[KHSSt06] André König, Matthias Hollick, Johannes Schmitt, Ralf Steinmetz; **Sicherheit und Verfügbarkeit in mobilen Ad hoc Netzen - Ein geographischer, schichtenübergreifender Ansatz**; 2. Essener Workshop "Neue Herausforderungen in der Netzsicherheit", Oktober 2006, S. .

Sicherheit und Verfügbarkeit in mobilen Ad hoc Netzen - Ein geographischer, schichtenübergreifender Ansatz

André König, Matthias Hollick, Johannes Schmitt, Ralf Steinmetz
[Andre.Koenig; Matthias.Hollick; Johannes.Schmitt, Ralf.Steinmetz]@KOM.tu-darmstadt.de
FG Multimedia Kommunikation (KOM), Technische Universität Darmstadt

Mobile Ad hoc Netze sind in den letzten Jahren verstärkt Gegenstand der Forschung geworden. Mögliche Einsatzgebiete für solche Netze sind Szenarien, in denen der Aufbau einer Kommunikationsinfrastruktur nicht oder nur schwer möglich ist. Genannt wird in diesem Zusammenhang oft der Einsatz von mobilen Ad hoc Netzen in militärischen- oder Katastrophenszenarien. Gerade dort spielt die Sicherheit des Netzes und die direkt damit verbundene Verfügbarkeit eine entscheidende Rolle. Verschiedenste Angriffsmöglichkeiten, die aufgrund der infrastrukturlosen Natur von Ad hoc Netzen möglich sind, wurden bereits identifiziert. Ziel unserer Arbeit ist die Entwicklung eines Verfahrens zur Etablierung von Routen in mobilen Ad hoc Netzen, die identifizierte, geographische Bedrohungsbereiche meiden. Dabei soll kein neues, eigenständiges Routingverfahren entwickelt werden. Mittels einer schichtenübergreifenden Architektur können bestehende Routingalgorithmen an die Sicherheitsanforderungen in der dynamischen Umgebung angepasst werden.

I. Motivation und Ziele

Mobile Ad hoc Netze zur Bereitstellung von Kommunikationsdiensten in Szenarien, in denen der Aufbau einer entsprechenden Infrastruktur nicht, oder nur schwer möglich ist, sind in den letzten Jahren verstärkt Gegenstand der Forschung geworden. Aufgrund der infrastrukturlosen Natur dieser Netze und der durch die Mobilität der Netzknoten notwendigen drahtlosen Datenübertragung ergeben sich für dieses neue Kommunikationsparadigma ebenfalls neue Angriffsmechanismen [1]. Unterschieden wird hierbei zwischen passiven und aktiven Attacken.

Ziel einer aktiven Attacke ist die methodische Einflussnahme auf den Verlauf von Datenströmen durch das Netz. Aufgrund der fehlenden Infrastruktur ist in einem mobilen Ad hoc Netz jeder Knoten am Routing von Datenpaketen von Sender zu Empfänger beteiligt. Unter Ausnutzung dieser Gegebenheit für einen Angriff wird es beispielsweise möglich, den Informationsfluss im Netz auf bestimmte (bösartige) Knoten zu konzentrieren. Die Verfügbarkeit (großer Teile) des Netzes kann dadurch erheblich beeinflusst werden. Um den gewünschten Effekt zu erzielen, ist es zur Durchführung eines aktiven Angriffs notwendig, das Routingprotokoll eines bösartigen Knotens entsprechend zu verändern. Mit Hilfe von Intrusion Detection Systemen (IDS) [2] kann dieses veränderte Verhalten eines Knotens erkannt werden.

Während aktive Attacken die Eigenschaften der Ad hoc Routingverfahren ausnutzen, basieren passive Angriffsmechanismen (hauptsächlich) auf der drahtlosen Art der Datenübertragung. Eine globale Verkehrsanalyse oder das gezielte Abhören der Kommunikation einzelner Knoten ist in einer drahtlos vernetzten Umgebung leicht möglich. Im Gegensatz zu aktiven Attacken ist zur Durchführung eines passiven Angriffs weder eine spezifische Veränderung im Verhalten des angreifenden Knotens, noch die Ausstrahlung von Funksignalen im Allgemeinen notwendig. Die Erkennung von passiven Attacken ist deshalb gemeinhin nicht möglich.

Ziel unserer Arbeit ist die Gewährleistung der Sicherheit und der Verfügbarkeit von Kommunikationsdiensten in einem mobilen Ad hoc Netz. Als Gegenmaßnahme für die vorgestellten Angriffsmechanismen entwickeln wir ein Verfahren, welches den Aufbau von geographisch sicheren Routen ermöglicht. Als geographisch sichere Route bezeichnen wir eine Route, die außerhalb des geographischen Einflussbereichs von bösartigen Knoten verläuft.

Im Folgenden beschreiben wir die zur Erreichung unseres Ziels entwickelte Architektur und zeigen erste Simulationsergebnisse.

II. Annahmen – Ansatz – Architektur

Zum Aufbau von Routen mit den gewünschten geographischen Eigenschaften setzten wir voraus, dass die Position von (zumindest einigen) Knoten im Netz z.B. durch GPS oder Triangulation von Signalstärken ermittelt werden kann.

Da die Erkennung von passiven Angriffen wie beschrieben im Allgemeinen nicht möglich ist, nehmen wir an, dass passive Angriffe auf bestimmte Bereiche des Netzes beschränkt werden können. Solche Bereiche sind z.B. Randgebiete des Netzes oder ausgewiesene Zonen mit geringen (physikalischen) Sicherheitsvorkehrungen.

Um den gewünschten Einfluss auf den geographischen Verlauf der Route zu erhalten, verwenden wir den in Abbildung 1 gezeigten, schichtenübergreifenden Ansatz. Eine analoge Architektur wurde bereits in [3] vorgestellt.

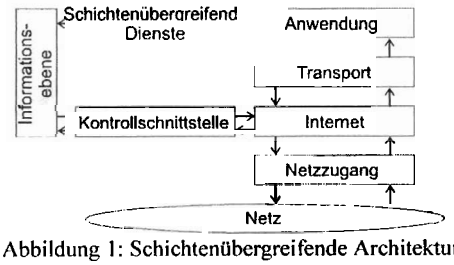

Abbildung 1: Schichtenübergreifende Architektur

Eine zusätzliche Informationsebene ermöglicht den direkten und flexiblen Informationsaustausch zwischen der Anwendungs- und der Internetebene des Internet Schichtenmodells. So können z.B. Sicherheitsrichtlinien für verschiedene Klassen von Datenströmen und die benötigten

Positionsinformationen an das Routingverfahren übergeben werden.

Da unsere Arbeit nicht auf die Entwicklung eines neuen, eigenständigen Routingprotokolls zielt, sondern ein Verfahren entwickelt werden soll, dass mit verschiedenen existierenden Routingprotokollen für mobile Ad hoc Netze eingesetzt werden kann, benutzen wir die in Abbildung 1 gezeigte Kontrollschnittstelle zur Beeinflussung eines existierenden Routingverfahrens. Die dafür benötigten Informationen erhält diese Schnittstelle zum Teil von der Anwendungsschicht des Knotens über die schichtenübergreifende Informationsebene. Weitere, zur Steuerung notwendige Informationen von anderen Knoten im Netz werden über einen zusätzlichen Kontroll Header ausgetauscht. Dieser wird zwischen die Header der Internet- und der Transportschicht eingefügt. Der Aufbau des entstehenden Frames ist in Abbildung 2 skizziert.

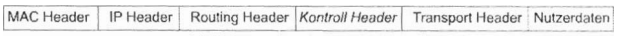

Abbildung 2: Zusätzlicher Header

Abbildung 3 zeigt das Format des Kontroll Headers für die Phase der Routenfindung. Enthalten ist unter anderem eine Beschreibung der zu umgehenden, geographischen Bedrohungsbereiche.

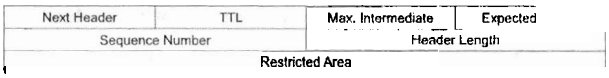

Abbildung 3: Header Format für Routenfindung

III. Erste Simulationsergebnisse

Zur ersten Evaluation unseres Ansatzes verwenden wir das Simulationsszenario aus Abbildung 4. Ein mobiles Ad hoc Netz wird hier unterteilt in einen sicheren (zugangskontrollierten) Bereich und einen unsicheren Bereich in dem (passive und aktive) Angriffe potentiell möglich sind. Sender und Empfänger befinden sich an statischen Positionen in der linken bzw. rechten unteren Ecke des Feldes. Die Sendereichweite beträgt 250 Meter für alle beteiligten Knoten. Diese Entfernung muss als Sicherheitsabstand um den unsicheren Bereich eingehalten werden. So kann ausgeschlossen werden, dass Routen durch den Einflussbereich bösartiger Knoten verlaufen.

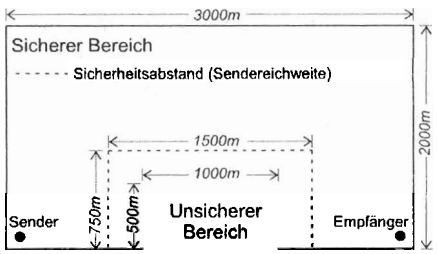

Abbildung 4: Simulationsszenario

Abbildung 5 zeigt den Vergleich der Konnektivität bei Verwendung eines unveränderten AODV Protokolls [4] und AODV in Verbindung mit unserer Erweiterung. Verglichen wird die Anzahl der erfolgreichen Route Requests als Anteil der insgesamt gesendeten Route Requests im Bezug zur Anzahl der Knoten im Netz. Zur Evaluation von AODV nehmen wir an, dass sich keine bösartigen Knoten im unsicheren Bereich befinden. Routen können also unbeeinträchtigt durch diesen Bereich aufgebaut werden. Routen die unter Verwendung unserer Erweiterung aufgebaut werden, verlaufen im Gegensatz dazu nicht durch den unsicheren Bereich. Knoten, die sich in diesem Bereich befinden, können also nicht zum Aufbau von Routen verwendet werden. Für den Fall, dass sich keine bösartigen Knoten im Netz befinden, bedingt dies einen etwas geringeren Grad an Konnektivität. Dagegen ist bereits ein entsprechend modifizierter, bösartiger Knoten ausreichend, um die Kommunikation zwischen Sender und Empfänger für ein unverändertes AODV Protokoll (in unserem Szenario) vollständig zu unterbinden.

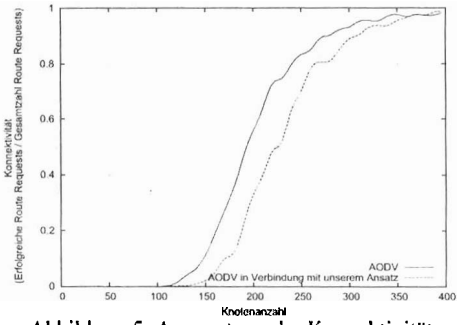

Abbildung 5: Auswertung der Konnektivität

Die durch unsere Architektur gewonnene Kompatibilität ermöglicht eine nahtlose Integration von bestehenden Knoten (z.B. auf Basis von AODV) in die durch erweiterte Knoten gebildete Route. Abbildung 6 zeigt die resultierende, deutliche Steigerung der Konnektivität für ein Szenario mit 400 beteiligten Knoten im Netz und variablem Anteil an Knoten, die mit unserer Erweiterung ausgestattet sind.

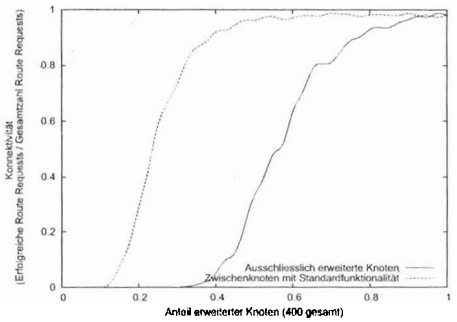

Abbildung 6:
Konnektivität für Zwischenknoten mit Standardfunktionalität

Unsere zukünftige Arbeit im Bereich schichtenübergreifender Sicherheitsdienste zielt auf die Erweiterung der vorgestellten Architektur auf die Transport- und die Netzzugangsschicht des Internet Schichtenmodells.

IV. Literaturverzeichnis

[1] B. Wu, J. Chen, J. Wu, M. Cardei; A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks; to appear in Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.Z. Du (eds.), Springer, 2006

[2] C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, K. Levitt; Intrusion detection: A specification-based intrusion detection system for AODV; Proceedings of the 1st ACM workshop on Security of Ad hoc and sensor networks; October 2003

[3] M. Conti, J. Crowcroft, G. Maselli, G. Turi; A modular cross-layer architecture for Ad hoc networks; In J. Wu, Handbook on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks; CRC Press LLC, 2004

[4] C. Perkins, E. Belding-Royer, S. Das; RFC 3561 - Ad hoc On-Demand Distance Vector (AODV) Routing; 2003