Integrierte Sicherheit für Mobile Ad-hoc Netzwerke

Frank Kargl, Stefan Schlott, Michael Weber
Abteilung Medieninformatik, Universität Ulm
{frank.kargl,stefan.schlott,michael.weber}@informatik.uni-ulm.de

Abstract: Während der Aufbau von MANETs bereits recht gut verstanden ist, wurde der Schutz der entstehenden Netzwerke und seiner Teilnehmer vor Angriffen, die hier möglich sind, bisher etwas vernachlässigt. Zwar gibt es eine Vielzahl von Arbeiten, diese betrachten aber meist singuläre Fragestellungen, ohne den Gesamtkontext mit seinen vielfältigen Abhängigkeiten in Betracht zu ziehen.

Ziel dieses Beitrags ist es, die besonderen Sicherheitsprobleme bei MANETs kurz zu analysieren und die Querbezüge aufzuzeigen. Daraus leiten wir eine Sicherheitsarchitektur für Mobile Ad-hoc Netzwerke mit dem Namen „*SAM*“ ab.

1 Einleitung

Mobile Ad-hoc Netzwerke weisen einige spezifischen Besonderheiten im Hinblick auf deren Sicherheit auf. Ein wesentlicher Aspekt ist, dass in klassischen Netzwerken eine Trennung zwischen einer (meist zentral administrierten) Routing-Infrastruktur und normalen Knoten möglich ist. Somit kann sich die Routing-Infrastruktur leicht z.B. durch Passwörter oder Message Authentication Codes (MAC) vor den „normalen Knoten“ schützen. Dies ist bei MANETs nicht gegeben, da hier jeder Knoten gleichzeitig auch ein Router ist. Bösartige Knoten (sog. *Malicious Nodes*) haben also relativ leichtes Spiel.

Weiterhin haben Knoten eine starke Motivationen, sich nicht an der gemeinsamen Routing-Infrastruktur zu beteiligen, um eigene Ressourcen zu schonen. In einem MANET erbringen alle Knoten gemeinsam eine Leistung, von der wiederum alle profitieren. Das Ergebnis dieser Leistung ist die Konnektivität, zu welcher alle beitragen und die alle benutzen. Dabei wendet ein Knoten einen Teil seiner Ressourcen (CPU, Bandbreite, Batterie) auf, um den Verkehr von anderen weiterzuleiten, in der Erwartung, dass diese einen Teil ihrer Ressourcen dazu aufwenden, seine Datenpakete zu transportieren. Die Verlockung ist natürlich groß, die eigenen Aufwendungen für andere Knoten einzusparen, d.h. selbst keine Datenpakete weiterzuleiten, die Leistung der anderen Knoten für den Datentransport aber in Anspruch zu nehmen. In dem Maße, wie die Zahl dieser *egoistischen Knoten* in einem Netzwerk ansteigt, sinkt natürlich auch die Leistung des Gesamtnetzes.

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

Tabelle 1: Angriffsbaum A: Ressourcen einsparen

2 Angriffsanalyse

Ausgangspunkt für die Erstellung einer Sicherheitsinfrastruktur sollte immer die Analyse möglicher Angriffe sein. Wir greifen hier auf die von Bruce Schneier in [Sc99] vorgestellten *Attack Trees* (Angriffsbäume) an. Ausgehend von einem Ziel bzw. einer Motivation wird ein hierarchischer Baum mit Wegen erstellt, wie das Ziel eines Angriffs zu erreichen ist. Daraus lässt sich umgekehrt ableiten, welche Angriffe durch eine Schutzmaßnahme unterbunden werden.

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

Wir haben entsprechende Angriffsbäume für diverse Angriffsformen erstellen, die hier aus Platzgründen nicht dargestellt werden können. Für einen kompletten Überblick siehe [Ka03]. Durch die Analyse dieser Bäume gewinnt man schnell einen Eindruck von den Schwächen und Verwundbarkeiten der Protokolle. Untersuchungen haben gezeigt, dass Ad-hoc Netze durch solche Angriffe stark in ihrer Leistungsfähigkeit beeinträchtigt werden [Ka03, KK+04].

3 Verwandte Arbeiten

Arbeiten zur Sicherheit von Mobilen Ad-hoc Netzen lassen sich grob in drei Kategorien einteilen: *„Authentifizierung und Schlüsselaustausch“* [ZH99, HBC01], *„Sicheres Routing“* [PH02, PH03, HPJ02, SDL$^+$02, Za02] und *„Erkennung und Verhinderung egoistischer Knoten“* [MGLB00, ZL00, BB02, MM02]. Eine umfassende Literaturliste zu Sicherheit in Ad-hoc Netzwerken findet sich in [Zh].

Ein grundlegendes Problem aller Arbeiten ist die fehlende Integration der verschiedenen Teilbereiche. So setzen beispielsweise sichere Routingprotokolle wie SAODV [Za02] oft voraus, dass kryptographische Schlüssel zwischen den beteiligten Parteien vereinbart wurden. Wie dies ohne existierende Routen effizient geschehen soll, bleibt offen. Umgekehrt gehen Authentifizierungslösungen wie in [HBC01] meist davon aus, dass eine funktionierende Routing-Infrastruktur zwischen den Knoten existiert. Andererseits setzen Systeme zur Erkennung egoistischer Knoten wie CORE [MM02] oft implizit voraus, dass Knoten über eine eindeutige Identität verfügen und nicht unter beliebig vielen selbst-generierten Identitäten aktiv werden kann. Sichere Routingprotokolle gehen von ähnlichen Annahmen aus.

Ein Thema, welches bisher noch gar nicht berücksichtigt wurde, ist die Möglichkeit der Erstellung von Bewegungsprofilen in Ad-hoc Netzen. Wie in [ČHH02] gezeigt, können Knoten in Ad-hoc Netzen unter Umständen recht genau lokalisiert werden. Eine Sicherheitsinfrastruktur sollte Mechanismen enthalten, welche die Privatsphäre der Teilnehmer schützt. Schließlich definieren viele Authentifizierungslösungen für Ad-hoc Netze nicht klar, was unter einer Identität eines Knotens oder Benutzers eigentlich zu verstehen ist. Damit bleibt dann aber unklar, was eigentlich authentifiziert wird.

4 SAM

Während die bisherigen Ansätze und Projekte also immer nur einen Teil der Sicherheitsprobleme von Ad-hoc Netzwerken adressieren, schlagen wir eine *Sicherheitsarchitektur für Mobile Ad-hoc Netzwerke* (kurz *SAM* [Ka03]) vor, welche ausgehend von der durchgeführten Sicherheitsanalyse eine umfassende und in den Teilkomponenten aufeinander abgestimmte Sicherheitslösung für Mobile Ad-hoc Netzwerke darstellt, welche die oben aufgezeigten Abhängigkeiten berücksichtigt. Teilweise werden existierende Ideen aus bestehenden Arbeiten aufgegriffen, teilweise müssen jedoch auch neue Ansätze entwickelt werden. SAM enthält folgende Teilkomponenten[1]:

ManetIDs: Das Authentisierungs-Modul *ManetIDs* dient dazu, die Identität der Knoten in einem MANET zweifelsfrei festzustellen. Dieser Vorgang ist in den Route-Request/-Reply Vorgang des Routingprotokolls *SDSR* (s.u.) integriert. Gleichzeitig werden Sitzungsschlüssel mit allen an einer Route beteiligten Knoten ausgetauscht, welche für die Verschlüsselung der nachfolgenden Datenkommunikation und im

[1] eine ausführliche Beschreibung aller Komponenten findet sich in [Ka03]

Rahmen des IDS Systems *MobIDS* (s.u.) genutzt werden können. Um die Erstellung von Bewegungsprofilen zu verhindern, nutzen die Initiatoren einer Kommunikationsbeziehung für jeden Route-Request ein neues Pseudonym, welches zudem in regelmäßigen Abständen gewechselt werden kann. Desgleichen können sich potentielle Kommunikationspartner unter wechselnden Pseudonymen im Netz registrieren.

SDSR: Diese Komponente erweitert das DSR Protokolle um die Fähigkeit, Modifikationen an den DSR-Nachrichten zu erkennen. Gefälschte Nachrichten werden verworfen, eine Meldung an das IDS führt gegebenenfalls zum Ausschluss des Verursachers aus dem MANET. SDSR ist ein reaktives Protokoll, in dessen Routensuche die Authentifizierung von Knoten und der Austausch von Sitzungsschlüssel integriert ist.

MobIDS: Das „ *Mobile Intrusion Detection System*“ [KK+04] dient der Erkennung und dem Ausschluss von fehlerhaften, egoistischen oder böswilligen Knoten. Hierzu greift es auf eine Reihe von *Sensoren* zurück, welche Auffälligkeiten im Verhalten eines Knotens bemerken. Die Sensoren liefern Meldungen an den *Bewerter*, welche diese zu einer lokalen Bewertung zusammenführt. Anschließend verteilt der *Distributor* diese Information im Netz. Das *Ausschluss-System* sorgt dafür, dass Knoten mit einer negativen Bewertung nicht am Netz teilnehmen können. Dabei fließen auch Informationen des Routingprotokolls in den Bewertungsvorgang ein.

5 Zusammenfassung

Das Thema Sicherheit in MANETs ist sehr komplex und wurde lange Zeit gegenüber dem reinen Routingprozeß vernachlässigt. Gleichzeitig ist jedoch zweifelhaft, ob ohne entsprechende Sicherheitssysteme ein Durchbruch bei der Nutzung von MANETs zu erreichen ist. Diese Netze sind ohne entsprechende Schutzmechanismen zu verletzlich, als dass sich Anwender wirklich auf sie verlassen könnten. SAM stellt hier einen Ansatz dar, der verschiedene bisherige Lösungen erweitert und mit neuen Komponenten zu einem umfassenden Sicherheitsframework integriert. Dies erscheint uns auf Grund der vielfältigen Querbezüge bei Sicherheitsfragestellungen in MANETs unbedingt notwendig.

Literatur

[BB02] Buchegger, S. und Boudec, J.-Y. L.: Performance analysis of the confidant protocol: Cooperation of nodes - fairness in distributed ad-hoc networks. In: *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*. Lausanne, CH. June 2002.

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

[HBC01] Hubaux, J., Buttyan, L., und Capkun, S.: The Quest for Security in Mobile Ad Hoc Networks. In: *Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*. 2001. verfügbar unter `http://citeseer.nj.nec.com/493788.html`.

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

[Ka03] Kargl, F.: *Sicherheit in Mobilen Ad hoc Netzwerken*. PhD thesis. University of Ulm. Ulm, Germany. 2003. verfügbar unter `http://medien.informatik.uni-ulm.de/~frank/research/dissertation.pdf`.

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

[MGLB00] Marti, S., Giuli, T. J., Lai, K., und Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: *Mobile Computing and Networking*. S. 255–265. 2000. verfügbar unter `citeseer.nj.nec.com/marti00mitigating.html`.

[MM02] Michiardi, P. und Molva, R.: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: *Proceedings of the 6th IFIP Communication and Multimedia Security Conference*. Portorosz, Slovenia. September 2002.

[PH02] Papadimitratos, P. und Haas, Z. J.: Secure Routing for Mobile Ad hoc Networks. In: *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*. San Antonio, TX. January 2002. verfügbar unter `http://wnl.ece.cornell.edu/Publications/cnds02.pdf`.

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

[Sc99] Schneier, B.: Modeling security threats. *Dr Dobb's Journal*. December 1999. verfügbar unter `http://www.ddj.com/documents/s=896/ddj9912a/9912a.htm`.

[SDL+02] Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., und Belding-Royer, E. M.: A Secure Routing Protocol for Ad Hoc Networks. In: *Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP)*. November 2002. verfügbar unter `http://signl.cs.umass.edu/pubs/aran.icnp02.ps`.

[Za02] Zapata, M. G.: Secure Ad hoc On-Demand Distance Vector Routing. *ACM Mobile Computing and Communications Review (MC2R)*. 6(3):106–107. July 2002. verfügbar unter `http://doi.acm.org/10.1145/581291.581312`.

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

[ZH99] Zhou, L. und Haas, Z. J.: Securing Ad Hoc Networks. *IEEE Network*. 13(6):24–30. 1999. verfügbar unter `http://citeseer.nj.nec.com/zhou99securing.html`.

[ZL00] Zhang, Y. und Lee, W.: Intrusion detection in wireless ad-hoc networks. In: *Mobile Computing and Networking*. S. 275–283. 2000. verfügbar unter `http://citeseer.nj.nec.com/zhang00intrusion.html`.