Teil ihrer Ressourcen dazu aufwenden, seine Datenpakete zu transportieren. Die Verlockung ist natürlich groß, die eigenen Aufwendungen für andere Knoten einzusparen, d.h. selbst keine Datenpakete weiterzuleiten, die Leistung der anderen Knoten für den Datentransport aber in Anspruch zu nehmen. Derart unkooperative Knoten werden als *egoistische Knoten* bezeichnet.

Bezogen auf das Telefoniebeispiel werden viele Besitzer von Mobiltelefonen nach Wegen suchen, um einerseits via Bluetooth kostengünstig telefonieren zu können und andererseits möglichst wenig fremden Verkehr weiterleiten zu müssen, da dieser Vorgang insbesondere die eigene Batterielebensdauer stark verkürzen kann.

Vor dem Hintergrund des bisher Gesagten ist es leicht einzusehen, dass eine Absicherung von Ad-hoc Netzen absolut notwendig ist. Vor der Entwicklung konkreter Sicherheitsmechanismen steht jedoch zwingend eine strukturierte Analyse der möglichen Angriffen, gegen welche man sich schützen will.

2 Angriffsanalyse

Ausgangspunkt für die Erstellung einer Sicherheitsinfrastruktur sollte immer die Analyse möglicher Angriffe sein. Ich greife hier auf die von Bruce Schneier in [Sc99] vorgestellten *Attack Trees* (Angriffsbäume) zurück. Ausgehend von einem Ziel bzw. einer Motivation wird ein hierarchischer Baum mit Wegen aufgestellt, wie das Ziel eines Angriffs zu er-

Baum A: Ressourcen einsparen
OR 1. Keine Teilnahme am Routing
OR 1. Keine Weiterleitung von Routing-Daten
OR 1. Route Request nicht weiterleiten
2. Route Reply nicht weiterleiten
3. Hop-Limit/TTL in Route Request/Reply auf 0 (bzw. kleinen Wert) setzen
2. Routing Daten modifizieren
OR 1. Topologie modifizieren
OR 1. Route Request fälschen
OR 1. Zusätzliche Hops in Route Request einbauen (Tunneling Attack)
2. Route Reply fälschen
OR 1. Eigene ID im RREP durch Umleitung über benachbarte Knoten ersetzen
OR 1. ...

Tabelle 1: Angriffsbaum A: Ressourcen einsparen

reichen ist. Daraus lässt sich umgekehrt sehr schön ableiten, welche Angriffe durch eine Schutzmaßnahme unterbunden werden.

Tabelle 1 zeigt beispielhaft einen Ausschnitt aus einem solchen Angriffsbaum, der Möglichkeiten aufzeigt, wie ein egoistischer Knoten in einem auf dem DSR Protokoll basierenden Ad-hoc Netzwerk eigene Ressourcen auf Kosten anderer einsparen kann. So könnte er beispielsweise gemäß A.1.2.1.2.1 die durch ihn laufenden Route-Requests so modifizieren, dass die Route um ihn herum führt. Er müsste dann keinen Datenverkehr weiterleiten und hätte sein Ziel („Ressourcen einsparen“) erreicht.

Ich habe entsprechende Angriffsbäume für diverse Angriffsformen erstellt, die hier aus Platzgründen nicht dargestellt werden können. Für einen kompletten Überblick siehe [Ka03, KSW+04]. Durch die Analyse dieser Bäume gewinnt man sehr schnell einen Eindruck der Schwächen und Verwundbarkeiten der Protokolle.

Wie stark wirkt sich aber die Anwesenheit von egoistischen oder böswilligen Knoten in einem Ad-hoc Netzwerk auf dessen Leistungsfähigkeit aus? Um den Einfluss auf ungeschützte Netzwerke zu analysieren, habe ich mit dem Simulationstool ns-2 eine Reihe von Simulationen durchgeführt, welche diese Effekte veranschaulichen sollen. Ein kurzer Ausschnitt dieser Ergebnisse wird im Folgenden wiedergegeben.

Die Implementierung des DSR Routing Protokolls in ns-2 (Version 2.1b8) wurde derart modifiziert, dass eine frei wählbare Anzahl von Knoten ein bestimmtes egoistisches oder böswilliges Verhalten zeigt. Für die vollständigen Ergebnisse und genauen Simulationsparameter siehe [Ka03, KK+04].

Als typische Vertreter von egoistischen Knoten wurden zwei verschiedene Arten modelliert. Der Knoten vom Typ *Egoistisch-1* leitet gar keine Pakete weiter, d.h. sowohl Kontrollpakete (Route-Requests) als auch Datenpakete werden verworfen. In der Praxis reicht

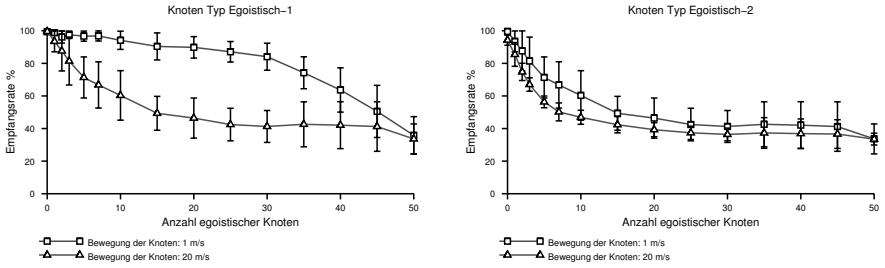

Abbildung 1: Simulation egoistischer Knoten

es hier, Route-Requests zu verwerfen, da dann keine gültigen Routen durch diesen Knoten zu Stande kommen und er somit auch nicht zur Weiterleitung von Verkehr herangezogen wird. Der Knoten generiert allerdings selbst ungehindert Verkehr, wie jeder andere Knoten im Netz. Knoten vom Typ *Egoistisch-2* nehmen zwar ganz normal am Routing-Betrieb teil, d.h. sie können auch Bestandteil einer Source-Route werden, allerdings weigern sie sich, normalen Datenverkehr weiterzuleiten. Es wurden jeweils Simulationen mit Knotengeschwindigkeiten von $1\frac{m}{s}$ und $20\frac{m}{s}$ durchgeführt, um die Auswirkung der Mobilität auf die Ergebnisse zu erfassen. Abbildung1 gibt die Ergebnisse der Simulationen wieder.

Wie man sieht vermindert die Anwesenheit von egoistischen Knoten die Wahrscheinlichkeit, dass Datenpakete das Ziel erreichen, deutlich.

3 Verwandte Arbeiten

Arbeiten zur Sicherheit von Mobilen Ad-hoc Netzen lassen sich grob in drei Kategorien einteilen: *„Authentifizierung und Schlüsselaustausch“* [ZH99, AG00, HBČ01], *„Sicheres Routing“* [PH02, PH03, HPJ02, HJP02, SDL$^+$02, Gu02] und *„Erkennung und Verhinderung egoistischer Knoten“* [MGLB00, ZL00, BB02, MM]. Eine umfassende Literaturliste zu Sicherheit in Ad-hoc Netzwerken findet sich in [Zh].

Ein grundlegendes Problem all dieser Arbeiten ist die fehlende Integration der verschiedenen Teilbereiche. So setzen beispielsweise sichere Routingprotokolle wie SAODV [Gu02] oder *Intrusion Detection Systeme* für Ad-hoc Netze wie CORE [MM] oft voraus, dass kryptographische Schlüssel zwischen den beteiligten Parteien vereinbart wurden. Wie dies ohne existierende Routen effizient geschehen soll, bleibt offen. Umgekehrt gehen Authentifizierungslösungen wie in [HBČ01] meist davon aus, dass eine funktionierende Routing-Infrastruktur zwischen den Knoten existiert, über welche das Authentifizierungsprotokoll ablaufen kann. Weiter setzen Systeme zur Erkennung egoistischer Knoten wie CORE [MM] implizit voraus, dass Knoten über eine eindeutige Identität verfügen und nicht unter beliebig vielen selbst-generierten Identitäten aktiv werden können. Sichere Routingprotokolle gehen von ähnlichen Annahmen aus.

Ein Thema, welches bisher noch gar nicht berücksichtigt wurde, ist die Möglichkeit der Erstellung von Bewegungsprofilen in Ad-hoc Netzen. Wie in [ČHH02] gezeigt, können Knoten in MANETs unter Umständen recht genau lokalisiert werden. Eine Sicherheitsinfrastruktur sollte Mechanismen enthalten, welche die Privatsphäre der Teilnehmer schützt.

Schließlich definieren viele Authentifizierungslösungen für Ad-hoc Netze nicht klar, was unter einer Identität eines Knotens oder Benutzers eigentlich zu verstehen ist. Damit bleibt dann aber unklar, was eigentlich authentifiziert wird.

4 SAM

Während die bisherigen Ansätze und Projekte also immer nur einen Teil der Sicherheitsprobleme von Ad-hoc Netzwerken adressieren, ging meine Dissertation einen anderen Weg und entwarf eine komplette *Sicherheitsarchitektur für Mobile Ad-hoc Netzwerke* (kurz *SAM* [Ka03, KSW+04]). Ausgehend von der durchgeführten Sicherheitsanalyse wurde dabei eine in den Teilkomponenten aufeinander abgestimmte Sicherheitslösung für Mobile Ad-hoc Netzwerke entwickelt, welche die oben aufgezeigten Abhängigkeiten berücksichtigt. Dabei konnten stellenweise existierende Ideen aus bestehenden Arbeiten aufgegriffen und modifiziert werden, teilweise mussten jedoch auch neue Ansätze entwickelt werden.

SAM besteht aus verschiedenen Teilkomponenten, welche jeweils in ihren Abhängigkeiten genau beschrieben sind. Eine ausführliche Beschreibung aller Komponenten würde den Rahmen dieses Beitrags sprengen, der interessierte Leser sei auf [Ka03] verwiesen. Im Folgenden werden die einzelnen Teile kurz beschrieben, anschließend soll exemplarisch die Funktionsweise des sicheren Routingprotokolls SDSR detailliert vorgestellt werden.

MANET-IDs: Diese Komponente widmet sich der Fragestellung, wie Knoten im Ad-hoc Netz eindeutig zu identifizieren sind. Breiten Raum nimmt dabei die Frage ein, was eigentlich eine Identität in einem Ad-hoc Netz auszeichnet und wie diese beschaffen sein muss, um als Ausgangsbasis für eine Sicherheitsarchitektur dienen zu können. Dieser Punkt wurde in früheren Arbeiten stets vernachlässigt. MANET-IDs sind ein System zur Identifizierung von Geräten, welches auch ohne ständigen Kontakt zu einer zentralen Infrastruktur genutzt werden kann und welches über effiziente Mechanismen zum Rückruf und zur Sperrung von Identitäten verfügt. Diese werden vor allem vom später vorgestellten Mobile Intrusion Detection System genutzt. Der Authentifizierungsvorgang ist in den Route-Request/-Reply Vorgang des Routingprotokolls *SDSR* integriert. Gleichzeitig werden Sitzungsschlüssel mit allen an einer Route beteiligten Knoten ausgetauscht, welche für die Verschlüsselung der nachfolgenden Datenkommunikation und im Rahmen des IDS Systems *MobIDS* genutzt werden können. Weiterhin bieten MANET-IDs eine Unterstützung von *Pseudonymen*. Damit kann ein Benutzer oder Gerät im MANET seine Identität verschleiern, was den Wert von Bewegungsprofilen deutlich einschränkt.

Secure Dynamic Source Routing (SDSR): Diese Komponente erweitert das DSR Protokoll um die Fähigkeit, Modifikationen an den DSR-Nachrichten zu erkennen.

Gefälschte Nachrichten werden verworfen, eine Meldung an das IDS führt gegebenenfalls zum Ausschluss des Verursachers aus dem MANET. SDSR ist ein reaktives Protokoll, in dessen Routensuche die Authentifizierung aller an einer Route beteiligten Knoten sowie der Austausch von Sitzungsschlüsseln mit all diesen Routern integriert ist. Dies ist insbesondere die Voraussetzung für eine korrekte Funktion des MobIDS Systems.

MobIDS: Das „ *Mobile Intrusion Detection System*“ [KK$^+$04, KKSW04] dient der Erkennung und dem Ausschluss von fehlerhaften, egoistischen oder böswilligen Knoten aus dem Ad-hoc Netz. Hierzu greift es auf eine Reihe von *Sensoren* zurück, welche Auffälligkeiten im Verhalten eines Knotens bemerken. Die Sensoren liefern Meldungen an den *Bewerter*, welcher diese zu einer lokalen Bewertung zusammenführt. Anschließend verteilt der *Distributor* diese Information im Netz. Das *Ausschluss-System* sorgt dafür, dass Knoten mit einer negativen Bewertung nicht am Netz teilnehmen können. Dabei fließen auch Informationen des Routingprotokolls in den Bewertungsvorgang ein. Umgekehrt wird eine Ausschlussentscheidung durch das Routingprotokoll umgesetzt, indem ausgeschlossene Knoten keine neuen Routen mehr aufbauen dürfen.

5 Secure Dynamic Source Routing

Im Rahmen meiner Arbeit wurde auf Basis des DSR Protokolls das SDSR Protokoll entwickelt. SDSR ist wie DSR ein *reaktives* Protokoll, welches mit *Source-Routen* arbeitet. Will ein Knoten S ein Datenpaket P an einen anderen Knoten D schicken und besitzt keine gültige Route zu D, so initiiert er eine *Routensuche* (*Route Discovery*). Die Route Discovery gliedert sich in zwei Phasen. In der ersten Phase wird ein *Route Request* im Netz geflutet. Erreicht ein solches *RREQ Paket* den Zielknoten, so schickt dieser ein *Route Reply (RREP) Paket* über die reverse Source Route zurück.

Während des Protokollablaufs werden Pakete mittels asymmetrischer Kryptographie signiert. Die hierzu notwendigen Schlüsselpaare sind Bestandteil der MANET-IDs. In diesem Rahmen kann die Authentizität von öffentlichen Schlüsseln verifiziert werden. SDSR beinhaltet ebenfalls Mechanismen, um öffentliche Schlüssel bei Bedarf zwischen Knoten auszutauschen. Im Übrigen werden verschiedene Optimierungen und Zusatzmechanismen aus Gründen der Übersichtlichkeit hier nicht dargestellt.

5.1 Route Request Phase

Das Route Request Paket, welches D als Broadcast verschickt, hat einen Aufbau wie in Abbildung 2 Schritt 1 gezeigt. Das erste Feld ist ein Typbezeichner und kennzeichnet das Paket als RREQ. Dann folgen Absender- und Ziel-ID (S bzw. D) sowie eine Route Request ID, welche der Absender eindeutig vergibt. Hinzu kommt mit $DHPK_S$ ein öffentlicher Diffie-Hellmann Schlüssel, den S zufällig wählt. Wie durch die gestrichelte

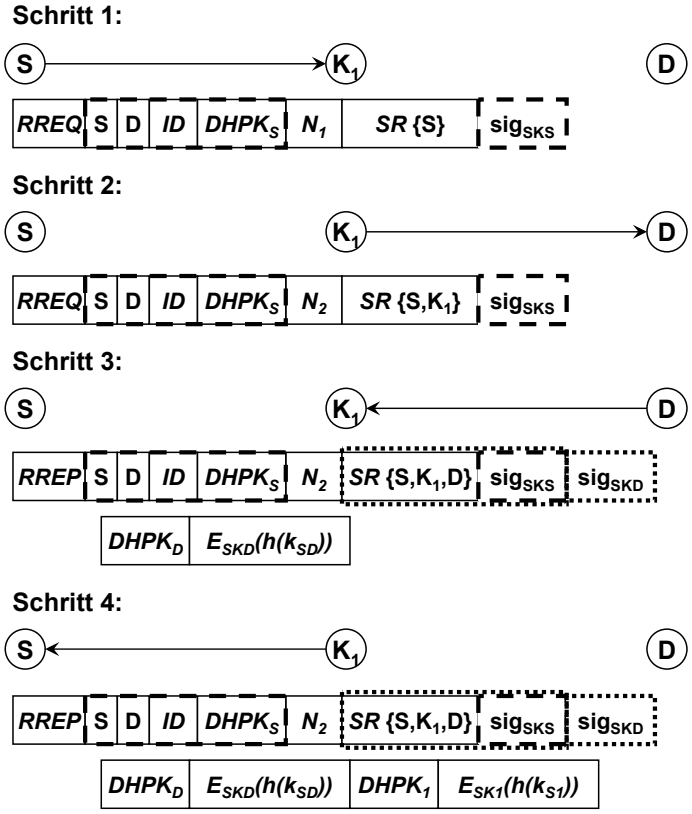

Abbildung 2: Route Discovery bei SDSR

Umrandung angedeutet ist, signiert S diese Felder mit seinem MANET-ID Schlüssel und hängt diese Signatur an den RREQ an. Zusätzlich fügt S noch eine zufällige Nonce N_1 sowie eine Sourceroute mit sich selbst als einzigem Eintrag hinzu. S muss sich N_1 bis zum Eintreffen der Route Replies merken.

Jeder Zwischenknoten K_i, der einen solchen RREQ empfängt, prüft zunächst, ob er bereits einen RREQ mit gleichem Absender und gleicher Request ID weitergeleitet hat. In diesem Fall verwirft er das Paket.

Ansonsten flutet er den RREQ weiter, wie in Abbildung 2 Schritt 2 zu sehen ist. Vorher fügt er sich noch der Source-Route hinzu und berechnet eine neue Nonce. Dabei gilt $N_{i+1} = \{N_i\}_{k_i}$. Die neue Nonce N_{i+1} entsteht also, indem die alte Nonce N_i durch ein symmetrisches Verschlüsselungsverfahren wie AES mit dem Schlüssel k_i verschlüsselt wird. Den zufällig gewählten Schlüssel k_i kennt nur K_i und merkt ihn sich für den Route Reply.

Erreicht der RREQ das Ziel D, endet die Route Request Phase. Bevor D einen Route Reply generiert, prüft er die Signatur von S, was beweist, dass S den RREQ selbst geschickt hat.

Stimmt die Signatur nicht, verwirft D den RREQ.

5.2 Route Reply Phase

Stimmt die Signatur, generiert D einen Route Reply. Im Route Reply signiert D mit seiner MANET-ID die Source Route und die Signatur von S (siehe Abbildung 2 Schritt 3 – gepunktete Linie). Damit wird erreicht, dass sich die Source Route ab diesem Zeitpunkt nicht mehr ändern kann und dass der Reply eindeutig dem Request zugeordnet wird. Schließlich fügt D noch seinen öffentlichen DH-Schlüssel $DHPK_D$ hinzu. Dieser wird, wie schon $DHPK_S$, zufällig generiert. D ist zu diesem Zeitpunkt schon in der Lage, den gemeinsamen Sitzungsschlüssel k_{SD} gemäß dem Diffie-Hellmann Verfahren zu berechnen.

Zu diesem Schlüssel berechnet D nun

$$sig_{PK_D}(k_{SD}) = \{h(k_{SD})\}_{SK_D}$$

Es wird also der Hashwert des gemeinsamen Schlüssels mit dem geheimen RSA Schlüssel von D verschlüsselt. Später kann S anhand von $DHPK_D$ ebenfalls k_{SD} berechnen. Nun kann er die Signatur mit PK_D entschlüsseln und die Hashwerte vergleichen. Stimmen die Werte überein, ist sich S sicher, dass er den gleichen Schlüssel wie D berechnet hat und dass der Wert tatsächlich von D kommt. Die restlichen Felder übernehmen die Werte aus dem RREQ unverändert.

In Abbildung 2 Schritt 4 ist gezeigt, wie der Zwischenknoten K_1 den RREP entlang der Sourceroute weiterleitet. Zunächst prüft K_1 die Signaturen von S und D, um deren Authentizität sicherzustellen. Dann berechnet er ebenfalls einen zufälligen öffentlichen Diffie-Hellmann Schlüssel $DHPK_{K_1}$ und trägt diesen im Paket ein. Außerdem bestimmt er den gemeinsamen geheimen Schlüssel k_{SK_1} und fügt analog D einen signierten Hashwert dieses Schlüssels dem Paket hinzu. Damit kann S später den gemeinsamen Schlüssel berechnen und verifizieren.

Schließlich muss der Zwischenknoten die empfangene Nonce N_{i+1} mit seinem geheimen Schlüssel k_i *entschlüsseln* und somit N_i wieder herstellen. Da nur K_i den Schlüssel k_i kennt, wird damit sichergestellt, dass der Route Reply den gleichen Weg nimmt wie zuvor der Route Request.

Erreicht der RREP schließlich S, so prüft dieser zunächst, ob die Signatur von D stimmt. Damit weiß S, dass D den RREP geschickt hat und dass der RREP sich auf den eigenen RREQ bezieht. Außerdem steht damit fest, dass die Source Route auf dem Rückweg nicht mehr verändert wurde. Als nächstes prüft S, ob die empfangene Nonce N_1 der abgeschickten Nonce entspricht. Falls ja, steht damit fest, dass Route Request und Route Reply die gleiche Sequenz von Zwischenknoten durchlaufen haben.

Jetzt muss lediglich noch geprüft werden, ob die Sequenz der durchlaufenen Knoten auch der in der Source Route angegebenen Abfolge entspricht. Dies kann S prüfen, indem er gemäß Diffie-Hellmann die gemeinsamen geheimen Schlüssel k_{SK_i} und k_{SD} berechnet und dann die Ergebnisse mit den signierten Hashwerten vergleicht. Durch die Signaturen

werden die Knoten zuverlässig authentifiziert.

Als Ergebnis der Route Discovery lässt sich festhalten:

- S kennt eine oder mehrere Routen zu D.
- S hat die Authentizität aller anderen Knoten geprüft.
- S ist sich sicher, dass die Source Route unterwegs nicht manipuliert wurde.
- S hat gemeinsame geheime Schlüssel mit jedem K_i und D vereinbart.

Diese Aussagen wurden in obigem Text lediglich informell erläutert. In [Ka03] wird deren Korrektheit formal mittels BAN Logik verifiziert. Weiterhin werden die Laufzeiteigenschaften des Protokolls durch Simulationen untersucht. Zusätzlich zum geschilderten Basisablauf sind außerdem verschiedene Erweiterungen und Optimierungen beschrieben.

Damit ist auf sicherem Weg eine Route von S nach D aufgebaut. Durch die ausgetauschten Sitzungsschlüssel können S und D ihren Datenverkehr verschlüsseln, was ein Abhören durch andere Knoten verhindert. Die geheimen Sitzungsschlüssel werden außerdem von manchen Sensoren des MobIDS Systems zur Erkennung egoistischer Knoten benötigt.

6 Zusammenfassung

Wie zahlreiche wissenschaftliche Veranstaltungen belegen, sind Mobile Ad-hoc Netze heute eines der aktivsten Forschungsgebiete im Bereich von mobilen Kommunikationssystemen. Deren Absicherung ist dabei ein essentieller Bestandteil, um einen produktiven Betrieb überhaupt erst zu ermöglichen.

Meine Dissertation stellt die Sicherheitsinfrastruktur für Mobile Ad-hoc Netze „SAM“ vor, welche die Bereiche Authentifizierung, sicheres Routing und Erkennung und Ausschluss böswilliger und egoistischer Knoten umfasst. Die Arbeit ist die erste ihrer Art, welche durchgängig alle beteiligten Aspekte untersucht und Lösungen vorschlägt. Frühere Beiträge zum Thema befassten sich nur mit einzelnen Teilgebieten und übersahen meist bestehende Abhängigkeiten.

Aufbauend auf einer umfangreichen Angriffsanalyse, wurden so genannte Angriffsbäume erstellt, welche eine strukturierte und umfassende Analyse der Sicherheit von Ad-hoc Routingprotokollen ermöglichen. Daraus wurde die Architektur von SAM abgeleitet.

Im Rahmen der Authentifizierungskomponente wurde der Begriff der Identität in MANETs erstmals genauer definiert. Bisher blieb meist unklar, ob Geräte oder Personen authentifiziert wurden und was eine solche Authentifizierung aussagt. Das MANET-ID System ist ein eigenständiges Authentifizierungssystem für MANETs, welches sich von anderen Arbeiten insbesondere durch die klar definierten Anfangsbedingungen unterscheidet. Auch der Rückruf von Zertifikaten und die globale Sperrung von Knoten sind Alleinstellungsmerkmale.

Das SDSR Protokoll ist ein hochfunktionales und sicheres Routingprotokoll für MANETs. Authentifizierung und die der Austausch von Sitzungsschlüsseln sind hier effizient in den Routingprozess integriert. Auch die Verteilung von öffentlichen Schlüsseln, die bei vielen anderen Protokollen vorausgesetzt wird, ist bei SDSR explizit beschrieben. Besonders ist zu erwähnen, dass SDSR, im Gegensatz zu vielen anderen Protokollen, mittels BAN Logik formal untersucht wurde, was das Vertrauen in seine Sicherheit stärkt.

Verglichen mit den bisherigen Arbeiten anderer Autoren entwickelt MobIDS mit dem aktivitätsbasierten und dem kombinierten Overhearing, mit iterativem und eindeutigem Probing und dem Route Request Scanning vor allem die Sensoren zur Erkennung egoistischer Knoten in MANETs deutlich weiter. Aber auch der Ausschluss von Knoten ist hier präziser beschrieben als bei anderen Lösungen.

7 Werdegang

Dr. Frank Kargl studierte von 1991 bis 1997 Informatik an der Universität Ulm. In der gleichen Zeit war er Mitbegründer der Firma arago Institut für komplexes Datenmanagement GmbH in Frankfurt/Main, wo er IT Sicherheitsprojekte im Finanzsektor betreute. Von 1997 bis 1998 war er im Universitätsrechenzentrum Ulm unter anderem für die Anbindung des LANs an nationale und internationale Forschungsnetze und die Netzwerksicherheit zuständig. Von 1998 an arbeitete Herr Kargl bei Prof. Weber an der Universität Ulm an Sicherheitsthemen, Middleware für Softwareagenten und mobilen Netzen. Im Jahr 2003 promovierte er mit Auszeichnung zum Thema „Sicherheit in Mobilen Ad hoc Netzwerken“.

Literatur

[AG00] Asokan, N. und Ginzboorg, P.: Key agreement in ad hoc networks. *Computer Communications*. 23:1627–1637. 2000.

[BB02] Buchegger, S. und Boudec, J.-Y. L.: Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In: *Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing*. S. 403–410. Canary Islands, Spain. January 2002. IEEE Computer Society.

[ČHH02] Čapkun, S., Hamdi, M., und Hubaux, J.-P.: GPS-free Positioning in Mobile Ad-Hoc Networks. *Cluster Computing*. 5(2). April 2002.

[Gu02] Guerrero Zapata, M.: Secure Ad hoc On-Demand Distance Vector Routing. *ACM Mobile Computing and Communications Review (MC2R)*. 6(3):106–107. July 2002.

[HBČ01] Hubaux, J.-P., Buttyán, L., und Čapkun, S.: The Quest for Security in Mobile Ad Hoc Networks. In: *Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*. 2001.

[HJP02] Hu, Y.-C., Johnson, D. B., und Perrig, A.: SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In: *Proceedings of the 4th IEEE Workshop*

on Mobile Computing Systems and Applications (WMCSA 2002). S. 3–13. Calicoon, NY. June 2002. IEEE.

[HPJ02] Hu, Y.-C., Perrig, A., und Johnson, D. B.: Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks. In: *Proceedings of MobiCom 2002*. Atlanta, Georgia, USA. September 2002.

[Ka03] Kargl, F.: *Sicherheit in Mobilen Ad hoc Netzwerken*. PhD thesis. University of Ulm. Ulm, Germany. 2003. verfügbar unter `http://vts.uni-ulm.de/query/longview.meta.asp?document_id=3704`.

[KK+04] Kargl, F., , Klenk, A., Schlott, S., und Weber, M.: Sensors for Detection of Misbehaving Nodes in MANETs. In: *Proceedings of Workshop Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2004) (to appear)*. Dortmund, Germany. July 2004.

[KKSW04] Kargl, F., Klenk, A., Schlott, S., und Weber, M.: Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks. In: *Proceedings of 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004) (to appear)*. Heidelberg, Germany. August 2004.

[KRSW03] Kargl, F., Ribhegge, S., Schlott, S., und Weber, M.: Bluetooth-based Ad-Hoc Networks for Voice Transmission. In: *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS-36)*. Hilton Waikoloa Village, HA. January 2003.

[KSW+04] Kargl, F., Schlott, S., Weber, M., Klenk, A., und Geiß, A.: Securing Ad hoc Routing Protocols. In: *Proceedings of 30th Euromicro Conference (to appear)*. Rennes, France. August 2004.

[MGLB00] Marti, S., Giuli, T. J., Lai, K., und Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: *Mobile Computing and Networking*. S. 255–265. 2000.

[MM] Michiardi, P. und Molva, R. Prevention of Denial of Service attacks and Selfishness in Mobile Ad Hoc Networks.

[Pe01] Perkins, C. E. (Hrsg.): *Ad Hoc Networking*. Addison-Wesley. 2001.

[PH02] Papadimitratos, P. und Haas, Z. J.: Secure Routing for Mobile Ad hoc Networks. In: *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*. San Antonio, TX. January 2002.

[PH03] Papadimitratos, P. und Haas, Z. J.: Secure Link State Routing for Mobile Ad Hoc Networks. In: *IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet*. Orlando, FL. January 2003.

[Sc99] Schneier, B.: Modeling security threats. *Dr Dobb's Journal*. December 1999.

[SDL+02] Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., und Belding-Royer, E. M.: A Secure Routing Protocol for Ad Hoc Networks. In: *Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP)*. November 2002.

[Zh] Zhu, F. Paper list: Security for ad hoc networks. `http://www.ccs.neu.edu/home/zhufeng/security_manet.html`.

[ZH99] Zhou, L. und Haas, Z. J.: Securing Ad Hoc Networks. *IEEE Network*. 13(6):24–30. 1999.

[ZL00] Zhang, Y. und Lee, W.: Intrusion detection in wireless ad-hoc networks. In: *Mobile Computing and Networking*. S. 275–283. 2000.