Humboldt University Berlin
Computer Science Department
Systems Architecture Group

Rudower Chaussee 25
D-12489 Berlin-Adlershof
Germany

Phone: +49 30 2093-3400
Fax: +40 30 2093-3112
http://sar.informatik.hu-berlin.de

Sicherheit in selbstorganisierenden drahtlosen Netzen. Ein Überblick über typische Fragestellungen und Lösungsansätze

HU Berlin Public Report
SAR-PR-2005-04

July 2005

Author:

Torsten Dänicke

Sicherheit in selbstorganisierenden drahtlosen Netzen. Ein Überblick über typische Fragestellungen und Lösungsansätze

Torsten Dänicke

(Humboldt-Universität zu Berlin, Institut für Informatik)

Zusammenfassung. Selbstorganisierende drahtlose Netzwerke finden heutzutage immer mehr Anwendungsbereiche. Auf Grund ihrer Besonderheiten eignen sie sich vorzüglich zur Vernetzung von Computern oder Geräten an Orten, an denen andere Methoden zur Vernetzung nicht möglich oder nicht wünschenswert sind. Gleichzeitig werfen die Besonderheiten der selbstorganisierenden drahtlosen Netzwerke neue Fragen und Probleme auf. Ziel dieser Arbeit ist es, einen Überblick über typische Fragestellungen und Lösungen zur Sicherheit in selbstorganisierenden drahtlosen Netzwerken zu liefern. Bei der Recherche zu diesem Thema stützte ich mich vorrangig auf kommerzielle und wissenschaftliche Suchmaschinen wie Google [Goo] und die digitale Bibliothek für wissenschaftliche Literatur Citeseer [CSMIT], [CSUNIZH] und [CSIST]. Bereits vorhandene Bibliographien [Bibl1] bis [Bibl4] wurden in der Arbeit berücksichtigt. Einzelne Überblicke über Sicherheit in selbstorganisierenden drahtlosen Netzen, die in dieser Bibliographie aufgeführt sind, waren ebenso eine nahezu unerschöpfliche Quelle an Verweisen auf Konferenzpapiere, Journalbeiträgen, Buchkapitel, Dissertationen, Diplom-, Studien- und Semesterarbeiten.

Leider war es nicht immer möglich den korrekten Erscheinungsort und das Erscheinungsdatum der angegebenen Literatur zu bestimmen. Aus diesem Grund wurden in den Quellenangaben nur Titel, die Verfasser und ein Hyperlink verwendet. Der Quellenverweis enthält neben der Abkürzung des erstgenannten Verfassers ebenfalls die Jahreszahl der Erscheinung, soweit sie zu bestimmen war.

Die Rechte der Veröffentlichungen liegen bei den jeweiligen Autoren oder Verlagen. Deshalb ist es nicht auszuschließen, dass die Verweise irgendwann auf Grund von rechtlichen Schritten nicht mehr verfügbar sind. In diesem Fall ist eine wiederholte Suche mit den angegebenen Suchmaschinen zu empfehlen. Citeseer stellt beispielsweise häufig eine gecachte Version des jeweiligen Dokumentes zur Verfügung.

Zu Beginn der vorliegenden Arbeit wird auf die Eigenschaften und Besonderheiten drahtloser Ad Hoc Netzwerke eingegangen und die Anforderungen an Sicherheit werden kurz erläutert.

Den Forschungsschwerpunkten zur Sicherheit in drahtlosen selbstorganisierenden Netzwerken ist jeweils ein erläuterndes Kapitel gewidmet und es werden Beispiele aus diesen Bereichen genannt. Im 4. Kapitel werden die möglichen Gefahren, denen ein Ad Hoc Netz ausgesetzt ist, herausgestellt. Die Erkennung von Eindringlingen und die Motivation zur Kooperation der Knoten sind Gegenstand des 5. Kapitels.

Die Charakteristiken drahtloser Ad Hoc Netzwerke (siehe auch [RFC]) erfordern bei jedem Thema besondere Maßnahmen zur Sicherung. Bereits entwickelte und erprobte Verfahren zur Sicherung 'verdrahteter' Netze sind schwer oder gar nicht adaptierbar.

Sicheres Routing weist auf Probleme und Lösungen angesichts der Bedrohungen und Besonderheiten drahtloser Ad Hoc Netzwerke hin.

Einige Forscher verfolgen die viel weitergehende Frage nach Vertrauen in dynamischen Gruppen. Lösungen zum Schlüsselmanagement und der Authentifizierung decken nur einen Teil der

Problematik des Vertrauens ab. Auch Protokolle zum Keyestablishment oder Protokolle für das Gruppenkeymanagement sind eine Basis für eine sichere Kommunikation der Teilnehmer.

Im Kapitel über Sonstige Dokumente werden all jene Dokumente aufgeführt, deren Inhalt weit mehr umfasst als ein spezielles Kapitel oder bei denen eine konkrete Einordnung nicht möglich war. Hierbei handelt es sich meistens um Zusammenfassungen zur Sicherheit in Ad Hoc Netzen oder um einzelne Spezialfälle.

Veröffentlichungen zu Sensornetzen als Spezialfall drahtloser selbst-organisierender Netzwerke sind in einem eigenen Bereich mit aufgeführt.

Im Anhang ist abschließend die Bibliographie aufgeführt, die nach den die Arbeit gliedernden Themen sortiert ist..

Keywords: Security. Wireless Networks.

Table of Content

1. Einführung

Selbstorganisierende drahtlose Netzwerke finden heutzutage immer mehr Anwendungsbereiche. Auf Grund ihrer Besonderheiten eignen sie sich vorzüglich zur Vernetzung von Computern oder Geräten an Orten, an denen andere Methoden zur Vernetzung nicht möglich oder nicht wünschenswert sind. Gleichzeitig werfen die Besonderheiten der selbstorganisierenden drahtlosen Netzwerke neue Fragen und Probleme auf. Ziel dieser Arbeit ist es, einen Überblick über typische Fragestellungen und Lösungen zur Sicherheit in selbstorganisierenden drahtlosen Netzwerken zu liefern. Bei der Recherche zu diesem Thema stützte ich mich vorrangig auf kommerzielle und wissenschaftliche Suchmaschinen wie Google [Goo] und die digitale Bibliothek für wissenschaftliche Literatur Citeseer [CSMIT], [CSUNIZH] und [CSIST]. Bereits vorhandene Bibliographien [Bibl1] bis [Bibl4] wurden in der Arbeit berücksichtigt. Einzelne Überblicke über Sicherheit in selbstorganisierenden drahtlosen Netzen, die in dieser Bibliographie aufgeführt sind, waren ebenso eine nahezu unerschöpfliche Quelle an Verweisen auf Konferenzpapiere, Journalbeiträgen, Buchkapitel, Dissertationen, Diplom-, Studien- und Semesterarbeiten.
Leider war es nicht immer möglich den korrekten Erscheinungsort und das Erscheinungsdatum der angegebenen Literatur zu bestimmen. Aus diesem Grund wurden in den Quellenangaben nur Titel, die Verfasser und ein Hyperlink verwendet. Der Quellenverweis enthält neben der Abkürzung des erstgenannten Verfassers ebenfalls die Jahreszahl der Erscheinung, soweit sie zu bestimmen war.
Die Rechte der Veröffentlichungen liegen bei den jeweiligen Autoren oder Verlagen. Deshalb ist es nicht auszuschließen, dass die Verweise irgendwann auf Grund von rechtlichen Schritten nicht mehr verfügbar sind. In diesem Fall ist eine wiederholte Suche mit den angegebenen Suchmaschinen zu empfehlen. Citeseer stellt beispielsweise häufig eine gecachte Version des jeweiligen Dokumentes zur Verfügung.
Zu Beginn der vorliegenden Arbeit wird auf die Eigenschaften und Besonderheiten drahtloser Ad Hoc Netzwerke eingegangen und die Anforderungen an Sicherheit werden kurz erläutert.
Den Forschungsschwerpunkten zur Sicherheit in drahtlosen selbstorganisierenden Netzwerken ist jeweils ein erläuterndes Kapitel gewidmet und es werden Beispiele aus diesen Bereichen genannt. Im 4. Kapitel werden die möglichen Gefahren, denen ein Ad Hoc Netz ausgesetzt ist, herausgestellt. Die Erkennung von Eindringlingen und die Motivation zur Kooperation der Knoten sind Gegenstand des 5. Kapitels.
Die Charakteristiken drahtloser Ad Hoc Netzwerke (siehe auch [RFC]) erfordern bei jedem Thema besondere Maßnahmen zur Sicherung. Bereits entwickelte und erprobte Verfahren zur Sicherung 'verdrahteter' Netze sind schwer oder gar nicht adaptierbar.
Sicheres Routing weist auf Probleme und Lösungen angesichts der Bedrohungen und Besonderheiten drahtloser Ad Hoc Netzwerke hin.
Einige Forscher verfolgen die viel weitergehende Frage nach Vertrauen in dynamischen Gruppen. Lösungen zum Schlüsselmanagement und der Authentifizierung decken nur einen Teil der Problematik des Vertrauens ab. Auch Protokolle zum Keyestablishment oder Protokolle für das Gruppenkeymanagement sind eine Basis für eine sichere Kommunikation der Teilnehmer.
Im Kapitel über Sonstige Dokumente werden all jene Dokumente aufgeführt, deren Inhalt weit mehr umfasst als ein spezielles Kapitel oder bei denen eine konkrete Einordnung nicht möglich war. Hierbei handelt es sich meistens um Zusammenfassungen zur Sicherheit in Ad Hoc Netzen oder um einzelne Spezialfälle.
Veröffentlichungen zu Sensornetzen als Spezialfall drahtloser selbst-organisierender Netzwerke sind in einem eigenen Bereich mit aufgeführt.
Im Anhang ist abschließend die Bibliographie aufgeführt, die nach den die Arbeit gliedernden Themen sortiert ist.

2. Besonderheiten drahtloser Ad Hoc Netzwerke

Drahtlose Ad Hoc Netwerke haben ein Reihe von Besonderheiten. Frank Kargl erwähnt in [Kar03]: Verwendung von mobilen Komponenten, die nur eine eingeschränkte Sicherheit bieten und limitierte Ressourcen (Energie, Speicher, Rechenleistung) haben, häufige Topologieänderungen sind normal funknetzbasierte Kommunikation, die leicht abhörbar ist, was Authentifizierung mit Klartext-Passwörtern inakzeptabel macht keine Trennung zwischen einer (zentral administrierten) Routinginfrastruktur und normalen Knoten. Bhargava, Zoltowski und Meunier [BZM02] fügen noch an, dass zwischen den Kommunikationspartnern kein vordefiniertes Vertrauen existiert.

3. Anforderungen an Sicherheit

Folgende Merkmale sollte ein sicheres System aufweisen:

- -Verfügbarkeit (Availability)
- -Vertraulichkeit (Confidentiality)
- -Integrität (Integrity)
- -Authentizität (Authenticity)
- -Verbindlichkeit (Non-repudiation)
- -Zugriffskontrolle (Access control)
- -Anonymität, Pseudonymität

Verfügbarkeit
Verfügbarkeit stellt sicher, dass ein System im normalen Betrieb nicht fehlerhaft arbeitet. Angriffe auf die Verfügbarkeit oder Störungen bedeuten auch meist einen Ausfall der durch das System zur Verfügung gestellten Funktionalitäten. Denial of service (DoS) Attacken sind typische Angriffe auf die Verfügbarkeit.

Vertraulichkeit
Vertraulich ist eine Nachricht dann, wenn der Sender der Nachricht sicherstellen kann, dass nur der rechtmäßige Empfänger Zugriff auf den Inhalt der Nachricht bekommt. Die Nachricht ist auf dem Übertragungsweg geheim zu halten. Dazu werden heutzutage in der elektronischen Kommunikation Verschlüsselungsverfahren angewendet. Dehnt man den Begriff der Vertraulichkeit weiter aus, ist selbst die Tatsache des Informationsaustausches geheim zu halten. Daraus folgt, dass die Identitäten des Senders und des Empfängers geschützt werden müssen. Auch die Dauer, das Volumen und der Zeitpunkt der Informationsübertragung lassen unter Umständen unerwünschte Rückschlüsse auf die Beziehung zwischen den beiden Kommunikationspartnern zu.

Integrität
Eine Veränderung der übertragenen Daten ist eine Verletzung der Integrität. Durch Nutzung kryptographischer Funktionen lässt sich eine Manipulation der Daten erschweren.

Authentizität
Ist zweifelsfrei festzustellen welche Identität ein Teilnehmer oder Daten einer Kommunikation hat, spricht man von Authentizität. Meist will man jedoch sicherstellen, dass eine bestimmte Nachricht zu einem bestimmten Absender gehört.

Verbindlichkeit
Verbindlichkeit stellt sicher, dass dem Absender einer Nachricht nachgeweisen werden kann, dass dieser auch die Nachricht gesendet hat (der Absender kann nicht leugnen, die Nachricht geschickt zu haben). Es soll also ausgeschlossen sein, dass irgend jemand eine gültige Nachricht eines Absenders einem Empfänger wiederholt zustellt.

Zugriffskontrolle
Der Zugriff auf bestimmte Dienste, Funktionen oder Anwendungen eines Netzwerkes lässt sich nach Feststellung der Identität eines Kommunikations-partners regeln. Dazu muss aber Authentizität gewährleistet sein.

Anonymität
Ist die tatsächliche Identität eines Anwenders nicht ermittelbar, dann ist das Ziel Anonymität erreicht. Durch die Sorge der Anwender vor übermässiger Datensammlung durch private und staatliche Einrichtungen wächst auch die Bedeutung der Anonymität. Pseudonymität bedeutet, dass "zwar die Nutzung von Diensten ohne Aufdeckung der eigenen Identität möglich ist, die (wiederholte) Nutzung aber einem (bestimmten) Pseudonym zurechenbar bleibt" (aus [Spe03] Kapitel 2.1.7). Pseudonomysierungsverfahren für Ad Hoc Netzwerke werden beispielsweise in [Kar03] entwickelt.

4. Bedrohungen und Angriffe

In diesem Abschnitt werden verschiedene Verfahren von Angriffen vorgestellt. Es lassen sich zwei Arten von Angriffen im drahtlosen Ad Hoc Netzwerk unterscheiden: passive und aktive. Beim passiven Angriff sendet der Angreifer keine Nachrichten aus. Er empfängt nur die übertragenen Nachrichten, sammelt sie und wertet sie aus. Aufzuspüren sind passive Angreifer daher nur sehr schwer oder gar nicht. Beim aktiven Angriff werden Nachrichten erzeugt, geändert oder sogar gelöscht, d.h. einfach verworfen oder nicht weitergeleitet, und der Angreifer richtet so Schaden an.
Schaden entsteht auch, wenn sich ein Knoten auf MAC-Ebene nicht korrekt verhält. Das kann dazu führen, dass die Kommunikation für alle anderen Teilnehmer gestört ist, ähnlich wie bei einem DoS Angriff. Deshalb werden diese Fehlverhalten hier mit aufgeführt.

4.1. Ziele und Methoden eines Angreifers

Frank Kargl zählt in [Kar03] folgende Ziele eines Angreifers auf:

-Zugriff auf Informationen (Information Theft)
-Störung des Netzwerks (Denial Of Service)
-Eindringen in das Netz / in Knoten (Intrusion)
-Manipulation von Daten (Tampering)

4.1.1. Aktive Methoden

-Löschen/Ändern von Informationen (Loss/Modification of Information)
-Fälschen von Information (Forgery of Information)
-Maskieren, Verstellen (Masquerade)
-Dienstverweigerung, Sabotage
-Zugriffsverletzung (Authorization Violation)
-Leugnen der Kommunikation (Denial Of Communication Act)

4.1.2. Passive Methoden

Das Belauschen (Eavesdropping) von und Zugriff auf übertragene Informationen ist ein Angriff auf die Vertraulichkeit. Erfolgt die Nachrichten-übertragung unverschlüsselt ist es leicht, den Inhalt der Nachrichtenpakete zu lesen und zu analysieren. Eine Verkehrsanalyse (Traffic Analysis) ist eine Methode, um herauszufinden wer mit wem kommuniziert; außerdem den Zeitpunkt, die Dauer und das Volumen der Kommunikation. Daraus lassen sich Interessen und Gewohnheiten des Anwenders ermitteln, bedeuten somit einen Angriff auf die Anonymität.

4.2. Angriffe

4.2.1. Aktive Angriffe

In [Gre] werden mehrere Angriffstypen in die Ebenen des TCP/IP-Referenzmodells untergebracht:

-**Netzwerkebene:**
- Wurmloch
- schwarzes Loch
- byzantinischer Angriff
- Information disclosure
- Ressourcenverbrauch
- Routing
  - Routing table overflow
  - Routing table poisoning
  - Packet replication
  - Route Cache poisoning
  - Rushing

-**Transportebene:**
- Session Hijacking

-**Applikatonsebene:**
- Repudation

-**Andere:**
- Veränderung der Geräte
- Man-in-the-Middle
- Distributed DoS
- Syn flooding
- Impersonation, Identitätsänderung

[Bur03] und [Lu02] erläutern verschiedene Angriffe auf Ad Hoc Netze. [Lu02] beschränkt sich dabei auf Routingprotokolle drahtloser Netze.
Erläuterungen zu Angriffen auf Ad Hoc Netze finden sich ebenso in [Arg05], zu finden allerdings unter 'Sicheres Routing'.
Sogenannte 'Stealth Attacks' werden in [Jak03a] beschrieben. Dabei handelt es sich um Methoden, die die Kosten und die Sichtbarkeit des Angreifers minimieren.
Auswirkungen von typischen DoS-Angriffen auf Ad Hoc Netzwerke finden in [Aad04] Erwähnung.
Auch vermeintlich sichere Routingalgorithmen sind anfällig gegen Rushingangriffe, wie in [Hu03a] gezeigt wird. Diese Art von Angriff wird meist auf on-demand Routingalgorithmen, basierend auf DSR, angewendet.
Eine Seminararbeit [Bac04] führt spezielle Angriffe in Ad-Hoc Netzen vor, sowie Angriffe auf AODV und in Sensornetzen.

4.2.2. Passive Angriffe

Belauschen und das Durchführen von Verkehrsanalysen sind Angriffe auf Vertraulichkeit und Anonymität. Neuere Arten von passiven Angriffen sind Thema der Arbeit [Kong03c].

4.2.3. MAC-Ebene Fehlverhalten

Auf MAC-Ebene gibt es auch einige Spielregeln, die von Angreifern gebrochen werden können. [Tri04] berichtet über Bandbreitenklau in Funknetzen durch Manipulation der Netzwerkkarte.
In der Bibliographie gibt es weitere Dokumente mit Einblicken über das Schummeln in der MAC-Ebene und dessen Auswirkungen. In [Kya04] findet man auch gleich eine Modifikation des IEEE 802.11 Protokolls, damit eigennützige Knoten einfach erkannt werden können.

5. Erkennung von Eindringlingen (Intrusion Detection)

In drahtlosen Ad Hoc Netzen sind, im Gegensatz zu verdrahteten Netzen, die Zugriffsmöglichkeiten auf den Übertragungskanal wesentlich einfacher. Es gibt keine Kabel und keine Switches zum Anzapfen. Auch fehlen Router und Gateways. Jeder Teilnehmer im Ad Hoc Netz muss auf diese Gefahren vorbereitet sein.
Ein Knoten im drahtlosen Ad Hoc Netzwerk ist eine autonome Einheit, die sich frei bewegen kann. Physikalische Sicherheit (Schutz gegen Wegtragen, Aufschrauben, Analysieren, Manipulieren wie in [CCC03] dokumentiert) ist schwer zu realisieren. Auch ist es schwierig einen kompromitierten Knoten im Netzwerk zu finden. Jeder Knoten im Netz muss demzufolge in einem Modus arbeiten können, ohne Vertrauen in irgendeinen Knoten zu besitzen.
Die Struktur von Ad Hoc Netzen ist dezentralisiert. Viele in Ad Hoc Netzen verwendete Algorithmen hängen vom kooperativen Verhalten der einzelnen Knoten im Netz ab. Neue Arten von Angriffen auf dezentrale Architekturen, mit dem Ziel, die kooperativen Algorithmen zu brechen, werden sich weiter entwickeln.
Techniken, die das Eindringen erschweren, wie Verschlüsselung und Authentifizierung, können das Risiko des Eindringens nur mindern aber nicht ausschliessen.
In [Bay] wird das Eindringen als Menge von Aktionen definiert, welche die Integrität, Vertraulichkeit oder Verfügbarkeit der Ressource kompromitieren. Erkennung von Eindringlingen basiert auf der Annahme, dass Benutzer- und Programmaktivitäten beobachtbar sind und diese Aktivitäten aufgezeichnet werden. IDS haben leichten Zugriff auf diese aufgezeichneten Daten und analysieren sie. Signifikante Änderungen vom normalen Systemverhalten werden als Angriffe gewertet.
Es lassen sich zwei Arten von IDS erkennen: *netzwerkbasierte* IDS (befindet sich auf dem Netzwerk Gateway, loggt und überprüft alle Pakete, die über die Netzwerkschnittstelle transportiert werden) und *hostbasierte* IDS (befindet sich auf dem Host, loggt und analysiert die Daten, die vom Benutzer oder den Programmen auf diesem Host generiert werden). Wegen fehlender Infrastruktur sind netzwerkbasierte IDS für Ad Hoc Netzwerke schlecht nutzbar. Die begrenzte Sende- und Empfangsreichweite der Knoten hat zur Folge, dass die geloggten Daten nur diesen Sende- und Empfangsbereich betreffen. Weiterhin treten Anomalien in Ad Hoc Netzwerken häufig auf, so dass darauf basierte IDS nicht zwischen falschem Alarm und tatsächlichem Eindringen unterscheiden können.

Eine zu empfehlende ausführliche Erläuterung der IDS-Grundlagen und Probleme der traditionellen IDS mit Ad hoc Netzwerken findet sich in [Kle03].

5.1. Erkennung von sich fehlverhaltenden Knoten

In dieser Liste sind die Modelle vorgestellt, die sich mit der Erkennung von sich fehlverhaltenden Knoten und mit dem Routing im Angesicht von diesen beschäftigen. Padmanabhan stellt in [Pad03] ein sicheres Traceroute vor, um bei der Erkennung und Lokalisation von sich fehlverhaltenden Knoten zu helfen. [Kar04a] stellt MobIDS vor, genauere Angaben zu MobIDS finden sich jedoch in [Kar03].

5.1.1. IDS

Hier wird auf Intrusion Detection Systeme sowohl im Allgemeinen eingegangen, wie zum Beispiel in [Kle03], als auch verschiedene Modelle für drahtlose Ad Hoc Netzwerke vorgestellt. Weiterhin befindet sich auch eine Bibliographie [Me01] in der Liste. Klenk bewertet in seiner Arbeit [Kle03] auch verschiedene IDS und Eindringlingsvermeidungsstrategien. Eine beispielhafte Einführung in IDS in Ad Hoc Netzen ist in [ZhaYo00] zu finden.

5.1.2. Watchdog, Pathrater

Die Arbeit von Sergio Marti, T.J. Giuli, Kevin Lai und Mary Baker [Mar00] stellt Watchdog und Pathrater im Original vor. Sie haben DSR mit zwei Komponenten versehen. Watchdog erkennt verbotenes packet forwarding und Pathrater bewertet jede benutzte Route, um dann böswillige Knoten in den benutzen Routen zu vermeiden. Die Arbeiten von Klenk [Kle03] und Kargl [Kar03] gehen ebenfalls darauf ein und finden eine Bewertung für das System.

5.1.3. Kooperation

Für Kooperation innerhalb des Netzwerkes zu sorgen ist nicht nur eine Strategie die Leistungsfähigkeit (Durchsatz, Reichweite) des gesamten Netzes zu erhöhen. Sie wird auch zum Vermeiden von Fehlverhalten verwendet und weiterhin zum Erkennen von sich fehlverhaltenden Knoten und sogar Eindringlingen. Es wird dabei von Annahme ausgegangen, dass ein unkooperativer Knoten auf jeden Fall ein sich fehlverhaltender Knoten, wenn nicht gar ein Eindringling, ist. Eine Analyse der Erfordernisse für kooperatives Verhalten findet sich in der Arbeit von Philipp Obreiter, Birgitta König-Ries und Michael Klein in [Ob03].

5.1.3.1. CONFIDANT

Sonja Buchegger stellt in [Buc02b] ihr CONFIDANT ('**C**ooperation **O**f **N**odes, **F**airness **I**n **D**ynamic **A**d Hoc **N**e**T**works') zum ersten Mal vor. In diesem Ansatz wird das Verhalten von einem Knoten von seinen Nachbarn beobachtet und ein eigennütziger Knoten wird vom Netzwerk isoliert. In [Buc02c] wird auch eine Performanceanalyse durchgeführt. Sie versehen ein DSR-Protokoll mit CONFIDANT und vergleichen die Performance mit einem wehrlosem

DSR. Dabei wird festgestellt, dass ein mit CONFIDANT ausgestattetes Protokoll in einem Netz mit einem Anteil von bis zu 60% böswilligen Knoten sich in Bezug auf Durchsatz signifikant besser verhält als ein wehrloses Protokoll. (Zu bemerken ist noch, dass die Performanceanalyse vollständig in GloMoSim implementiert und durchgeführt wurde.)
Die Arbeiten von Klenk [Kle03] und Kargl [Kar03] haben CONFIDANT ebenfalls ein Kapitel gewidmet.

5.1.3.2. Core

Pietro Michiardi und Refik Molva entwickelten in [Mic01] einen anderen Ansatz.
In diesem System bewerten sich die Knoten gegenseitig und tauschen die Bewertungen aus. Bei negativer Bewertung wird der negativ bewertete Knoten bestraft. So sollen die einzelnen Knoten zur Kooperation bewegt werden. Ein Feature von CORE ist, dass ein DoS durch Broadcasting von negativen Bewertungen für 'gute' Nutzer verhindert wird.
Neben den Originaldokumenten [Mic01] und [Mic03] sind auch hier die Arbeiten [Kle03] und [Kar03] mit jeweils einem Kapitel zu empfehlen.

5.1.3.3. Nuglets, Counters

Nuglets sind eine virtuelle Währung. Zum ersten Mal in [But00] von Buttyan und Hubaux in ihrem Packet Trading Model angerissen. Nuglets werden zur Verrechnung gegenseitiger Dienste verwendet und sorgen so für Kooperation.
Ein Knoten verdient Nuglets, wenn er Pakete für einen anderen Knoten weiterleitet und er muss Nuglets ausgeben, wenn er selbst Verkehr erzeugt.
In [Sal03] wird ein Schema (als Teil des Terminodes-Projektes) vorgestellt, in dem die benutzten Protokolle mit symmetrischen kryptographischen Schlüssel arbeiten, um für einen Operator die Möglichkeit zu bieten, alle am Routing beteiligten Knoten zu identifizieren, um auf deren Konten etwas abzubuchen oder gutzuschreiben.
Da Klenk in [Kle03] einen Vergleich der hier aufgezählten IDS und Kooperationsmechanismen gemacht hat, sei er hier nochmals als vertiefende Lektüre zum Verschaffen eines diesbezüglichen Überblicks erwähnt.

6. Sicheres Routing

Die meisten Arbeiten zur Sicherheit in Ad Hoc Netzen konzentrieren sich auf Angriffe der Routingverfahren und auf sichere Routingprotokolle, die diesen Angriffen widerstehen sollen. Angriffe wurden bereits im 4. Kapitel aufgeführt. Diese sind dann zumeist Ausgangspunkt für einen neuen, sicheren Routingalgorithmus oder einer Protokollerweiterung, welche dann die Folgen des Angriffs mildern oder gar keinen Erfolg für den Angriff sichern.
Das Problem sicherer Routingprotokolle ist, dass sie schwierig zu entwerfen sind. Existierende Routingprotokolle sind auf das rasche Verbreiten von Routinginformationen optimiert, da sich die Topologie des Netzwerkes schnell verändern kann. Sicherheitsmechanismen verbrauchen Ressourcen und können den Austausch von Routinginformationen verzögern oder gar verhindern [Arg02].
Eine Liste vorhandener (ungesicherter) Routingalgorithmen für Ad Hoc Netzwerke findet sich in [Wiki]. Ebenso stellt Elizabeth M. Royer in [Roy99] einige Mechanismen ungesicherter Routingalgorithmen vor.

6.1. Überblicke und allgemein gehaltene Dokumente

Hier finden sich Arbeiten zu Sicherheitsproblemen aktueller Routingalgorithmen [Cho03], [YanH04], Verletzbarkeiten und Schutz [Put04b] und verschiedene Überblicke aktueller Mechanismen zur Sicherung von Routingprotokollen [Arg02], [Hu04], [Ink04]. Die hier aufgezählten Arbeiten sind nur ein Teil der Liste. Weitere Arbeiten sind in der Bibliographie zu finden.
Buttyan und Vajda [But04] entwickeln ein formales Framework zur Analyse von on-demand source routing Protokollen, analysieren damit 2 "sichere" Protokolle und entdecken noch unbekannte Angriffe gegen diese.
[Arg05] ist ein aktueller Überblick zu sicheren Routingprotokollen und weiterer verwendeten Mechanismen zur Absicherung von mobilen Ad Hoc Netzwerken. [LiHu02] ist ein etwas älterer Überblick.

6.2. Proaktive sichere Routingalgorithmen (table driven)

Hier sind die sicheren proaktiven Routingalgorithmen aufgelistet. Es stellte sich heraus, dass nicht leicht zu entscheiden ist, ob ein Paper einen komplett neuen Routingalgorithmus vorstellt oder ob es sich nicht "nur" um eine Protokollerweiterung eines bereits vorhanden Algorithmus handelt. SEAD ist ein solcher Kandidat, vorgestellt von Yih-Chun Hu, David B. Johnson und Adrian Perrig in [Hu02b]. Er basiert auf DSDV und benutzt Einweghashfunktionen, um die Distanzvektoraktualisierungen von jedem Knoten zu authentisieren. Böswillige Knoten sollen so nicht mehr die Distanzvektorwerte beim Update mit kleineren Entfernungen fälschen können. Sie können sehr wohl größere Werte eintragen, aber diese Route wird zu Gunsten einer kürzeren Route verworfen.

6.3. Reaktive sichere Routingalgorithmen (on demand)

Reaktive Routingalgorithmen bestimmen die Route von der Quelle zum Ziel erst bei Bedarf. Der Quellknoten initiiert einen Prozess, der die Route im Netz bestimmt. Er ist beendet, wenn eine Route gefunden wurde oder alle möglichen Permutationen von Routen untersucht wurden [Roy99].
Papadimitratos und Haas stellen in [Pap02a] SRP (**S**ecure **R**outing **P**rotocol) vor. Es garantiert eine korrekte Routediscovery, so dass falsche Routereplies verworfen oder niemals den Routerequester erreichen.
ANODR [Kong03a], MASK [ZhaYa05] und ASR [ZhuB04] sind Routingalgorithmen, deren Autoren sich mit dem Thema Anonymität und Verkehrsanalyse beschäftigen und jeweils ein Protokoll konzipiert haben, die sicherstellen, dass die realen Identitäten der Übertragenden geschützt bleiben.
ARAN [San02] '**A**uthenticated **R**outing for **A**d Hoc **N**etworks' entdeckt und schützt gegen böswillige Aktionen in einer *besonderen* Ad Hoc Netzwerk Umgebung (hierbei ist eine Trusted CA nötig). Jeder Knoten, der ein RREQ oder RREP weiterleitet, muss es signieren.
Die Idee hinter SAODV [Zap05] 'Secure AODV' ist nach Hu und Perrig [Hu04] eine Signatur, welche die meisten Felder eines Route Requests (RREQ) und Route Reply (RREP) authentisiert und Hash Ketten, die die Hop Counts authentisieren.
Ein sicheres on-demand Routingprotokoll von Hu, Perrig und Johnson ist ARIADNE [Hu02c]. Es hindert Angreifer an der Manipulation von Routen. Ausserdem verhindert es eine Anzahl an Denial-of-Service Angriffen. Es basiert auf DSR und benutzt das Broadcastauthentifizierungsprotokoll namens TESLA [Per02a]. Darauf wird in Kapitel 6.7. noch einmal eingegangen.

SAR [Yi01a] 'Security-Aware Ad hoc Routing' führt eine verhandelbare Metrik ein, um sichere, nicht zwingend die kürzesten, Routen zu finden. Mehrere Techniken können verwendet werden: Zeitstempel, Sequenznummern, Passwörter, Zertifikate, Digests, digitale Signaturen, Verschlüsselung, Zeugnisse, Verkettungen von digitalen Signaturen, um verschiedene Schutzebenen, sogenannte 'level of protection', bei der Übertragung zu haben. Die 'Sicherheitsmetrik' wird in RREQ Pakete verpackt. Ein Knoten kann solch ein Paket nur verarbeiten oder weiterleiten, wenn die erforderte Sicherheit unterstützt wird.

6.4. Hierarchische sichere Routingalgorithmen

Das SLSP '**S**ecure **L**ink **S**tate **P**rotocol' von Papadimatros und Haas [Pap03d] benutzt digitale Signaturen und Einweg-Hash-Ketten, um die Link-State Aktualisierungen zu sichern. So ist es robust gegen einzelne byzantinische Angriffe und widerstandsfähiger gegen Angriffe auf Netzwerk- und Knotenressourcen.

6.5. Hybride sichere Routingalgorithmen

Einen sicheren Routingalgorithmus hybrider Kategorie stellen Po-Wah Yau und Chris Mitchell in [Yau04] vor. Der Algorithmus ist allerdings noch nicht fertig. Eine Sicherheitsanalyse der Autoren hat einige Fragen aufgeworfen, die noch gelöst werden müssen.

6.6. Geographisch sichere Routingalgorithmen

Das 'Terminodes Project' ist ein 10-Jahres Forschungsprogramm (2000-2010) mit Fokus auf einen verteilten Ansatz *aller* Netzwerkfunktionen. In [Hub01a] und [Bla02] werden die Routingkomponenten beschrieben.

6.7. Protokollerweiterungen für Routingalgorithmen

Packet Leashes [Hu01b], mit denen existierende Protokolle ausgestattet werden können, sind eine spezifische Lösung gegen Tunnelangriffe. Jedes Paket enthält hierbei zusätzliche Informationen, mit denen Empfängerknoten feststellen können, ob ein Paket unrealistische Entfernungen zurückgelegt hat.
Mittels TESLA, vorgestellt in [Per02a], werden Broad- und Multicast-Nachrichten authentisiert. Über eine zu versendende Nachricht wird ein MAC berechnet, in den ein Schlüssel eingeht. Ein Initialschlüssel ist Ausgangspunkt für eine Hashkette. Die Zeit ist in Intervalle eingeteilt und ein Schlüssel ist nur in einem Intervall zum Verschlüsseln von Nachrichten gültig. Dieser Schlüssel wird dann zu einem späteren Zeitpunkt versendet, mit dem dann alle Knoten die Authentizität der Nachricht bestimmen können. Bei Veröffentlichung des Schlüssels müssen bereits alle damit verschlüsselten Nachrichten ihre Empfänger erreicht haben.
Funktionieren kann TESLA allerdings nur, wenn alle Knoten hinreichend genau synchronisierte Uhren haben. Das Maximum des Zeitsychronisationsfehlers zwischen zwei beliebigen Knoten im Netz muss darüber hinaus allen Knoten bekannt sein.

7. Vertrauen

In Ad Hoc Netzen hängt die Sicherheit der Kommunikation von der richtigen Wahl der zum Ziel benuzten Route ab [BZM02]. Es ist für einen Knoten wichtig die Zuverlässigkeit/Vertrauenswürdigkeit (in [BZM02] wird als englischer Begriff '*reliability*' verwendet) einer Route zu kennen. Die Forschungsprobleme beim Finden vertrauenswürdiger Routen sind folgende:

- Wie berechnet man die Vertrauenswürdigkeit eines einzelnen Knotens? Der Vertrauenswert beschreibt die Fähigkeit eines Knotens Pakete weiterzuleiten oder einen sicheren Weg zu benutzen.
- Wie berechnet man die Vertrauenswürdigkeit einer Route, abhängig von den Vertrauenswerten der Knoten am Pfad entlang?

Die Herstellung von Vertrauensbeziehungen geht über Keymanagement hinaus. Was Vertrauen mit Sicherheit zu tun hat, wird in [LiuZ04] und [Lam01] erörtert. [Pir04] und [Esc02a] beschäftigen sich mit der Frage, wie Vertrauen hergestellt wird.

8. Keymanagement, Authentication

Die Sicherheit ist in den meisten Fällen vom richtigen Keymangement abhängig. Hier müssen die Fragen zur Schlüsselerzeugung, -speicherung und -verteilung beantwortet werden. Auch wird hier entschieden, welche Art von Kryptosystem verwendet wird. Wird eines mit symmetrischen Schlüsseln oder öffentlichen Schlüsseln verwendet? Kann auch ein Kryptosystem mit elliptischen Kurven verwendet werden? Jedes System hat Vorzüge aber auch Nachteile, wobei die Kryptographie mit elliptischen Kurven noch recht neu ist.
Traditionelles Keymanagement hat Voraussetzungen, die es unbrauchbar für eine Nutzung in einem Ad Hoc Netzwerk macht. Nur in speziellen Ad Hoc Umgebungen kann die benötigte Trusted Third Party benutzt werden, sofern die Infrastruktur dafür vorhanden ist. Der Normalfall für Ad Hoc Netzwerke ist dies jedoch nicht.

8.1. Allgemein gehaltene Dokumente

In [Bind] werden die Charakteristiken des Keymangements in drahtlosen Ad Hoc Netzen aufgezählt, erläutert und die wichtigsten Verfahren vorgestellt.
[Fok02] beleuchtet auch den theoretischen Hintergrund und stellt die Verfahren ausführlicher als [Bind] vor.
Einen Überblick über hauptsächlich in drahtlosen Umgebungen verwendete Schlüsselverwaltungsprotokolle geben die Autoren von [Sin04]. Sie unterscheiden dabei two-party Protokolle, verdrahtete und drahtlose Gruppenkommunikationsprotokolle. Sie analysieren die Protokolle auf Verwundbarkeiten und führen eine Performance-analyse vergleichbarer Protokolle durch.
Capkun stellt in 'Mobility helps Scecurity in Ad Hoc Networks' [Cap03c] einen Mechanismus vor, in welchem die Mobilitätseigenschaft der Knoten helfen soll, Sicherheitsassoziationen zwischen den Knoten aufzubauen.

8.2. Verteiltes Schlüsselmanagement

Bei dieser Art von Schlüsselmanagement werden die Funktionen der Zertifizierungsinstanz auf mehrere Knoten verteilt und von diesen erbracht. Sind dabei nicht alle Knoten des Netzes beteiligt, d.h., gibt es nur einige sogenannte Server, dann ist es eine partiell verteilte Zertifizierungsstelle. Sind dagegen alle Knoten des Netzes daran beteiligt, dann ist sie vollständig verteilt.
In [Schi04] wird die Idee der Schwellwertkryptographie im Bezug zu mobilen Ad Hoc Netzwerken näher betrachtet. Schwellwertkryptographie bezeichnet eine Schema, dass *n* Teilnehmer sich die Fähigkeit, eine kryptographische Operation (zum Beispiel die Erzeugung einer digitalen Signatur) durchzuführen, teilen. Dabei können *t* (*t*<=*n*) Teilnehmer diese Operation durchführen, aber nicht *t*-1 Teilnehmer. Diese Schema wird (*n*,*t*) Schwellwert genannt.
Zu erwähnen ist die Arbeit [Kong01] zu einer vollständig verteilten Zertifi-zierungsinstanz, in der jeder Knoten ein Zertifizierungsserver ist und einen Teil des geteilten Geheimnis trägt. Die Architektur basiert auf Shamirs Secret Sharing [Sha79].
Eine partiell verteilte Schlüsselverwaltung wird in [ZhoL99] beschrieben und in [ZhoL00] wird darauf aufbauend COCA vorgestellt, eine fehlertolerante und sichere Online CA. Die Autoren kommen zu dem Schluss, dass COCA das Stadium einer prototypischen Online CA verlassen hat.
MOCA (**MO**bile **C**erticate **A**uthority) in [Yi01b], [Yi02b] und [Yi03a] verfolgt ein ähnliches Ziel wie COCA. Sie präsentieren aber weitere Vorschläge zu offenen Fragen. Die Auswahl der Serverknoten wird von der Annahme geleitet, dass es beispielsweise leistungsstärkere Knoten als andere gibt.
Das Verfahren kann man folgendermaßen beschreiben: Unter *n* MOCA-Knoten wird der private Schlüssel der CA aufgeteilt und jede Menge von *k* MOCA-Knoten kann den Schlüssel rekonstruieren. Damit aber der private Schlüssel niemals rekonstruiert wird, werden digitale Schwellwertsignaturen benutzt.
Was anschließend folgt, beschreiben Yi und Kravets in [Yi01b] Kapitel 3.1:
"Any client requiring a certification service needs to contact at least *k* MOCA nodes with its request data. The contacted MOCA nodes each generate a partial signature over the received data and send it back. Then, the client needs to collect at least *k* such pieces of partial signatures to reconstruct the full signature by the CA and successfully receives the certification service."

8.2. Selbstorganisierende Infrastruktur

Ein neuer Ansatz zur Authentifizierung öffentlicher Schlüssel wurde zusammen mit PGP entwickelt und verbreitet. Jeder Nutzer kann die Schlüssel signieren von deren Authentizität er sich selbst überzeugt hat. Ist ein Schlüssel von vielen vertrauenswürdigen Nutzern signiert, dann wird dieser Schlüssel auch als authentisch angesehen. Vertrauen ist hier transitiv: A vertraut B und B vertraut C, dann vertraut A auch C. So entsteht das *Web of Trust*.
In [Hub01b] und [Cap02b] benutzen Hubaux, Buttyan und Capkan Zertifikatsketten. Benutzer und Zertifikate werden als gerichteter Graph *G(V,E)* aufgefasst. Die Knoten V sind die Benutzer, die Kanten E sind die Zertifikate.
$AB \in E$ heisst: A hat den Schlüssel von B signiert.
Jeder Knoten hält eine begrenzte Anzahl an Zertifikaten in einem Repository. Will nun ein Benutzer *S* mit *D* kommunizieren, tauschen beide ihre Zertifikatsgraphen aus und vereinigen sie. Danach suchen beide nach einer Zertifikatskette von *S* zu *D* und von *D* zu *S*. Existieren diese Ketten, dann haben sich beide Knoten von der Authentizität des öffentlichen Schlüssels des jeweilig anderen überzeugt.

8.3. Resurrecting Duckling

Authentifizierung durch 'Prägen' ist eine Methode, die Stajano und Anderson in [Sta99] entwickelten. In Analogie zu dem in der Natur vorkommenden Phänomen, dass das erste sich bewegende Objekt, welches ein Entenküken sieht, seine Mutter sein muss. Ein 'Küken' wird geprägt, in dem es einen geheimen Schlüssel zur Verschlüsselung über einen extra dafür eingerichteten Übertragungskanal zugeschickt bekommt und akzeptiert. Ab diesem Zeitpunkt gehorcht das "Küken" nur noch der "Mutter". Der Tod des "Kükens" kann automatisch, auf Befehl oder andere Weise ausgelöst werden, danach ist das "Küken" wieder bereit für eine neue Prägung.
Dirk Balfanz, D. K. Smetters, Paul Stewart und H. Chi Wong erweiterten diese Methode in [Bal02], um öffentliche Schlüssel und Schlüssel für Gruppen-kommunikation verwenden zu können.

8.4. Kryptobasierte Identitäten

Die direkte Ableitung der Identität und Adresse eines Netzteilnehmers aus dessen öffentlichen Schlüssel ist die Idee von kryptobasierten Identitäten.
Nach [Spe03] ist die gegenseitige Abhängigkeit zwischen Routing- und Sicherheitsmechanismen Thematik des Entwurfes [Bob02] von Bobba, Eschenauer, Gligor und Arbaugh. Sichere Routingalgorithmen setzen Sicherheitsmechanismen voraus, die wiederum funktionstüchtige sichere Routen voraussetzen. Dieses klassische "Henne-Ei-Problem" der zyklischen Abhängigkeit wird nach Aussage der Autoren eliminiert und die Lösung mit Hilfe des DSR-Protokolls illustriert. Der öffentliche Schlüssel hat kein Zertifikat oder Ähnliches. Die kryptobasierte Identität ist ein 128 Bit langer Hashwert des öffentlichen Schlüssels; die kryptobasierte Adresse setzt sich aus einem 64 Bit langen Netzwerkpräfix und einem 64 Bit langen Hashwert des Schlüssels zusammen. Sie kann somit direkt als IPv6-Adresse verwendet werden. Beide Werte sind statistisch einmalig und kryptographisch verifizierbar. Die Rechtmäßigkeit der Werte lässt sich beispielsweise mit der Erzeugung einer digitalen Signatur mit Hilfe des geheimen Schlüssels beweisen.
Die Authentifizierung von Knoten und Nachrichten ohne Schlüsselübertragung über sichere Kanäle oder eine Zertifizierung der Schlüssel ist damit möglich. Ein gravierendes Problem ist nur, dass ein Knoten sich beliebig viele Schlüsselpaare erzeugen kann.

8.5. Schlüsselmanagement mit ID-basierter Kryptographie

Identitätsbasierte Kryptographie ist der umgekehrte Fall von kryptobasierten Identitäten. Aus der Identität wird der öffentliche Schlüssel abgeleitet.
Ein beliebiger Bitstring kann als öffentlicher Schlüssel für ein Public-Key-Verfahren verwendet werden. Im vorgestellten Schema in [Khal03] wird die Knotenidentität als öffentlicher Schlüssel verwendet. Um zu vermeiden, dass sich ein Benutzer zu seiner Identität (seinem öffentlichen Schlüssel) seinen geheimen Schlüssel erzeugt, wird ein vertrauenswürdiger Dritter vorausgesetzt. Private Key Generation Service (PKG) heisst die Trusted Third Party.
Der PKG-Server besitzt das Master-Public-Key-Schlüsselpaar. Dieses Paar wird beim Start des Netzwerkes von allen teilnehmenden Knoten verteilt erzeugt. Der öffentliche Schlüssel ist allen Knoten bekannt und wird auch an neu hinzu-kommende Knoten ausgegeben. Der private Schlüssel des PKG wird in (n,t)-Schwellwertmanier auf n Knoten verteilt. Ist der öffentliche Schlüssel der PKG erzeut und allen bekannt, dann kann ein Knoten seine Identität als öffentlichen Schlüssel benutzen. Der private Schlüssel des Masterschlüsselpaares wird zur Erzeugung des geheimen Schlüssels für einen Knoten verwendet. Ein Knoten, der seinen vollständigen privaten Key erhalten will, muss dafür t andere Knoten kontaktieren.

9. Keyestablishment Protokolle, Gruppenkeymangement

Will eine Gruppe von Knoten eine sichere Sitzung eröffnen, in der nur für die Gruppe bestimmte Informationen ausgetauscht werden, müssen sie sich vorher auf ein Geheimnis einigen. Das gängige Beispiel ist, dass mehrere Leute, die sich kennen, in einem geschlossenen Konferenzraum sitzen und mit ihren Laptops in Ad Hoc Manier eine sichere Sitzung aufbauen wollen.
Asokan beschreibt in seiner Arbeit [Aso99] ein passwortbasiertes Verfahren. Hielati evaluiert in [Hie01] verschiedene Protokolle und bewertet sie nach ihrer Nutzbarkeit für Ad Hoc Netzwerke. Im Überblick von Rafaeli [Raf03] werden die Architekturen zum Gruppenkeymanagement in drei Klassen unterteilt: zentral strukturierte, dezentral struktuierte und verteilte Architekturen. Anschliessend beschreibt er die gängigen Ziele der vorgestellten Klassen und stellt die wichtigsten Protokolle zu jeder Klasse vor.

10. Sonstige Dokumente

In diesem Abschnitt sind all jene Dokumente aufgeführt, bei denen die konkrete Einordnung in die oben behandelten Abschnitte nicht möglich war. Teilweise umfassen sie fast alle hier vorgestellten Bereiche, wie beispielsweise das Terminodesprojekt in [Hub99] und [Bla01]. Weiterhin können es Spezialfälle mit besonderen Anforderungen sein [Kong02b]. Es gibt einen Bericht über eine Arbeitssitzung in [But02]. Dort werden die verschiedenen Aspekte von Sicherheit in drahtlosen Ad Hoc Netzen beleuchtet.
Die Diplomarbeit von Ingo Riedel [Rie03] beschäftigt sich mit Kryptographie auf Basis elliptischer Kurven. Die kryptograpischen Fähigkeiten von RFID-Tags (kleine Chips mit extrem wenig Ressourcen) sind das Thema in [Jue].

11. Dokumente zu Sensornetzen

Sensornetzwerke sammeln Daten über ihre jeweilige Umgebung. Sie werden meistens, ähnlich wie Ad Hoc Netze, mit mobilen Geräten aufgebaut. Dadurch haben sie auch mit denselben Problemen zu kämpfen. Der Unterschied jedoch zu Ad Hoc Netzwerken ist, dass es normalerweise in Sensornetzen eine Basisstation gibt. Diese Basisstation empfängt die Daten der einzelnen Sensoren, meist übernimmt sie auch die Netzwerkverwaltung. Die Sensoren sind nur für das Weiterleiten ihrer Beobachtungen konzipiert und haben weniger Rechenleistung als Teilnehmer eines 'normalen' Ad Hoc Netzwerkes. Aus diesem Grund fand eine Klassifikation wie bei den Ad Hoc Netzwerken nicht statt.

1. Anhang mit Referenzen

[Bibl1] ***Security for Ad Hoc Networks***, http://www.cs.utsa.edu/~hmanchal/Research/adhoc_security.html

[Bibl2] ***Sensor Networks Security Webpage***, http://www.ee.ucla.edu/~saurabh/robust/

[Bibl3] ***Wireless Ad Hoc Networks Bibliography***, http://w3.antd.nist.gov/wctg/manet/manet_bibliog.html

[Bibl4] ***Bibliography***, http://www.cs.ucl.ac.uk/staff/M.Rogers/bibliography.html

[Bay] ***Security in ad hoc networks***, Arun Kumar Bayya et al., Universität von Kentucky, http://cs.engr.uky.edu/~singhal/term-papers/Fourth-paper.doc

[CCC03] ***Hack a Bike - keep on hacking in a free world!,*** http://www.ccc.de/hackabike/index_de.html

[CSIST] ***Computer and Information Science Papers CiteSeer Publications ResearchIndex***, School of Information Sciences and Technology, http://citeseer.ist.psu.edu/

[CSUNIZH] ***Computer and Information Science Papers CiteSeer Publications ResearchIndex***, University of Zurich, Department of Informatics, http://sherry.ifi.unizh.ch/

[CSMIT] ***Computer and Information Science Papers CiteSeer Publications ResearchIndex***, MIT, http://citeseer.csail.mit.edu/

[Goo] **Google**, www.google.de

[Gre] ***Security in Ad Hoc Networks***, Michal Grega, Jakub Jakubiak, Krzystof Marcisz, Szymon Szott, http://www.cs.tut.fi/kurssit/83390/presentations/ad_hoc_security.pdf

[RFC] ***RFC-Index***, ftp://ftp.rfc-editor.org/in-notes/rfc2501.txt

[Sha79] ***How to share a secret***, Adi Shamir, http://crypto.csail.mit.edu/classes/6.857/papers/secret-shamir.pdf http://www.iks-jena.de/mitarb/lutz/security/cryptfaq/q104.html

[Spe03] ***Diplomarbeit spemaus***, Raimund Specht, http://www.spemaus.de/studium/diplomarbeit/html/

[Tri04] ***Drängler im WLAN***, Spiro Trikaliotis, http://www.heise.de/security/artikel/49366/0

[Wiki] ***Ad hoc protocol list - Wikipedia, the free encyclopedia***, http://en.wikipedia.org/wiki/Ad_hoc_protocol_list

2. Anhang mit sortiertem Literaturverzeichnis

Angriffe

Allgemein

[Bac04] **Seminar: Sicherheit in Ad-Hoc Netzen, Thema 3, Spezielle Angriffe in Ad-Hoc Netzen,** Christian Backs, Sven Eric Neuz, http://www.sec.informatik.tu-darmstadt.de/de/lehre/SS04/seminar_adhoc/ausarbeitungen/Angriffe.pdf

[Lu02] ***Vulnerability of Wireless Routing Protocols***, Qifeng Lu, http://www.people.umass.edu/qifeng/Files_Web/Vulnerability_Qifeng Lu.pdf

Aktive Angriffe

[Aad04] ***Denial of Service resilience in ad hoc networks***, Imad Aad, Jean-Pierre Hubaux, Edward W. Knightly, http://icapeople.epfl.ch/iaad/publ/mobicom-2004.pdf

[Bel03] ***Using Link Cuts to Attack Internet Routing***, Steven M. Bellovin, Emden R. Gansner, http://www.cs.columbia.edu/~smb/papers/reroute.pdf

[Bur03] ***Ad hoc network specific attacks***, Adam Burg, http://www13.informatik.tu-muenchen.de/lehre/seminare/WS0304/UB-hs/burg-ad_hoc_specific_attacks-paper.pdf

[Hu03a] ***Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols***, Yih-Chun Hu, Adrian Perrig, David B. Johnson, http://www.ece.cmu.edu/~adrian/projects/secure-routing/wise2003.pdf

[Jak03a] ***Stealth Attacks on Ad-Hoc Wireless Networks***, Markus Jakobsson, Susanne Wetzel, Bulent Yener, http://guinness.cs.stevens.edu/~swetzel/papers/stealth.pdf

[Karl02] ***Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures***, Chris Karlof, David Wagner, http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf

[Kuz03] ***Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)***, Aleksandar Kuzmanovic, Edward W. Knightly, http://www2.ece.rice.edu/networks/papers/dos.ps.gz

[Nin03] ***How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols***, Peng Ning, Kun Sun, http://discovery.csc.ncsu.edu/pubs/TRMisuseAODV.pdf

[Wang03] ***On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol***, Weichao Wang, Yi Lu, Bharat K. Bhargava, http://www.cs.purdue.edu/homes/wangwc/ICT03wangwc.pdf

[Zhe03] ***Preventing Replay Attacks for Secure Routing in Ad Hoc Networks***, Jane Zhen, Sampalli Srinivas, ADHOC-NOW 2003, LNCS 2865, pp. 140-150, 2003

[ZhoZ04] ***Geographic Ad Hoc Routing Security: Attacks and Countermeasures***, Zhi Zhou, Kin Choong Yow, http://www.oldcitypublishing.com/FullText/AHSWNfulltext/AHSWN1.3fulltext/Zhi.pdf

Passive Angriffe

[Kong03c] ***A New Set Of Passive Routing Attacks In Mobile Ad Hoc Networks***, Jiejun Kong, Xiaoyan Hong, Mario Gerla, http://www.cs.ucla.edu/~jkong/publications/MILCOM03-jkong.ps.gz

MAC-Ebene Fehlverhalten

[Cag04a] ***On Selfish Behavior in CSMA/CA Networks***, Mario Cagalj, Saurabh Ganeriwal, Imad Aad, Jean-Pierre Hubaux, http://www.mics.org/getDoc.php?docid=978&docnum=1

[Cag04b] ***On Cheating in CSMA/CA Ad Hoc Networks***, Mario Cagalj, Saurabh Ganeriwal, Imad Aad, Jean-Pierre Hubaux http://icwww.epfl.ch/publications/documents/IC_TECH_REPORT_200427.pdf http://lcawww.epfl.ch/cagalj/SelfOrg/CagaljGAH04.pdf

[Car04] ***Detection and Prevention of MAC Layer Misbehavior in Ad Hoc Networks***, Alvaro A. Cardenas, Svetlana Radosavac and John S. Baras, http://www.glue.umd.edu/~acardena/Papers/f30-cardenasv2.pdf

[Kok00] ***An Analysis of Short-Term Fairness in Wireless Media Access Protocols***, Can Emre Koksal, Hisham Kassab, Hari Balakrishan, http://nms.lcs.mit.edu/papers/fair-sigmet00.ps, http://citeseer.ist.psu.edu/koksal00analysis.html

[Kon02] ***Multiple Access in Ad-Hoc Wireless LANs with Noncooperative Stations***, Jerzy Konorski, http://lcawww.epfl.ch/cagalj/SelfOrg/Konorski02.pdf

[Kya02] ***Detection and Handling of MAC Layer Misbehavior in Wireless Networks***, Pradeep Kyasanur, Nitin H. Vaidya, http://www.cs.huji.ac.il/labs/danss/sensor/detectionoffaults/kyasanur_2002detectionandhandling.pdf

[Kya04] ***Selfish MAC Layer Misbehavior in Wireless Networks***, Pradeep Kyasanur, Nitin H. Vaidya, http://www.crhc.uiuc.edu/wireless/papers/kyasanur2004tmc.ps

[Nan00] ***Achieving MAC Layer Fairness in Wireless Packet Networks***, Thyagarajan Nandagopal, Tae-Eun Kim, Xia Gao, Vaduvur Bharghavan, http://timely.crhc.uiuc.edu/Papers/mobicom00.ps.gz

Erkennung von Eindringlingen

Erkennung von sich fehlverhaltenden Knoten

[Bra97] ***Detecting Disruptive Routers: A Distributed Network Monitoring Approach***, Kirk A. Bradley, Steven Cheung, Nick Puketza, Biswanath Mukherjee, Ronald A. Olsson, http://citeseer.ist.psu.edu/bradley97detecting.html

[Cap03a] ***SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks***, Srdjan Capkun, Levente Buttyan, Jean-Pierre Hubaux, http://www.hit.bme.hu/~buttyan/publications/CapkunBH03sasn.pdf

[Hu02a] ***Wormhole Detection in Wireless Ad Hoc Networks***, Yih-Chun Hu, Adrian Perrig, David B. Johnson, http://citeseer.ist.psu.edu/hu02wormhole.html http://monarch.cs.rice.edu/monarch-papers/tikreport.pdf

[Just03] ***Resisting Malicious Packet Dropping in Wireless Ad-Hoc Networks***, Mike Just, Evangelos Kranakis, Tao Wan, http://citeseer.ist.psu.edu/just03resisting.html

[Kar04a] ***Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks***, Frank Kargl, Andreas Klenk, Stefan Schlott, Michael Weber, http://medien.informatik.uni-ulm.de/forschung/publikationen/esas2004.pdf

[Kar04b] ***Sensors for Detection of Misbehaving Nodes in MANETs***, Frank Kargl, Andreas Klenk, Michael Weber, Stefan Schlott, http://medien.informatik.uni-ulm.de/forschung/publikationen/dimva2004.pdf

[Miz04a] ***Detecting Malicious Routers***, Alper T. Mizrak, Keith Marzullo, Stefan Savage, http://citeseer.ist.psu.edu/699872.html

[Miz04b] ***Fault-Tolerant Forwarding in the Face of Malicious Routers***, Alper T. Mizrak, Keith Marzullo, Stefan Savage, http://citeseer.ist.psu.edu/702811.html

[Pad02] ***Secure Traceroute to Detect Faulty or Malicious Routing***, Venkata N. Padmanabhan, Daniel R. Simon, http://citeseer.ist.psu.edu/padmanabhan02secure.html

Intrusion Detection Systems (IDS)

[Bha01] ***Security Enhancement in AODV protocol for Wireless Ad Hoc Networks***, S. Bhargava, D. P. Agrawal, http://www.mcl.hu/adhoc/literature/QoS and Security/Security Enhancements in AODV protocol for Wireless Ad Hoc Networks.pdf

[BZM02] ***Trusted Routing and Intruder Identification in Mobile Ad Hoc Networks***, Bharat Bhargava, Michael Zoltowski, Pascal Meunier, http://raidlab.cs.purdue.edu/grants/cerias02.pdf

[Guh02] ***Case-Based Agents for Packet-Level Intrusion Detection in Ad Hoc Networks***, R. Guha, O. Kachirski, D.G. Schwartz, S. Stoecklin, E. Yilmaz, http://ww2.cs.fsu.edu/~yilmaz/Papers/ucffsuiscis02final.pdf

[Kle03] ***Mobile Intrusion detection in mobilen Ad-Hoc Netzwerken***, Andreas Klenk, http://net.informatik.uni-tuebingen.de/members/klenk/da_klenk.pdf

[Me01] ***Intrusion Detection: A Bibliography***, Ludovic Mé, Cédric MichelSup'elec, Rennes, http://citeseer.ist.psu.edu/484682.html

[Mit02] ***Sensor-Based Intrusion Detection for Intra-Domain Distance-Vector Routing***, Vishal Mittal, Giovanni Vigna, http://citeseer.ist.psu.edu/mittal02sensorbased.html

[Stam03] ***Real-time Intrusion Detection for Ad hoc Networks***, Ioanna Stamouli, https://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-54.pdf

[Vig04] ***An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks***, Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, http://www.acsac.org/2004/papers/140.pdf

[ZhaYo00a] ***Intrusion Detection in Wireless Ad-Hoc Networks,*** Yongguang Zhang, Wenke Lee, http://citeseer.ist.psu.edu/zhang00intrusion.html

[ZhaYo03] ***Intrusion Detection Techniques for Mobile Wireless Networks***, Yongguang Zhang, Wenke Lee, Yi-An Huang, http://www.wins.hrl.com/people/ygz/papers/winet03.pdf

Watchdog, Pathrater

[Mar00] ***Mitigating Routing Misbehavior in Mobile Ad Hoc Networks***, Sergio Marti, T.J. Giuli, Kevin Lai, Mary Baker, http://citeseer.ist.psu.edu/marti00mitigating.html

Kooperation

Allgemein

[HuaE04] ***Rethinking Incentives for Mobile Ad Hoc Networks***, Elgan Huang, Ian Wassell, Jon Crowcroft, http://www.acm.org/sigs/sigcomm/sigcomm2004/workshop_papers/pin11-huang.pdf

[Ob03] ***Stimulating Cooperative Behavior of Autonomous Devices - An Analysis of Requirements and Existing Approaches***, Philipp Obreiter Birgitta Koenig-Ries, Michael Klein, http://www.ipd.uka.de/DIANE/docs/wis03.pdf

CONFIDANT

[Buc02b] ***Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks***, Sonja Buchegger, Jean-Yves Le Boudec, http://lcawww.epfl.ch/Publications/Buchegger/BucheggerL02b.pdf

[Buc02c] ***Performance Analysis of the CONFIDANT Protocol -- Cooperation Of Nodes -- Fairness In Dynamic Ad-hoc Networks,*** Sonja Buchegger, Jean-Yves Le Boudec, http://lcawww.epfl.ch/Publications/Buchegger/TR02_01.pdf

[Buc04] ***Coping with Misbehavior in Mobile Ad-hoc Networks***, Sonja Buchegger, http://icapeople.epfl.ch/sbuchegg/sonjaThesis.pdf

Core

[Mic01] ***CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks***, Pietro Michiardi, Refik Molva, http://www.eurecom.fr/~michiard/pub/michiardi-core.pdf

[Mic03] ***Ad hoc networks security***, Pietro Michiardi, Refik Molva, http://www.eurecom.fr/~michiard/pub/michiardi-ST-journal.pdf

Nuglets, Counters

[Ban03] ***Observation-based Cooperation Enforcement in Ad-Hoc Networks***, Sorav Bansal, Mary Baker, http://arxiv.org/pdf/cs.NI/0307012

[But00] ***Enforcing Service Availability in Mobile Ad-Hoc WANs***, Levente Buttyan, Jean-Pierre Hubaux, http://www.crysys.hu/publications/files/ButtyanH2000TR00_025.pdf

[But01] ***Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks***, Levente Buttyan, Jean-Pierre Hubaux, http://lcawww.epfl.ch/Publications/Buttyan/ButtyanH02.pdf

[Fel04] ***Hidden-Action in Multi-Hop Routing***, Michal Feldman, John Chuang, http://www.eecs.harvard.edu/p2pecon/confman/papers/s3p1.pdf

[He04]***SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks***, Qi He, Dapeng Wu, Pradeep Khosla, http://www.wu.ece.ufl.edu/mypapers/WCNC04_incentive.pdf

[Jak03b] ***A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks***, Markus Jakobsson, Jean-Pierre Hubaux, Levente Buttyan, http://icawww.epfl.ch/Publications/hubaux/JakobssonHB03.pdf

[Mir03] ***Friends and Foes: Preventing Selfishness in Open Mobile Ad-Hoc Networks***, Hugo Miranda, Luis Rodrigues, http://www.di.fc.ul.pt/~ler/reports/mdc03.ps.gz

[Ob04] ***Engineering Incentive Schemes for Ad Hoc Networks- A Case Study for the Lanes Overlay***, Philipp Obreiter, Birgitta Koenig-Ries, Georgios Papadopoulos, http://www.ipd.uka.de/~obreiter/publications/2004TR4.pdf

[Sal03] ***A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks***, Naouel Ben Salem, Levente Buttyán, Jean-Pierre Hubaux, Markus Jakobsson, http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/routingpay2/routingpay2.ps

[Wey04] ***Cooperation and Accounting Strategy for Multi-hop Cellular Networks***, Attila Weyland, Torsten Braun, http://www.iam.unibe.ch/~rvs/publications/lanman04-cooperation.pdf

[Xue05] ***Channel-Relay Price Pair: Towards Arbitrating Incentives in Wireless Ad hoc Networks***, Yuan Xue, Baochun Li, Klara Nahrstedt, http://www.eecg.toronto.edu/~bli/papers/wcmc-si.pdf

[ZhoS03] ***Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks***, Sheng Zhong, Jiang Chen, Yang Richard Yang, http://www.ieee-infocom.org/2003/papers/48_04.PDF

Sicheres Routing

Überblicke und allgemein gehaltene Dokumente

[Arg02] ***Current state of secure routing for mobile ad hoc networks***, Patroklos Argyroudis,
http://ntrg.cs.tcd.ie/~argp/public/adhoc-secure-routing-slides.pdf

[Arg05] ***Secure Routing for Mobile Ad hoc Networks***, Patroklos G. Argyroudis, Donal O'Mahony,
http://www.ctvr.ie/docs/secure-adhoc-routing.pdf

[But04] ***Towards Provable Security for Ad Hoc Routing Protocols***, Levente Buttyan, Istvan Vajda,
http://www.hit.bme.hu/~buttyan/publications/ButtyanV04sasn.pdf

[Cho03] ***Security problems for ad hoc routing protocols***, Jong Youl Choi,
http://www.cs.indiana.edu/~jychoi/files/Security_problems_for_ad_hoc_routing_protocols.pdf

[Hu04]***A Survey of Secure Wireless Ad Hoc Routing***, Yih-Chun Hu, Adrian Perrig,
http://www.ece.cmu.edu/~adrian/projects/AdHocSurvey.pdf

[Ink04] ***New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes***, Kai Inkinen,
http://www.tml.hut.fi/Studies/T-110.551/2004/papers/Inkinen.pdf

[LiHu02] ***Secure Routing in Wired Networks and Wireless Ad Hoc Networks***, Huaizhi Li, Zhenliu Chen, Xiangyang Qin, Chengdong Li, Hui Tan,
http://cs.engr.uky.edu/~singhal/term-papers/routing.pdf

[Put04a] ***Preventive and Corrective Protection for Mobile Ad Hoc Routing Protocols***, Ricardo Puttini, Rafael de Sousa, Ludovic Me,
http://www.redes.unb.br/material/TopicosTelecom/papers/parte2/paper6.pdf

[Put04b] ***On the Vulnerabilities and Protection of Mobile Ad Hoc Network Routing Protocols***, Ricardo Puttini, Rafael de Sousa, Ludovic Me,
http://www.rennes.supelec.fr/rennes/si/equipe/lme/PUBLI/PMS04a.pdf

[Roy99] ***A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks***, Elizabeth M. Royer, Chai-Keong Toh,
http://ntrg.cs.tcd.ie/htewari/papers/royer.pdf

[Smi97] ***Securing Distance-Vector Routing Protocols***, Bradley R. Smith,
http://www.cse.ucsc.edu/research/ccrg/publications/brad.masters.pdf

[Wang03] ***On Security Study of Two Distance Vector Routing Protocols for Mobile Ad Hoc Networks***, Weichao Wang, Yi Lu, Bharat K. Bhargava,
http://www.cs.purdue.edu/homes/wangwc/PerCom03wangwc.pdf

[YanH04] ***Security in Mobile Ad Hoc Networks: Challenges and Solutions***, Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang, http://www.cs.ucla.edu/wing/publication/papers/Yang.WC04.pdf

Proaktiv (table driven)

[Bink96] ***Authenticated Ad Hoc Routing at the Link Layer for Mobile Systems***, Jim Binkley, William Trost, http://www.cs.pdx.edu/~jrb/jrb.papers/adhoc2/adhoc2.ps

[HuaD] ***Secure Link State Routing Protocol: A Framework for Network Survivability***, Dijiang Huang, Amit Sinha, Deep Medhi, http://conrel.sice.umkc.edu/HRP/conference/acmws_RSv4.pdf

[Hu02b] ***SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks***, Yih-Chun Hu, David B. Johnson, Adrian Perrig, http://www.ece.cmu.edu/~adrian/projects/secure-routing/wmcsa02.pdf

[Lot01] ***Stochastic Routing in Ad Hoc Wireless Networks***, Christopher Lott, Demosthenis Teneketzis, http://www.eecs.umich.edu/techreports/systems/cspl/cspl-331.ps.gz

[WanT04] ***S-RIP: A Secure Distance Vector Routing Protocol***, Tao Wan, Evangelos Kranakis, P.C. van Oorschot, http://www.scs.carleton.ca/~kranakis/Papers/tao-srip.pdf

Reaktiv (on demand)

[Acs05] ***Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks***, Gergely Acs, Levente Buttyan, Istvan Vajda, http://eprint.iacr.org/2004/159.pdf

[Awe02] ***An On-Demand Secure Routing Protocol Resilient to Byzantine Failures***, Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru, Herbert Rubens, http://www.cnds.jhu.edu/pub/papers/wise2002_sec_routing.pdf

[Awe03a] ***ODSBR: An On-Demand Secure Byzantine Routing Protocol***, Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru, Herbert Rubens, http://www.cnds.jhu.edu/research/networks/archipelago/publications/ODSBR-Awerbuch-TechReport1-2003.pdf

[Awe04a] ***Mitigating Byzantine Attacks in Ad Hoc Wireless Networks***, Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru, Herbert Rubens, http://www.cnds.jhu.edu/research/networks/archipelago/publications/Awerbuch-MitigatingByzantine-TechReport1-March2004.pdf

http://citeseer.ist.psu.edu/661767.html

[Awe04b] ***Swarm Intelligence Routing Resilient to Byzantine Adversaries***, Baruch Awerbuch, David Holmer, Herbert Rubens, http://www.cnds.jhu.edu/research/networks/archipelago/publications/AHR-SwarmIntelligenceByzantineRouting-IZS2004.pdf

[Avr04] ***Highly Secure and Efficient Routing***, Ioannis Avramopoulos, Hisashi Kobayashi, Randolph Wang, Arvind Krishnamurthy, http://lambda.cs.yale.edu/cs425/doc/byzantine.pdf http://lambda.cs.yale.edu/~arvind/papers/amendment.pdf

[Bon04] ***Securing Ad Hoc Networks Using Ariadne***, Javier Bonny, Mounir Krichane, http://lasecwww.epfl.ch/securityprotocols/adhoc/ariadne_report.pdf

[Cap03b] ***BISS: Building Secure Routing out of an Incomplete Set of Security Associations***, Srdjan Capkun, Jean-Pierre Hubaux, http://lcawww.epfl.ch/Publications/Capkun/CapkunH03_wise.pdf

[Dah01] ***A Secure Routing Protocol for Ad Hoc Networks***, Bridget Dahill, Brian Neil Levine, Elizabeth Royer, Clay Shields, ftp://ftp.cs.umass.edu/pub/techrept/techreport/2001/UM-CS-2001-037.ps

[Hu01a] ***Implicit Source Routes for On-Demand Ad Hoc Network Routing***, Yih-Chun Hu, David B. Johnson, http://monarch.cs.rice.edu/monarch-papers/mobihoc01-flow.ps

[Hu02c] ***Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks***, Yih-Chun Hu, Adrian Perrig, David B. Johnson, http://citeseer.ist.psu.edu/531013.html http://www.ece.cmu.edu/~adrian/projects/secure-routing/ariadne.pdf

[Kar05] ***Secure Dynamic Source Routing***, Frank Kargl, Alfred Geiß, Stefan Schlott, Michael Weber, http://medien.informatik.uni-ulm.de/forschung/publikationen/hicss38.pdf http://medien.informatik.uni-ulm.de/forschung/publikationen.html

[Kong03a] ***An Anonymous On Demand Routing Protocol with Untraceable Routes for Mobile Ad-hoc Networks***, Jiejun Kong, Xiaoyan Hong, Mario Gerla, http://www.cs.ucla.edu/~jkong/publications/CSD-TR030020.pdf

[Kong03b] ***ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks***, Jiejun Kong, Xiaoyan Hong, http://www.sigmobile.org/mobihoc/2003/papers/p291-kong.pdf http://www.cs.ucla.edu/~jkong/publications/MOBIHOC03-jkong.pdf

[Pap02a] ***The Secure Routing Protocol (SRP) for Ad Hoc Networks***, Panagiotis Papadimitratos, Zygmunt J. Haas, Prince Samar, http://www.people.cornell.edu/pages/pp59/Docs/draft-secure_routing_for_ad_hoc_networks-00.pdf

[Pat05] ***Secure Routing and Intrusion Detection in Ad Hoc Networks***, Anand Patwardhan, Michaela Iorga, Jim Parker, Tom Karygiannis, http://ebiquity.umbc.edu/v2.1/_file_directory_/papers/155.pdf

[San02] ***A Secure Routing Protocol for Ad Hoc Networks***, Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, http://www.ece.cmu.edu/~adrian/731-sp05/readings/SDLSB-aran.pdf

[Yi01a] ***Security-aware Routing Protocol for Wireless Ad Hoc Networks***, Seung Yi, Prasad Naldurg, Robin Kravets, http://www-sal.cs.uiuc.edu/~rhk/pubs/SCI2002.pdf

[Yi02a] ***Integrating Quality of Protection into Ad Hoc Routing Protocols***, Seung Yi, Prasad Naldurg, Robin Kravets, http://mobius.cs.uiuc.edu/publications/sci02.ps

[Zap02a] ***Secure Ad hoc On-Demand Distance Vector Routing***, Manel Guerrero Zapata, http://ant.epsevg.upc.es/~tarom/guerrero_mc2r_2002.ps

[Zap05] ***Secure Ad hoc On-Demand Distance Vector (SAODV) Routing***, Manel Guerrero Zapata, http://ant.epsevg.upc.es/~tarom/draft-guerrero-manet-saodv-03.txt

[ZhaYa05] ***Anonymous Communications in Mobile Ad Hoc Networks***, Yanchao Zhang, Wei Liu, Wenjing Lou, http://ece.wpi.edu/~wjlou/publication/INFOCOM05_Zhang.pdf

[ZhuB04] ***Anonymous Secure Routing in Mobile Ad-Hoc Networks***, Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng, http://www.comp.nus.edu.sg/~mohan/papers/sec_rout.pdf

Hierarchisch

[Pap03d] ***Secure Link State Routing for Mobile Ad Hoc Networks***, Panagiotis Papadimitratos, Zygmunt J. Haas, http://people.ece.cornell.edu/~haas/wnl/Publications/saahn03.pdf

Hybrid

[Yau04] ***2HARP: A Secure Routing Protocol For Mobile Ad Hoc Networks***, Po-Wah Yau, Chris J. Mitchell, http://www.isg.rhul.ac.uk/~cjm/2asrpf.pdf

Geographisch

[Bla02] ***Self Organized Terminode Routing***, Ljubica Blazevic, Silvia Giordano, Jean-Yves Le Boudec, http://lcawww.epfl.ch/Publications/Blazevic/BlazevicGL01a.ps

[Bar01] ***Robust Position-Based Routing in Wireless Ad Hoc Networks with Irregular Transmission Ranges***, Lali Barrière, Pierre Fraigniaud, Lata Narayanan, Jaroslav Opatrny, http://www.lri.fr/~pierre/POSTSCRIPTS/WCMC_special_issue.ps

[Car03] ***Secure Position Aided Ad hoc Routing Protocol***, Stephen Carter, Alec Yasinsac, http://www.cs.fsu.edu/~yasinsac/Papers/CY03.pdf

[Hub01a] ***Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project***, Jean-Pierre Hubaux, Thomas Gross, Jean-Yves Le Boudec, Martin Vetterli, http://lcawww.epfl.ch/Publications/Hubaux/HubauxLGV01.pdf

Protokollerweiterungen

[Awe03b] ***Provably Secure Competitive Routing against Proactive Byzantine - Adversaries via Reinforcement Learning***, Baruch Awerbuch, David Holmer, Herbert Rubens,
http://www.cnds.jhu.edu/research/networks/archipelago/publications/LearningByzantineRouting-TechnicalReport2.pdf

[Hu01b] ***Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks***, Yih-Chun Hu, Adrian Perrig, David B. Johnson,
http://monarch.cs.rice.edu/monarch-papers/infocom03.pdf

[Hu02d] ***Ensuring Cache Freshness in On-Demand Ad Hoc Network Routing Protocols***, Yih-Chun Hu, David B. Johnson,
http://monarch.cs.rice.edu/monarch-papers/pomc.pdf

[Hu03b] ***Efficient Security Mechanisms for Routing Protocols***, Yih-Chun Hu, Adrian Perrig, David B. Johnson,
http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/4.pdf

[Lee02] ***Robust Routing in Wireless Ad Hoc Networks***, Seungjoon Lee, Minho Shin, Bohyung Han,
http://www.cs.umd.edu/~mhshin/paper/robust_routing_lee_han_shin.pdf

[Mat04] ***Securing Routing in Open Networks Using Secure Traceroute***, Gaurav Mathur, Venkata N. Padmanabhan, Daniel R. Simon,
http://citeseer.ist.psu.edu/699082.html
http://www.research.microsoft.com/~padmanab/papers/msr-tr-2004-66.pdf

[Pap02b] ***Secure Routing for Mobile Ad hoc Networks***, Panagiotis Papadimitratos, Zygmunt J. Haas,
http://people.ece.cornell.edu/~haas/wnl/Publications/cnds02.pdf

[Pap03a] ***Secure message transmission in mobile ad hoc networks***, Panagiotis Papadimitratos, Zygmunt J. Haas,
http://www.cs.huji.ac.il/labs/danss/sensor/adhoc/routing/papadimitratos_2003securemessage.pdf

[Pap03b] ***Secure Data Transmission in Mobile Ad Hoc Networks***, Panagiotis Papadimitratos, Zygmunt J. Haas,
http://people.ece.cornell.edu/~haas/wnl/Publications/wise03.pdf

[Per02a] ***The TESLA Broadcast Authentication Protocol***, Adrian Perrig, Ran Canetti, J. D. Tygar, Dawn Song,
http://www.ece.cmu.edu/~adrian/projects/tesla-cryptobytes/tesla-cryptobytes.ps.gz

[Put03] ***Certification and Authentication Services for Securing MANET Routing Protocols***, Ricardo Staciarini Puttini, Ludovic Me, Rafael Timoteo de Sousa,
http://www.rennes.supelec.fr/ren/rd/ssir/publis/mwcn03_puttini_me_desousa.pdf

[Ram02] ***Intrusion Resistant Ad Hoc Wireless Networks***, R. Ramanujan, S. Kudige, S. Takkella, T. Nguyen, F. Adelstein, http://www.eecis.udel.edu/~cshen/861/papers/milcom_2002_paper.pdf

[Son03] ***Secure Routing with Tamper Resistant Module for Mobile Ad Hoc Networks***, Joo-Han Song, Yoji Kawamoto, Vincent Wong, Victor Leung, http://www.sigmobile.org/mobihoc/2003/posters/p243-song.pdf

[Zap02b] ***Securing Ad hoc Routing Protocols***, Manel Guerrero Zapata, N. Asokan, http://ant.epsevg.upc.es/~tarom/guerrero_wise_2002.ps.gz

[ZhuS03] ***LHAP: A Lightweight Hop-by-Hop Authentication Protocol For Ad-Hoc Networks***, Sencun Zhu, Shouhuai Xu, Sanjeev Setia, Sushil Jajodia, http://www.cs.utsa.edu/~shxu/mwn03.pdf

Vertrauen

[Bha02] ***Authorization Based on Evidence and Trust***, Bharat Bhargava, Yuhui Zhong, http://www.cs.purdue.edu/homes/zhong/papers/Authorization.pdf

[Esc02a] ***On Trust Establishment in Mobile Ad-Hoc Networks***, Laurent Eschenauer, Virgil D. Gligor, John Baras, http://www.glue.umd.edu/afs/glue.umd.edu/home/enee/faculty/gligor/pub/cambridge02.ps

[Lan03] ***When Trust Does Not Compute - The Role of Trust in Ubiquitous Computing***, Marc Langheinrich, http://www.vs.inf.ethz.ch/publ/papers/ubicomp03-trust.pdf

[Lam01] ***Understanding Trust and Security***, Pradip Lamsal, http://www.cs.helsinki.fi/u/lamsal/asgn/trust/UnderstandingTrustAndSecurity.pdf

[LiX] ***Trust Model Based Self-Organized Routing Protocol for Secure Ad Hoc Networks***, Xiaoqi Li, http://www.cs.cuhk.hk/~lyu/student/phd/gigi/term2.pdf

[LiuZ04] ***A Dynamic Trust Model for Mobile Ad Hoc Networks***, Zhaoyu Liu, Anthony W. Joy, Robert A. Thompson, http://www.sis.uncc.edu/~zhliu/Research/Papers/ftdcs.pdf

[Pir04] ***Establishing Trust In Pure Ad-hoc Networks***, Asad Amir Pirzada, Chris McDonald, http://crpit.com/confpapers/CRPITV26Pirzada1.pdf

[Yao03] ***Trust Management for Widely Distributed Systems***, Walt Teh-Ming Yao, http://www.cl.cam.ac.uk/Research/SRG/opera/publications/Theses/wtmy2.pdf

Keymanagement, Authentication

Allgemein

[Bind] ***Decentralized Key Management in Ad Hoc Networks***, Joseph Binder, Hans-Peter Bischof, Alan Kaminsky, http://www.cs.rit.edu/~anhinga/Ungulate/publications/key-management-position.pdf

[Cap03c] ***Mobility Helps Security in Ad Hoc Networks***, Srdjan Capkun, Jean-Pierre Hubaux, Levente Buttyan, http://www.sigmobile.org/mobihoc/2003/papers/p46-capkun.pdf

[Fok02] ***Key management in Ad Hoc Networks***, Klas Fokine, http://www.ep.liu.se/exjobb/isy/2002/3322/exjobb.pdf

[Sin04] ***Key Management Protocols for Wireless Networks***, Mukesh Singhal, Rendong Bai, Yun Lin, Yongwei Wang, Mengkun Yang, Qingyu Zhang, http://www.cs.umbc.edu/courses/graduate/CMSC691A/Spring04/papers/keymanagement-survey-final.pdf

[Wei01] ***A Distributed Light-Weight Authentication Model for Ad-hoc Networks***, Andre Weimerskirch, Gilles Thonet, http://citeseer.ist.psu.edu/andr02distributed.html http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/adhocauth.pdf

Verteiltes Schlüsselmangement

[Bech04] ***A Cluster-Based Security Architecture for Ad Hoc Networks***, M. Bechler, H.-J. Hof, D. Kraft, F. Pählke, L. Wolf, http://www.ieee-infocom.org/2004/Papers/50_1.PDF

[Bis03] ***A new Framework for Building Secure Collaborative Systems in Ad Hoc Network***, Hans-Peter Bischof, Alan Kaminsky, Joseph Binder, http://www.cs.rit.edu/~anhinga/publications/montreal_October_03.pdf

[Kong01] ***Providing robust and ubiquitous security support for mobile ad-hoc networks***, Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, Lixia Zhang, http://www.cs.ucla.edu/~jkong/publications/ICNP01-jkong.pdf

[Kur04] ***Ensuring Security in Ad Hoc Networks***, Jimmy Kurian, http://www.tml.hut.fi/Studies/T-110.551/2004/papers/Kurian.pdf

[Leh03] ***Shared RSA Key Generation in a Mobile Ad Hoc Network***, Brian Lehane , Linda Doyle , Donal O'Mahony, http://ntrg.cs.tcd.ie/lehaneb/papers/milcom03.pdf

[Leh05] ***Ad Hoc Key Management Infrastructure***, Brian Lehane, Linda Doyle , Donal O'Mahony, http://ntrg.cs.tcd.ie/lehaneb/papers/itcc05.pdf

[Luo02] ***Self-securing Ad Hoc Wireless Networks***, Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu and Lixia Zhang, http://www.gta.ufrj.br/~eric/tese/artigos/ISCC02.pdf http://www.cs.huji.ac.il/labs/danss/sensor/adhoc/luo_2002selfsecuring.pdf

[Mor03] ***Certificate Management in Ad hoc Networks***, Matei Ciobanu Morogan, Sead Muftic, http://www.dsv.su.se/~matei/bin/4 – 2i1279/L8_AC5.pdf

[Pri03] ***Secure Long Term Communities In Ad Hoc Networks***, Nicolas Prigent, Christophe Bidan, Jean-Pierre Andreaux, Olivier Heen, http://www.rennes.supelec.fr/ren/perso/nprigent/papers/SASN2003.pdf

[Schi04] ***Key Management and Distribution for Threshold Cryptography Schemes***, Fabian Schilcher, http://www13.informatik.tu-muenchen.de/lehre/seminare/WS0304/UB-hs/FabianSchilcher_KeyManagement_report.pdf

[Xu04] ***Locality Driven Key Management Architecture for Mobile Ad-hoc Networks***, Gang Xu, Liviu Iftode, http://www.ececs.uc.edu/~cdmc/mass/mass2004/34810.pdf

[Yi01b] ***Practical PKI for Ad Hoc Wireless Networks***, Seung Yi, Robin Kravets, http://ncstrl.cs.uiuc.edu/Dienst/Repository/2.0/Body/ncstrl.uiuc_cs/UIUCDCS-R-2002-2273/pdf

[Yi02b] ***Key Management for Heterogeneous Ad Hoc Wireless Networks***, Seung Yi, Robin Kravets, http://www-sal.cs.uiuc.edu/~rhk/pubs/tr-2290-1734.pdf

[Yi03a] ***MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks***, Seung Yi, Robin Kravets, http://middleware.internet2.edu/pki03/presentations/06.pdf

[Yi03b] ***Composite Key Management for Ad Hoc Networks***, Seung Yi, Robin Kravets, http://ncstrl.cs.uiuc.edu/Dienst/Repository/2.0/Body/ncstrl.uiuc_cs/UIUCDCS-R-2003-2392/pdf

[Zap04] ***Key Management and Delayed Verification for Ad hoc Networks***, Manel Guerrero Zapata, http://ant.epsevg.upc.es/~tarom/guerrero_tiw_2004.ps

[ZhaYa05] ***AC-PKI: Anonymous and Certificateless Public Key Infrastructure for Mobile Ad Hoc Networks***, Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, Younggoo Kwon, http://www.ecel.ufl.edu/~zhang/files/ac-ICC.pdf

[ZhoL99] ***Securing Ad Hoc Networks***, Lidong Zhou, Zygmunt J. Haas, http://www.cs.cornell.edu/home/ldzhou/adhoc.pdf

[ZhoL00] ***COCA: A Secure Distributed Online Certification Authority***, Lidong Zhou, Fred B. Schneider, Robbert van Renesse, http://www.cs.cornell.edu/fbs/publications/cocaTOCS.pdf

[ZhuB]***Providing Efficient Certification Services Against Active Attacks in Ad Hoc Networks,*** Bo Zhu, Guilin Wang, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng, http://citeseer.ist.psu.edu/722019.html http://www.comp.nus.edu.sg/~mohan/papers/ipccc.pdf

[ZhuS03] ***Establishing Pair-wise Keys For Secure Communication in Ad Hoc Networks: A Probabilistic Approach (2003)***, Sencun Zhu, Shouhuai Xu, Sanjeev Setia, Sushil Jajodia, http://mason.gmu.edu/~szhu1/pke.ps http://citeseer.ist.psu.edu/zhu03establishing.html

Selbstorganisierende Infrastruktur (Web of Trust, Small worlds)

[Abe03] ***Identifying Peers Using a Self-Contained Directory***, Karl Aberer, Anwitaman Datta, Manfred Hauswirth, http://citeseer.ist.psu.edu/aberer03identifying.html http://www.p-grid.org/Papers/TR-IC-2003-25.pdf

[Cap02a] ***Small Worlds in Security Systems: an Analysis of the PGP Certificate Graph***, Srdjan Capkun, Levente Buttya n, Jean-Pierre Hubaux, http://citeseer.ist.psu.edu/capkun02small.html http://www.crysys.hu/publications/files/CapkunBH2002nspw.pdf

[Cap02b] ***Self-Organized Public-Key Management for Mobile Ad Hoc Networks,*** Srdjan Capkun, Levente Buttyan, Jean-Pierre Hubaux, http://citeseer.ist.psu.edu/capkun03selforganized.html

[Hub01b] ***The Quest for Security in Mobile Ad Hoc Networks,*** Jean-Pierre Hubaux, Levente Buttyan, Srdan Capkun, http://citeseer.ist.psu.edu/hubaux01quest.html http://www.crysys.hu/publications/files/HubauxBC2001a.ps

[WanW03] ***Self-managed heterogeneous certification in mobile ad hoc networks***, Weihong Wang, Ying Zhu, Baochun Li, http://www.eecg.toronto.edu/~bli/papers/vtc03.pdf

Resurrecting Duckling

[Bal02] ***Talking To Strangers: Authentication in Ad-Hoc Wireless Networks***, Dirk Balfanz, D. K. Smetters, Paul Stewart, H. Chi Wong, http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/balfan.pdf

[Sta99] ***The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks***, Frank Stajano, Ross Anderson, http://citeseer.ist.psu.edu/stajano99resurrecting.html

[Sta00] ***The Resurrecting Duckling what next?***, Frank Stajano, http://www-lce.eng.cam.ac.uk/publications/files/tr.2000.4.pdf

Kryptobasierte Identitäten

[Bob02] ***Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks***, Rakesh Babu Bobba, Laurent Eschenauer, Virgil Gligor, William Arbaugh, http://www.glue.umd.edu/afs/glue.umd.edu/home/enee/faculty/gligor/pub/SDSR-02.ps
http://citeseer.csail.mit.edu/bobba02bootstrapping.html
http://citeseer.ist.psu.edu/bobba02bootstrapping.html

Schlüsselmanagement mit ID-basierter Kryptographie

[Boy03] ***Multipurpose Identity-Based Signcryption***, Xavier Boyen, http://citeseer.ist.psu.edu/647307.html
http://eprint.iacr.org/2003/163.ps.gz

[Cul04] ***Efficient and Forward-Secure Identity-Based Signcryption***, Noel McCullagh, Paulo S. L. M. Barreto, http://citeseer.ist.psu.edu/mccullagh04efficient.html
http://eprint.iacr.org/2004/117.ps.gz

[Cai] ***Promoting Identity-Based Key Management in Wireless Ad Hoc Network,*** Lin Cai, Jianping Pan, Xuemin (Sherman) Shen, Jon W. Mark, http://bbcr.uwaterloo.ca/~cai/tr-ibc.pdf

[Khal03] ***Toward Secure Key Distribution in Truly Ad-Hoc Networks***, Aram Khalili, Jonathan Katz, William A. Arbaugh, http://www.cs.nmt.edu/~cs553/paper8.pdf

[Mcc04] ***A New Two-Party Identity-Based Authenticated Key Agreement***, Noel McCullagh, Paulo S. L. M. Barreto, http://eprint.iacr.org/2004/122.pdf

Keyestablishment Protokolle, Gruppenkeymanagement

[Ant02] ***Group Key Establishment in Wireless Ad Hoc Networks***, Eric Ricardo Anton, Otto Carlos Muniz Bandeira Duarte, http://www.gta.ufrj.br/ftp/gta/TechReports/AnDu02b.pdf

[Aso99] ***Key Agreement in Ad-hoc Networks***, N. Asokan, Philip Ginzboorg, http://www.semper.org/sirene/people/asokan/research/ccr.ps.gz

[Hie01] ***Efficient key agreement for ad-hoc networks***, Maarit Hietalahti, http://www.tcs.hut.fi/~mhietala/mhietala_mt.ps

[Hie] ***Key Establishment in Ad-Hoc Networks***, Maarit Hietalahti, http://www.tcs.hut.fi/~mhietala/KeyMan.ps

[Kak] ***Cryptographic Reflection***, Pankaj Kakkar, Carl A. Gunter, http://www.cis.upenn.edu/~switchware/papers/cr.pdf

[Kor04] ***Multicast security in ad hoc networks***, Pavel Korshunov, http://www.comp.nus.edu.sg/~cs4274/termpapers/0405-I/paper-13.pdf

[Laz03] ***Location-Aware Secure Wireless Multicast in Ad-Hoc Networks under Heterogeneous Path-loss***, Loukas Lazos, Radha Poovendran, Gregory H. Cirincione, https://www.ee.washington.edu/techsite/papers/documents/UWEETR-2003-0012.pdf

[LiXY02] ***Efficient Hybrid Key Agreement Protocol for Wireless Ad Hoc Networks***, Xiang-Yang Li, Yu Wang, Ophir Frieder, http://www.cs.iit.edu/~xli/paper/Conf/KeyAgree.pdf

[Mak00] ***Robust Membership Management for Ad-hoc Groups***, Silja Mäki, Tuomas Aura, Maarit Hietalahti, http://research.microsoft.com/users/tuomaura/Publications/maki-aura-hietalahti-nordsec00.pdf

[Per99] ***Efficient collaborative key management protocols for secure autonomous group communication***, Adrian Perrig, International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99), 1999

[Raf03] ***A Survey of Key Management for Secure Group Communication***, Sandro Rafaeli, David Hutchison, http://www.ece.cmu.edu/~adrian/731-sp04/readings/RH-group-key-est.pdf

[Rhe05] ***A Group Key Management Architecture for Mobile Ad-hoc Wireless Networks***, Kyung-Hyune Rhee, Young Ho Park, Gene Tsudik, http://www.iis.sinica.edu.tw/JISE/2005/200503_09.pdf

[Ver04] ***Progressive Authentication in Ad Hoc Networks***, Raja Rai Singh Verma, Donal O'Mahony, Hitesh Tewari, https://www.cs.tcd.ie/~omahony/euwi04.pdf

[Won00] ***Secure Group Communications Using Key Graphs***, Chung Kei Wong, Mohamed Gouda, Simon S. Lam, http://www.cs.utexas.edu/users/lam/Vita/IEEE/WGL00.pdf

[YanW] ***Secure Key Agreement for Group Communications***, Wen-Her Yang, Shiuh-Pyng Shieh, http://dsns.csie.nctu.edu.tw/ssp/docs/An Efficient Key Agreement Protocol for Group Communications.pdf

[Yas02a] ***Modeling Protocols for Secure Group Communication in Ad Hoc Networks (Extended Abstract)***, Alec Yasinsac, James A. Davis, http://www.cs.fsu.edu/~yasinsac/Papers/YD02.pdf
[Yas02b] ***A Family of Protocols for Group Key Generation in Ad Hoc Networks***, Alec Yasinsac, Vikram Thakur, Stephen Carter, Ilkay Cubukcu, http://www.cs.fsu.edu/~yasinsac/Papers/YTCC02.pdf

[ZhuS04] ***GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks***, Sencun Zhu, Sanjeev Setia, Shouhuai Xu, Sushil Jajodia, http://citeseer.ist.psu.edu/zhu04gkmpan.html http://www.cse.psu.edu/~szhu/papers/gkmpan.pdf

Sonstige Dokumente

[Ake02] ***Selfish Behavior and Stability of the Internet: A Game-Theoretic Analysis of TCP***, Aditya Akella, Srinivasan Seshan, Richard Karp, Scott Shenker, Christos Papadimitriou, http://lcawww.epfl.ch/cagalj/SelfOrg/Akella02.pdf

[Bla01] ***Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes***, Ljubica Blazevic, Levente Buttyan, Srdan Capkun, Silvia Giordano, Jean-Pierre Hubaux, Jean-Yves Le Boudec, http://lcawww.epfl.ch/Publications/Blazevic/BlazevicBCGHL01.ps

[Buc02a] ***Cooperative Routing in Mobile Ad-hoc Networks: Current Efforts Against Malice and Selfishness***, Sonja Buchegger, Jean-Yves Le Boudec, http://www.mics.org/getDoc.php?docid=343&docnum=1

[But02] ***Report on a Working Session on Security in Wireless Ad Hoc Networks***, Levente Buttyan, Jean-Pierre Hubaux, http://citeseer.ist.psu.edu/buttyfin02report.html http://www.crysys.hu/publications/files/ButtyanH2002mc2r.pdf

[Gah04] ***Secure Ad Hoc Networking***, Claes Gahlin, http://www.cs.umu.se/education/examina/Rapporter/ClaesGahlin.pdf

[He] ***Quest for Personal Control over Mobile Location Privacy***, Qi He, Dapeng Wu, Pradeep Khosla, http://www.wu.ece.ufl.edu/mypapers/IEEE_COM_MAG_location.pdf

[Hof02] ***Optimierung und Evaluation eines Sicherheitskonzepts für mobile Ad-hoc-Netze***, Hans-Joachim Hof, http://www.tm.uka.de/de/~hof/papers/DA_Achim_Hof.doc

[Hub99] ***The Terminode Project: Towards Mobile Ad-Hoc WAN***, J. P. Hubaux, J. Y. Le Boudec, S. Giordano, M. Hamdi, http://lcawww.epfl.ch/Publications/Hubaux/HubauxLGH99.ps

[Jue] ***Minimalist Cryptography for Low-Cost RFID Tags***, Ari Juels, http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/minimalist/Minimalist.pdf

[Kar03] ***Sicherheit in Mobilen Ad hoc Netzwerken***, Frank Kargl, http://medien.informatik.uni-ulm.de/~frank/research/dissertation.pdf

[Kong02a] ***Adaptive Security for Multi-layer Ad-hoc Networks***, Jiejun Kong, Haiyun Luo, Kaixin Xu, Daniel Lihui Gu, Mario Gerla, Songwu Lu, http://www.cs.ucla.edu/NRL/wireless/PAPER/wcmc02-onr.ps.gz

[Kong02b] ***Providing Real-time Security Support for Multi-level Ad-hoc Networks***, Jiejun Kong, Mario Gerla, http://www.cs.ucla.edu/NRL/wireless/uploads/jkong-milcom02.pdf

[Mac01] ***Game Theory and the Design of Self-Configuring, Adaptive Wireless Networks***, Allen B. MacKenzie, Stephrn B. Wicker, http://lcawww.epfl.ch/cagalj/SelfOrg/MacKenzieW01.pdf

[Mol] ***Security in Ad hoc Networks***, Refik Molva, Pietro Michiardi, http://www.eurecom.fr/~michiard/pub/michiardi-pwc-survey.pdf

[Nga02] ***Secure Cooperative Routing in Mobile Ad-hoc Networks***, C.H. Ngai, http://www.cs.cuhk.hk/~lyu/student/mphil/edith/term1.pdf

[Pap03c] ***Securing Mobile Ad Hoc Networks***, Panagiotis Papadimitratos, Zygmunt J. Haas, http://people.ece.cornell.edu/haas/wnl/Publications/crc03_1.pdf

[Rie03] ***Security in Ad-hoc Networks: Protocols and Elliptic Curve Cryptography on an Embedded Platform***, Ingo Riedel, http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/theses/da_riedel.pdf

[Sas03] ***Secure Verification of Location Claims***, Naveen Sastry, Umesh Shankar, David Wagner, http://www.cs.berkeley.edu/~nks/locprove/locprove-wise.ps

[Sta03] ***The Butt of the Iceberg: Hidden Security Problems of Ubiquitous Systems***, Frank Stajano, Jon Crowcroft, http://www.cl.cam.ac.uk/Teaching/2003/AdvSysTop/iceberg.pdf

[Vog05] ***Small Worlds and the Security of Ubiquitous Computing***, Harald Vogt, http://www.vs.inf.ethz.ch/publ/papers/hvogt-smallw-2005.pdf

[YanZ]***Security in Ad Hoc Networks***, Zheng Yan, http://keskus.hut.fi/opetus/s38030/k02/Papers/14-Zheng.pdf

[ZhaYo00b] ***Heterogeneous Networking: A New Survivability Paradigm***, Yongguang Zhang, Son K. Dao, Harrick Vin, Lorenzo Alvisi, Wenke Lee, http://www.cs.utexas.edu/users/lorenzo/papers/NSPW-pre.pdf

Dokumente zu Sensornetzen

[And] ***Key Infection: Smart Trust for Smart Dust***, Ross Anderson, Haowen Chan, Adrian Perrig
http://www-2.cs.cmu.edu/~haowen/key-infection.pdf

[Avi04] ***Efficient and Robust Query Processing in Dynamic Environments Using Random Walk Techniques***, Chen Avin, Carlos Brito,
http://www.cs.ucla.edu/~avin/papers/efficient.pdf

[Bas01] ***Secure Pebblenets***, Stefano Basagni, Kris Herrin, Danilo Bruschi, Emilia Rosti,
http://www.cs.huji.ac.il/labs/danss/sensor/adhoc/basagani_2001securepebblenets.pdf

[Cam05] ***Key Distribution Mechanisms for Wireless Sensor Networks: a Survey***, Seyit A. Camtepe, Bulent Yener, http://www.cs.rpi.edu/research/pdf/05-07.pdf

[Cap04] ***Secure Positioning in Sensor Networks***, Srdjan Capkun, Jean-Pierre Hubaux, http://www.terminodes.org/getDoc.php?docid=692&docnum=1

[Car00] ***Constraints and Approaches for Distributed Sensor Network Security***, David W. Carman, Peter S. Kruus, Brian J. Matt,
http://www.cs.umbc.edu/courses/graduate/CMSC691A/Spring04/papers/nailabs_report_00-010_final.pdf

[Chan03] ***Random Key Predistribution Schemes for Sensor Networks***, Haowen Chan, Adrian Perrig, Dawn Song,
http://www-2.cs.cmu.edu/~haowen/chan_randomkey.pdf

[Chan]***Key Distribution Techniques For Sensor Networks***, Haowen Chan, Adrian Perrig, Dawn Song, http://citeseer.ist.psu.edu/692195.html

[Chan05] ***PIKE: Peer Intermediaries for Key Establishment in Sensor Networks***, Haowen Chan, Adrian Perrig,
http://sparrow.ece.cmu.edu/~adrian/projects/pike.pdf

[Chen00] ***Security and Deployment Issues in a Sensor Network***, Mike Chen, Weidong Cui, Victor Wen, Alec Woo,
http://www.cs.berkeley.edu/~wdc/classes/cs294-1-report.pdf

[Deb03] ***Information assurance in sensor networks***, Budhaditya Deb, Sudeept Bhatnagar, Badri Nath,
http://www.research.rutgers.edu/~bdeb/wsna2003.pdf

[Den03] ***INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks***, Jing Deng, Richard Han, Shivakant Mishra,
http://www.cs.colorado.edu/~rhan/INSENS.pdf

[Du03a] ***A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks***, Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod Varshney, http://www.cis.syr.edu/~wedu/Research/paper/ccs10_sensor.pdf

[Du03b] ***A Witness-Based Approach For Data Fusion Assurance In Wireless Sensor Networks***, Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, Pramod Varshney, http://www.cis.syr.edu/~jdeng01/fusion_globecom03.pdf

[Du04]***A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge***, Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, Pramod Varshney, http://www.cis.syr.edu/~wedu/Research/paper/infocom04_sensor.pdf

[Dun04] ***Low-Power, Secure Routing for MICA2 Mote***, Breanne Duncan, David Malan, http://airclic.eecs.harvard.edu/publications/tr-06-04.pdf

[DutB04] ***Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust***, Bruno Dutertre, Steven Cheung, Joshua Levy, http://www.csl.sri.com/users/bruno/publis/sri-sdl-04-02.pdf

[DutP] ***Security Considerations in Wireless Sensor Networks***, Prabal K. Dutta, http://www.cse.ohio-state.edu/~duttap/presentations/SecurityConsiderationsInWSN.pdf

[Esc02a] ***A Key-Management Scheme for Distributed Sensor Networks***, Laurent Eschenauer, Virgil D. Gligor, http://www.glue.umd.edu/afs/glue.umd.edu/home/enee/faculty/gligor/pub/sensor-ccs9.ps

[Gan03] ***Analyzing and Modeling Encryption Overhead for Sensor Network Nodes***, Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu, http://moss.csc.ncsu.edu/~mueller/ftp/pub/mueller/papers/wsna03.pdf

[Gau04] ***Public Key Cryptography in Sensor Networks-Revisited***, Gunnar Gaubatz, Jens-Peter Kaps, Berk Sunar, http://www.crypto.wpi.edu/Publications/Documents/GaubatzKapsESAS04.pdf

[Gli04] ***Security in Sensor and Ad-Hoc Networks***, Virgil Gligor, http://www.sti.uniurb.it/events/fosad04/FOSAD2004-Gligor.pdf

[Gru03] ***Privacy-Aware Location Sensor Networks***, Marco Gruteser, Graham Schelle, Ashish Jain, Rick Han, and Dirk Grunwald, http://systems.cs.colorado.edu/Papers/Generated/2003PrivacyAwareSensors.pdf

[HuaQ03] ***Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks***, Qiang Huang, Johnas Cukier, Hisashi Kobayashi, Bede Liu, Jinyun Zhang, http://www.cis.upenn.edu/~lee/04cis640/readingList/papers/mjk/HCK+03.pdf

[HuaD04] ***Location-aware Key Management Scheme for Wireless Sensor Networks***, Dijiang Huang, Manish Mehta, Deep Medhi, Lein Harn, http://www.sce.umkc.edu/~dmedhi/papers/hmmh-sasn2004.pdf

[Hwa04] ***Energy-Memory-Security Tradeoffs in Distributed Sensor Networks***, David D. Hwang, Bo-Cheng Charles Lai, Ingrid Verbauwhede, http://www.emsec.ee.ucla.edu/pdf/2004adhocnow.pdf

[Karl03] ***Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures***, Chris Karlof, David Wagner, http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf

[Kri03] ***Efficient and Fault Tolerance Feature Extraction in Wireless Sensor Networks***, Bhaskar Krishnamachari, S. Sitharama Iyengar, http://ceng.usc.edu/~bkrishna/research/papers/KrishnamachariIyengarIPSN.pdf

[Kou02] ***Fault Tolerance Techniques for Wireless Ad hoc Sensor Networks***, Farinaz Koushanfar, Miodrag Potkonjak, Alberto Sangiovanni-Vincentelli, http://www-cad.eecs.berkeley.edu/Respep/Research/asves/paper2002/Farinaz_ieee_sensors02.pdf

[Law02a] ***Assessing Security-Critical Energy-Efficient Sensor Networks***, Yee Wei Law, S. Dulman, S. Etalle, P. Havinga, http://doc.utwente.nl/fid/1200

[Law02b] ***Key Management with Group-Wise Pre-Deployed Keying and Secret Sharing Pre-Deployed Keying***, Yee Wei Law, Sandro Etalle, Pieter Hartel, http://doc.utwente.nl/fid/1193

[Law03] ***A Formally Verified Decentralized Key Management Architecture for Wireless Sensor Networks***, Yee Wei Law, Ricardo Corin, Sandro Etalle, and Pieter H. Hartel, http://wwwhome.cs.utwente.nl/~ywlaw/pub/law03formally.pdf

[Laz02] ***Secure Broadcast in Energy-Aware Wireless Sensor Networks***, Loukas Lazos, Radha Poovendran, http://www.ee.washington.edu/research/nsl/papers/ISWC-02.pdf

[LiT05] ***Security Map of Sensor Network***, Tieyan Li, http://www.i2r.a-star.edu.sg/icsd/SecureSensor/papers/security-map.pdf

[LiuD03a] ***Multi-Level μ-TESLA: A Broadcast Authentication System for Distributed Sensor Networks***, Donggang Liu, Peng Ning, http://historical.ncstrl.org/litesite-data/ncsu_cs/TR-2003-08.ps.Z

[LiuD03b] ***Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks***, Donggang Liu, Peng Ning, http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/17.pdf

[LiuD03c] ***Efficient and Self-Healing Key Distribution with Revocation for Tactical Wireless Networks***, Donggang Liu, Peng Ning, http://historical.ncstrl.org/litesite-data/ncsu_cs/TR-2003-03.ps.Z

[LiuD03d] ***Location-Based Pairwise Key Establishments for Relatively Static Sensor Networks***, Donggang Liu, Peng Ning, Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (CCS'03), 2003, pp. 72 82.
[LiuD03e] ***Establishing Pairwise Keys in Distributed Sensor Networks***, Donggang Liu, Peng Ning, http://discovery.csc.ncsu.edu/~pning/pubs/ccs03-SNKeyMan.pdf

[Mal04a] ***Crypto for Tiny Objects***, David Malan, http://airclic.eecs.harvard.edu/publications/tr-04-04.pdf

[Mal04b] ***A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography***, David J. Malan, Matt Welsh, Michael D. Smith, http://airclic.eecs.harvard.edu/publications/secon04.pdf

[New04] ***The Sybil Attack in Sensor Networks: Analysis and Defenses***, James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, http://www.ece.cmu.edu/~adrian/projects/sybil.pdf

[Par05] ***Distributed Detection of Node Replication Attacks in Sensor Networks***, Bryan Parno, Adrian Perrig, Virgil Gligor, http://sparrow.ece.cmu.edu/~adrian/projects/revocation.pdf

[Per02b] ***SPINS: Security Protocols for Sensor Networks***, Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, http://www.ece.cmu.edu/~adrian/projects/mc2001/spins-wine-journal.pdf

[Per04] ***Security in Wireless Sensor Networks***, Adrian Perrig, John Stankovic, David Wagner, http://sparrow.ece.cmu.edu/~adrian/projects/sensornet-cacm2004.pdf

[Pie03] ***Random Key Assignment for Secure Wireless Sensor Networks***, Roberto Di Pietro, Luigi V. Mancini, Alessandro Mei, http://cesare.dsi.uniroma1.it/Sicurezza/doc/sasn2003.pdf

[Pom03] ***Sicherheit in Sensornetzen***, Danat Pomeranets, http://www.vs.inf.ethz.ch/edu/SS2003/DS/slides/12_sicherheit.pdf
[Prz03] ***SIA: Secure Information Aggregation in Sensor Networks***, Bartosz Przydatek, Dawn Song, Adrian Perrig, http://sparrow.ece.cmu.edu/~adrian/projects/sia.pdf

[Shi04] ***Designing Secure Sensor Networks***, Elaine Shi, Adrian Perrig, http://sparrow.ece.cmu.edu/~adrian/projects/secure-sensor-wireless-communications-2004.pdf

[Sli02] ***On Communication Security in Wireless Ad-Hoc Sensor Network***, Sasha Slijepcevic, Miodrag Potkonjak,Vlasios Tsiatsis, Scott Zimbeck, Mani B. Srivastava, http://www.ee.ucla.edu/~tsiatsis/research/pub/wetice02.pdf

[Und02] ***Security for Sensor Networks***, Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi, and John Pinkston, http://www.csee.umbc.edu/cadip/2002Symposium/sensor-ids.pdf

[Vog04] ***Exploring Message Authentication in Sensor Networks***, Harald Vogt, http://www.vs.inf.ethz.ch/publ/papers/vogt04esas.pdf

[WaG03] ***On Supporting Distributed Collaboartion in Sensor Networks***, Guiling Wang , Wensheng Zhang , Guohong Cao , Tom La Porta, http://www.cse.psu.edu/~gcao/paper/zhang/milicom-detection.pdf

[Woo02] ***Denial of Service in Sensor Networks***, Anthony D. Wood, John A. Stankovic, http://www.cs.virginia.edu/~adw5p/pubs/computer02-dos.pdf

[Ye04] ***Statistical En-route Filtering of Injected False Data in Sensor Networks***, Fan Ye, Haiyun Luo, Songwu Lu, Lixia Zhang, http://www.ieee-infocom.org/2004/Papers/51_2.PDF

[Yua02] ***Design Space Exploration for Energy-Efficient Secure Sensor Network***, Lin Yuan, Gang Qu, http://www2.imm.dtu.dk/~virk/02202_files/Design Space Exploration for Energy-Efficient Secure Sensor Network.pdf

[ZhaL03] ***Secure Communication in Sensor Networks***, Lanlan Zhang, http://www-i4.informatik.rwth-aachen.de/content/teaching/seminars/sub/2003_2004_ws_docs/secureCommunicationInSensorNetworks.pdf

[ZhaYa05] ***Securing Sensor Networks with Location-Based Keys***, Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, http://www.ecel.ufl.edu/~zhang/files/location-WCNC.pdf

[ZhuS03] ***LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks***, Sencun Zhu, Sanjeev Setia, Sushil Jajodia, http://www.cse.psu.edu/~gcao/teach/598/zhu-leap.pdf

Reports published by Humboldt University Berlin, Computer Science Department, Systems Architecture Group.

---

1. SAR-PR-2005-01: Linux-Hardwaretreiber für die HHI CineCard-Familie. Robert Sperling. 37 Seiten.
2. SAR-PR-2005-02, NLE-PR-2005-59: State-of-the-Art in Self-Organizing Platforms and Corresponding Security Considerations. Jens Peter Redlich, Wolf Müller. 10 pages.
3. SAR-PR-2005-03: Hacking the Netgear wgt634u. Jens-Peter Redlich, Anatolij Zubow, Wolf Müller, Mathias Jeschke, Jens Müller. 16 pages.
4. SAR-PR-2005-05: Sicherheit in selbstorganisierenden drahtlosen Netzen. Ein Überblick über typische Fragestellungen und Lösungsansätze. Torsten Dänicke. 48 Seiten.