Spezielle Sicherheitsrisiken für taktische mobile Adhoc-Netzwerke (MANETs) *

Elmar Gerhards-Padilla[1], Marko Jahnke[2]

[1]Universität Bonn, Institut für Informatik, Abt. IV
Römerstr. 164, 53117 Bonn

[2]Forschungsinstitut für Kommunikation, Informationsverarbeitung und Ergonomie
Forschungsgesellschaft für Angewandte Naturwissenschaften
Neuenahrer Str. 20, 53343 Wachtberg

Einleitung

Das Konzept der vernetzten Operationsführung führt zu neuen Anforderungen an die Kommunikation der Streitkräfte. Speziell die Kommunikation auf der letzten Meile stellt eine Herausforderung dar. Als Anforderungen an ein Kommunikationsnetz für die letzte Meile, die insbesondere für Netze im taktischen Einsatz gelten, lassen sich folgende Punkte identifizieren:

- **Sicherheit**
  Die Übertragung, Verarbeitung und Speicherung sensibler Daten (z. B. Positionsinformationen, Ausrüstungszustand, Vitaldaten, taktische Informationen) unter potentieller Feindeinwirkung stellen besonders hohen Sicherheitsanforderungen.
- **Selbstkonfiguration und Robustheit**
  Es besteht die Möglichkeit von kurzfristigen, unvorhergesehenen Veränderungen an der Kommunikationsinfrastruktur, z.B. durch Bewegung eigener Einheiten oder potenzielle Angriffe. Deshalb muss das Kommunikationsnetz ohne manuelle Intervention in der Lage sein, dynamisch auf Änderungen der Kommunikationsinfrastruktur zu reagieren.
- **Kommunikation überall**
  Um Kommunikation weitestgehend unabhängig von Einsatzgebiet und vorherrschenden Bedingungen zu ermöglichen, darf nicht von einer festen Kommunikationsinfrastruktur (z.B. verlegte Kabel, feste Access Points, feste Relay-Stationen) ausgegangen werden.
- **Mobile Knoten**
  Die Bewegungsfreiheit der Einheiten darf nicht durch das Kommunikationsnetz eingeschränkt werden. Stattdessen muss das Kommunikationsnetz auch bei Mobilität der Einheiten zuverlässige Kommunikation gewährleisten.
- **Kleine Geräte**
  Insbesondere bei mobilen Einheiten ist darauf zu achten, die Belastung durch Kommunikationshardware so gering wie möglich zu halten. Laptops sind aufgrund von Größe und Gewicht weniger geeignet. Geeignet erscheint der Einsatz von Kleinstgeräten wie sog. Sub-Notebooks, Personal Digital Assisstants, Ultra Mobile PCs oder auch Smartphones, die mit ausreichenden Kapazitäten erst in der jüngsten Vergangenheit kommerziell verfügbar wurden.
- **Geringe Kosten**
  Die Bundeswehr verfügt über einen eng begrenzten Etat. Aus diesem Grund ist es nötig die gewünschten Eigenschaften mit möglichst geringen Kosten zu realisieren. Dies geschieht, wo immer möglich, durch die Verwendung von COTS-Produkten (Commercial Off The Shelves).

Taktische MANETs

Seit einigen Jahren sind so genannte Mobile Adhoc-Netzwerke (MANETs) Forschungsthema. Dabei handelt es sich um selbstkonfigurierende Netze ohne feste Infrastruktur mit mobilen Knoten. Für den Einsatz in MANETs ist die Verwendung mobiler Kleinstgeräte mit entsprechenden Funkadaptern vorgesehen. Dadurch können die meisten der o. g. Anforderungen erfüllt werden und prädestinieren somit MANETs für den Einsatz auf der letzten Meile, z. B. im Infanterieeinsatz.

Ein mögliches Einsatzszenario ist in Abbildung 1 dargestellt. Es wird hier davon ausgegangen, dass jede Einheit über ein eigenes funkvernetztes Kommunikationsgerät verfügt.

* Erschienen in: IT-Report 2007, S. 59-62, Report Verlag, Bonn, Mai 2007.

Als Anwendungen sind IP-Sprachkommunikation, ein Führungsinformati-

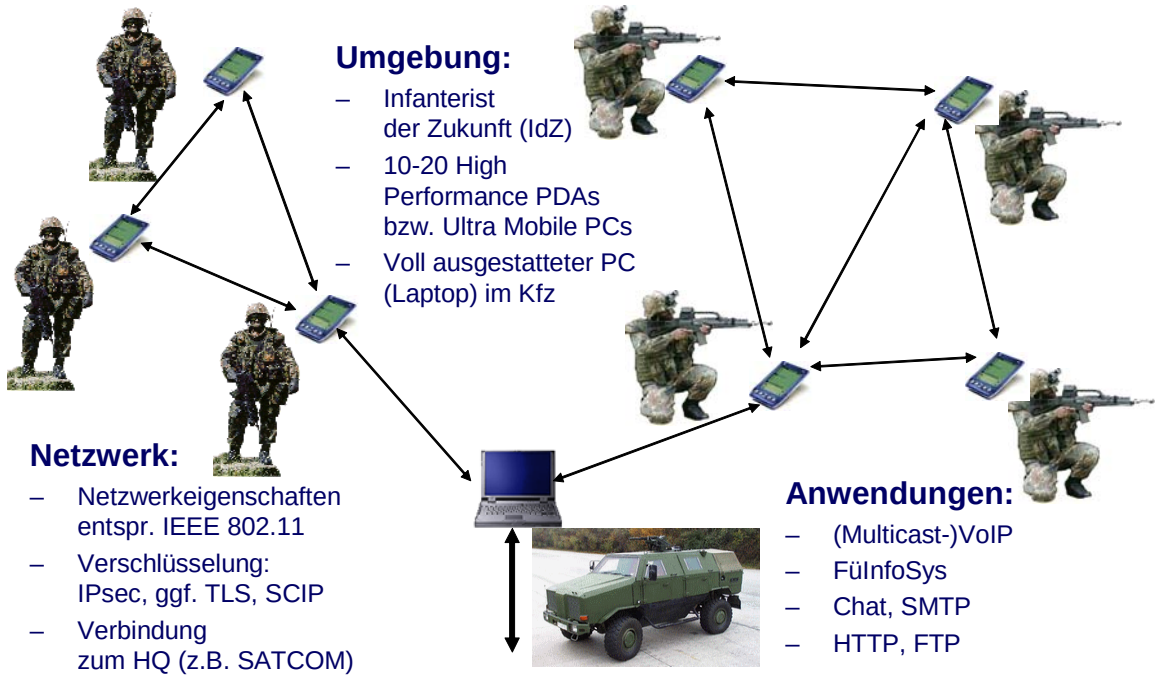

Abbildung 1: Mögliches Einsatzszenario für ein taktisches MANET

onssystem oder textbasierte Kommunikation (z.B. E-Mail oder Chat) denkbar. Mangels existierender Alternativen im militärischen Bereich wird vorläufig ein Funkübertragungsverfahren entsprechend der IEEE-Empfehlungen 802.11[a,b,g] angenommen.

Ein wesentlicher Aspekt, der MANETs von infrastrukturbasierten drahtlosen Netzen unterscheidet, ist das *Adhoc-Routing* und -*Forwarding*. Knoten sind oft nicht in direkter Funkreichweite miteinander verbunden, sondern müssen sich darauf verlassen, dass andere Knoten ihren Netzverkehr weiterleiten (Forwarding). Als Routing bezeichnet man das Finden eines Verbindungsweges (Pfad) zwischen zwei Knoten, die nicht direkt miteinander verbunden sind. In infrastrukturbasierten Netzen wird Routing durch spezielle, dedizierte Geräten, so genannten Routern, realisiert. Die fehlende Infrastruktur in MANETs führt dazu, dass potentiell jedes Endgerät im Netz in das Routing eingebunden ist. Aus diesem Grunde kann in MANETs jeder legitimierte Netzteilnehmer relativ einfach Einfluss auf das Routing nehmen.

Am Beispiel des Optimized Link State Routing Protokolls (*OLSR*) soll die Funktionsweise eines MANET-Routingprotokolls verdeutlicht werden. Bei OLSR erlernt jeder Knoten Informationen über seine Nachbarschaft durch den Austausch von Meldungen der Routinginstanzen innerhalb der Funknachbarschaft, die Hello-Nachrichten genannt werden. Einige speziell ausgewählte Knoten – die so genannten Multipoint Relays (MPRs) – propagieren ihre lokale Sicht mit Hilfe weiterer Meldungen global im Netz. Anhand der empfangenen Hello- und Topology-Control-Meldungen erlernt jeder Knoten die von ihm und anderen Knoten nutzbaren Routen im Netz.

Neben OLSR gibt es eine Fülle von weiteren MANET-Routingprotokollen. Diese unterscheiden sich in ihrer Vorgehensweise teilweise deutlich vom vorgestellten OLSR. Allen MANET-Routingprotokollen gemein ist jedoch, dass sie Routing-Meldungen versenden und anhand ampfangener Meldungen die Routen im Netz kennenlernen.

Angriffe gegen taktische MANETs

Schon durch die Verwendung von Funktechnologie sind taktische MANETs einem gegenüber drahtgebundenen Netzen deutlich höheren Bedrohungspotential ausgesetzt. Ein Mithören des Funkverkehrs ist prinzipiell möglich, wenn-

gleich auch entsprechend starke Verschlüsselungsverfahren für den Netzverkehr die Gefahr für das Mitlesen des Klartextes verringern. Die Störung durch Überlagerung von Funksignalen (Jamming) ist ebenfalls ein wichtiger Angriffspunkt, der im hier besprochenen Kontext nicht weiter vertieft werden soll.

Neben dieser von Außen stattfindenden Art von Angriffen gegen taktische MANETs sind unter der Voraussetzung, dass Verschlüsselungs- und Authentifizierungsmechanismen (z.B. Biometrie) zum Einsatz kommen, vorwiegend Angriffe von Innentätern zu betrachten. Dazu gehört nicht nur die Sabotage durch legitimierte Benutzer, sondern auch die nicht erkannte feindliche Übernahme von Knoten. Diese kann trotz etwaiger verdeckter Alarmmechanismen nicht ultimativ ausgeschlossen werden, wenn ein Soldat unter Einwirkung oder Androhung physischer oder psychischer Gewalt steht.

Ziele dieser Insider-Angriffe können folgende sein:

- **Mithören von Nachrichten**
  Ein Angreifer kann die über seinen Netzknoten geleiteten Nachrichten im Klartext mitlesen, wenn er in den Besitz eines Gerätes samt seines kryptographischen Schlüsselmaterials gelangt ist.
- **Aufklärung des Netzes**
  Ein Angreifer wird durch Übernahme eines Netzknotens prinzipiell in die Lage versetzt, die im Netz vorhandenen Informationen aktiv oder passiv in Erfahrung zu bringen.
- **(Selektives) Löschen von Daten**
  Es können über den Knoten des Angreifers geleitete Daten gelöscht werden. Dabei kann der Angreifer selektiv nur bestimmte Arten von Daten, z.B. einzelner Dienste oder einzelner Netzteilnehmer verwerfen.
- **Manipulation von Daten**
  Ein Angreifer kann versuchen, im Netz verbreitete Daten zu manipulieren und somit gezielt Falschinformationen einzuschleusen. Hier ist nicht nur die taktische Information gefährdet, sondern auch der zur Aufrechterhaltung des Netzes notwendige Steuerverkehr.
- **Isolation von Netzsegmenten**
  Auf verschiedene Arten können einzelne Knoten oder gesamte Netzbereiche am Versand oder Empfang des Netzverkehrs gehindert und so vom Netz abgetrennt werden.

Die zuletzt genannten potentiellen Ziele können auf verschiedene Weise erreicht werden. Meist stellen sich hier die Charakteristika von MANETs als Gründe für eine größere Verwundbarkeit heraus. Die jeweilige Umsetzung der Angriffe hängt dabei stark von den spezifischen Eigenschaften des Netzes ab, z.B. vom verwendeten Routing-Protokoll.

Ein einfaches Beispiel für Insider-Angriffe in MANETs stellt der so genannte Blackhole-Angriff dar. Abbildung 2 zeigt schematisch die

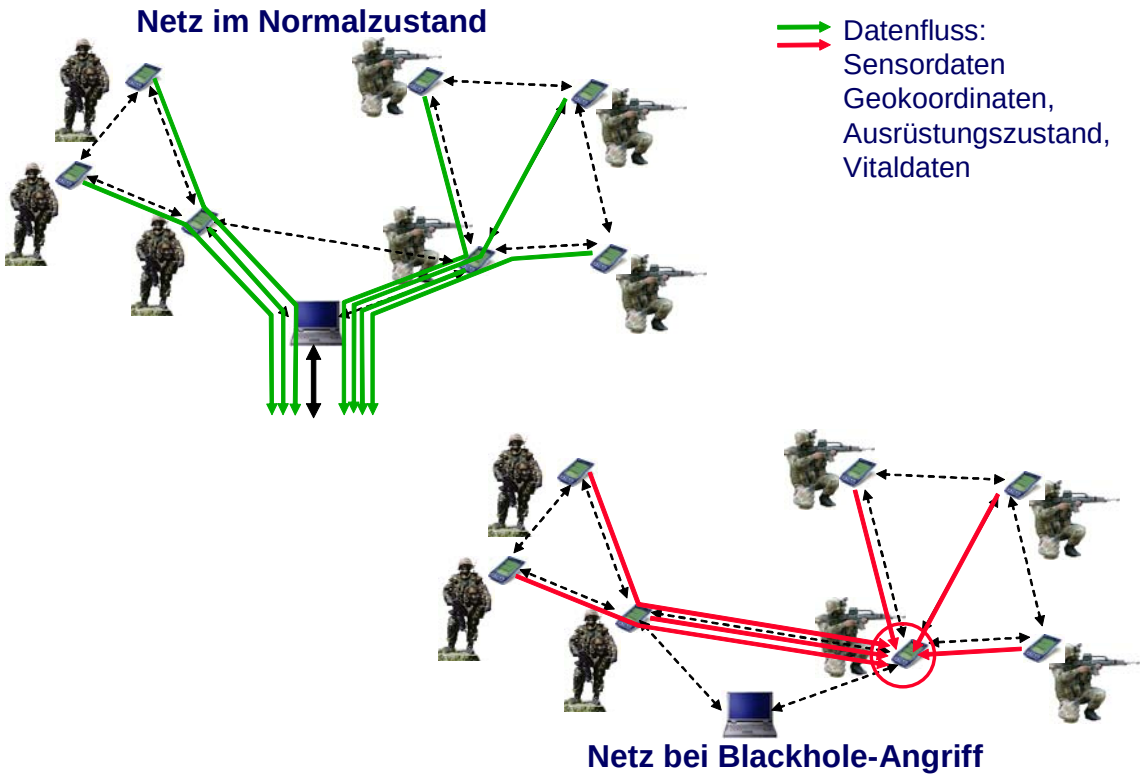

Abbildung 2: Schematische Darstellung eines Blackhole-Angriffes

Auswirkungen dieses Angriffs auf das o. g. mögliche Einsatzszenario. Der hier rot eingerahmte Knoten wird als von einem Angreifer übernommen betrachtet und versendet gefälschte Routing-Nachrichten, in denen er behauptet, alle anderen Knoten erreichen zu können. Damit scheint er zur Weiterleitung von Paketen für andere Knoten interessant, die ihm daraufhin den Netzverkehr zur Weiterleitung überlassen. Dies führt schlimmstenfalls zu dem hier skizzierten Szenario, in dem alle anderen Knoten versuchen, ihren Datenverkehr über den Angreifer an den Empfänger zu senden, der seinerseits die ihm übergebenen Netzpakete leicht verschwinden lassen kann. Mit Hilfe dieses Angriffes ist es dem Angreifer möglich, mit nur einem übernommenen Knoten seinen Einfluss auf ein ganzes Netzsegment auszudehnen.

Wie durch die genannten Beispiele ersichtlich, gehen die Bedrohungen, denen ein taktisches MANET ausgesetzt ist, weit über die bekannten Bedrohungen aus dem Bereich drahtgebundener Netze hinaus, wobei letztgenannte in MANETs weiterhin existieren. Aus diesem Grunde ist es notwendig, neue Detektions- und Reaktionsmechanismen zu entwickeln, die auch in der Lage sind, diesen in drahtgebundenen Netzen weniger wichtigen Angriffen zu begegnen.

Lösungsansätze

Das Forschungsgebiet zur Erkennung von Angriffen gegen MANETs genießt in ziviler wie militärischer Welt eine hohe Aufmerksamkeit.

Im Auftrag des Bundesamtes für Informationsmanagement und Informationstechnik der Bundeswehr wird derzeit das Forschungsprojekt „MANET Intrusion Detection for Tactical Environments“ (MITE) des Forschungsinstitutes für Kommunikation, Informationsverarbeitung und Ergonomie in Zusammenarbeit mit der Universität Bonn, der Fachhochschule Köln, sowie dem Fraunhofer-Institut für Graphische Datenverarbeitung in Darmstadt durchgeführt.

In diesem Forschungsvorhaben werden Verfahren entwickelt und untersucht, die sich zur Erkennung MANET-spezifischer Angriffe gegen taktische mobile Netze eignen. Ziel ist die Entwicklung eines so genannten Intrusion-Detection-Systems (IDS), das ein MANET mittels verteilter Komponenten überwacht und bei erkannten potentiell sicherheitsrelevanten Ereignissen frühzeitig warnt. Mittelfristig ist darüber hinaus geplant, dieses System um automatische Reaktionskomponenten gegen erkannte Angriffe zu erweitern, weil in einem taktischen MANET manuelle Interventionen schwierig durchzuführen sind.

Zu den ersten Zwischenergebnissen dieses Projektes zählen

- **Nachbildung und Analyse von Angriffen**
  Durch Verwendung spezieller Testumgebungen und dem Einsatz zusätzlicher Simulationen konnten verschiedene Angriffe nachgestellt und ihre Funktionsweise und Auswirkungen auf das Netz genauer untersucht werden.
- **Verfahren zur netzbasierten Anomalieerkennung**
  Durch Adaption und Weiterentwicklung von Verfahren aus dem drahtgebundenen Bereich konnten Verfahren entwickelt werden, die abnormales Netzverhalten auf Basis der Auswertung von Routingnachrichten und von Verkehrsstatistiken detektieren können.
- **Entwicklung spezieller Netz-Sensorik**
  Um den Umständen in verteilten MANETs gerecht zu werden, wurden verschiedene Erweiterungen für die verteilte Erfassung von Netzverkehr konzipiert und umgesetzt.
- **Ressourcenschonende IDS-Infrastrukturen**
  Auf der Basis von leichtgewichtigen Protokollen und COTS-Produkten für Netzmanagement wurde eine Kommunikationsinfrastruktur für die verteilten Komponenten des IDS entwickelt und prototypisch implementiert.

Bei allen genannten Teilergebnissen stehen unter anderem auch die besonderen Randbedingungen mobiler Kleinstgeräte im Mittelpunkt, da sie nur über begrenzte Kapazität bei der Verarbeitung, Speicherung und Übertragung von Daten verfügen, die eine Folge der Bauform sowie des begrenzten Energievorrates ist.

Trotz der ausgiebigen Verwendung von Simulationen steht im Gegensatz zu vielen anderen Forschungsaktivitäten beim hier beschriebenen Projekt immer die prototypische Implementierung im Vordergrund, um die Anforderungen des militärischen Auftraggebers auch im Hinblick auf einen späteren Feldeinsatz zu erfüllen.

Schlussfolgerungen und Ausblick

Der Vorteil von infrastrukturlosen mobilen Netzen beim Einsatz auf der letzten Meile der Kommunikationsverbindungen ist unbestritten. Die Existenz zusätzlichen Risiken, die durch die Verwendung dieser Netze entstehen, ebenso wenig. Die Entwicklung von adäquaten Sicherheitsmechanismen ist daher unumgänglich, um die positiven Effekte dieser Netze für die Schlagkraft der Truppe nutzbar zu machen.

Die Implikationen dieser Technologie auf die Möglichkeiten für Angriffe gegen Netze sind vielfältig und deutlich weit reichender, als man dies bei auf der gemeinsamen IP-Technologie basierenden Netzen vermutet hätte.

Obwohl bereits einige viel versprechende Lösungsansätze aufgezeigt werden konnten, sind noch viele Herausforderungen im Bereich taktischer MANETs ungelöst. Forschungsprojekte wie das genannte MITE-Projekt zeigen Lösungswege auf, die schließlich in industrielle Produkte für den breiten militärischen Einsatz einfließen werden.

Autoren

Dipl.-Inform. **Elmar Gerhards-Padilla**
ist wissenschaftlicher Mitarbeiter am Institut für Informatik, Abt. IV, der Universität Bonn und befasst sich dort u. a. im Forschungsvorhaben MITE mit Sicherheitsaspekten von Adhoc-Netzen.

Dipl.-Inform. **Marko Jahnke**
ist wissenschaftlicher Mitarbeiter am Forschungsinstitut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) und ist Projektleiter des Forschungsvorhabens MITE.