SICHERBARES AD-HOC SATCOM SYSTEM (tAHSD)

CODE JAHRESTAGUNG 2022 – INNOVATIONSKONFERENZ CYBER/IT
PATRICK ROSENTHAL, 13.07.2022

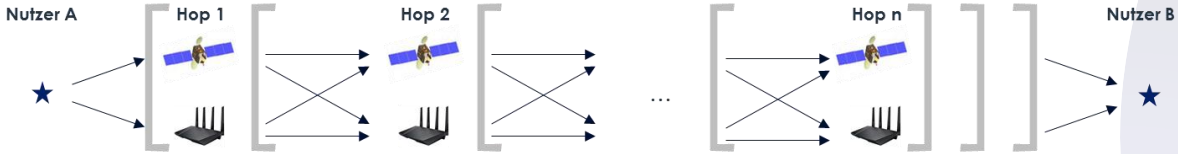
ÜBERSICHT

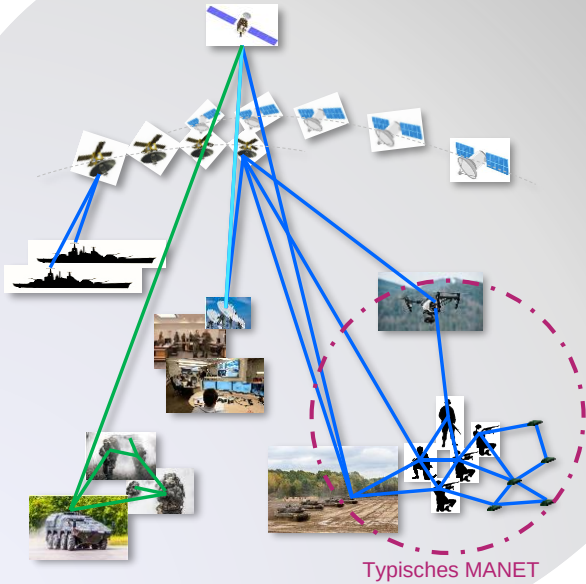
1. Ad-hoc Satcom (AHS) Konzept
2. BOS@Satcom Demonstrator
3. Angriffspunkte & Sicherungsmöglichkeiten
4. Maßnahmen tAHSD vs. MANET, Weitere Aspekte, Fazit

Date: 13/07/2022
Ref: CODE2022_tAHSD_Rosenthal_V01
Template: 83230347-DOC-TAS-EN-011

AHS KONZEPT 1/2

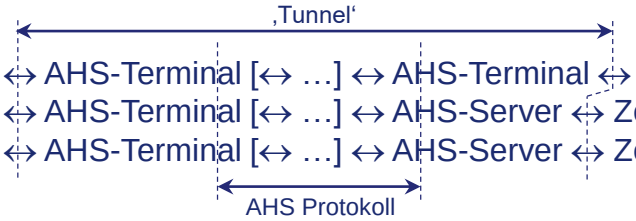
/// MANET & AHS Topologie: Jeder Knoten ist gleichwertiger Router





/// AHS Datenübertragungen

- An-(/Ab)meldung, zentr. Routenanfrage, Statistische Daten — AHS-Terminal [→ …] → AHS-Server (‚Zentrale Einheit')
- Freigabe, Routen, Deaktivierung — AHS-Server [→ …] → AHS-Terminal
- Nutzdatenübertragung (Route im Datenpaket, ggf. Routenaktualisierung)



Date: 13/07/2022
Ref: CODE2022_tAHSD_Rosenthal_V01
Template: 83230347-DOC-TAS-EN-011

AHS KONZEPT 2/2

Vom MANET zu tAHSD - taktisches Ad Hoc Satcom System / Demonstrator

/// Satellitenverbindungen > ermöglicht **Zentrale Einheit**

/// Zentrale Einheit > ermöglicht Zentrales Routing & Überwachung & PKI

/// Neuartiger Routing Algorithmus > Routenumschaltung je Paket, **skaliert** $\sim a\sqrt{N}\cdot \lg N\,, a < 1\mu s$

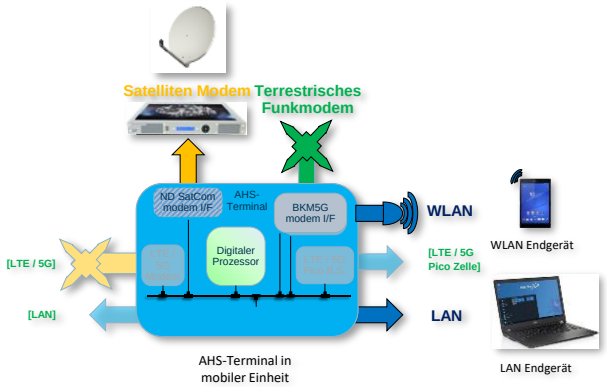
/// Neuartiges AHS-Protokoll > **Transparenter Tunnel, flexible Dienste**

/// Kompatibel mit beliebigen vorhandenen Simplex- oder Duplex-Punkt-zu-Punkt Verbindungen

/// An ein AHS-Terminal können z.B. 4 Funkmodems und >50 Endgeräte per LAN oder WLAN o.a. angeschlossen werden

/// Keine Veränderung an Endgeräten oder Modems nötig

- Beibehaltung der vorhandenen Sicherungsverfahren



Zentrale Komponente, Transparenter Tunnel, flexible Dienste, hohe Verbindungsredundanz

⇒ **MANET wird sicherbar !**

Date: 13/07/2022
Ref: CODE2022_tAHSD_Rosenthal_V01
Template: 83230347-DOC-TAS-EN-011

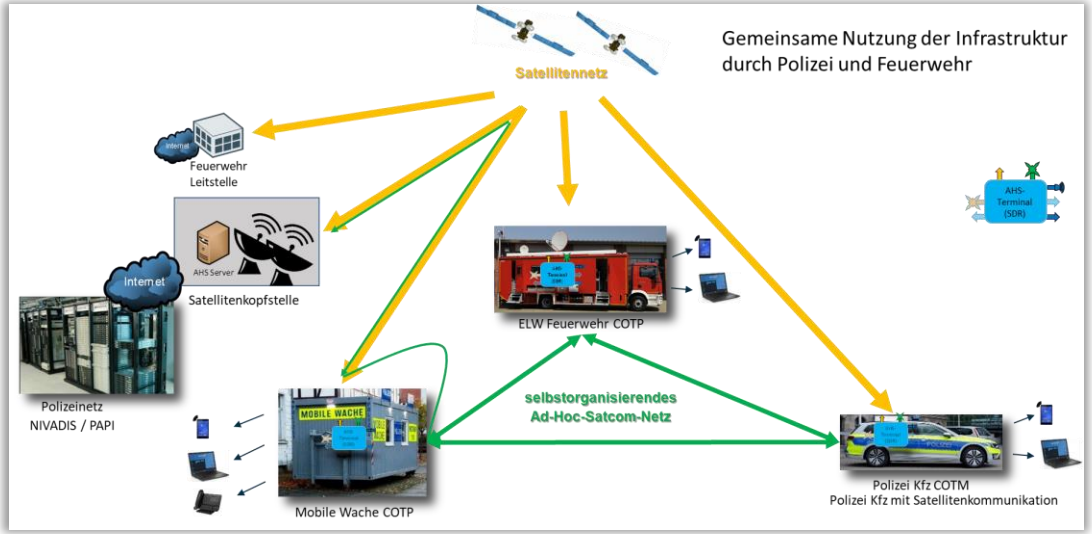
BOS@SATCOM DEMONSTRATOR

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

BOS@Satcom wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie unter dem Förderkennzeichen 50YB2012 und 50YB2014 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.



Quelle: ASDN Autorisierte Stelle Digitalfunk Niedersachsen

Projekt Partner:

POLIZEI NIEDERSACHSEN

Business Experience
Telecommunication – IT – Media

ND SATCOM

DLR Deutsches Zentrum für Luft- und Raumfahrt

ThalesAlenia Space
a Thales / Leonardo company

eutelsat

Machbarkeit in Feldtests mit 2 GEO-Satelliten bestätigt:
Skalierbarkeit, Flexibilität, Integierbarkeit in bestehende Komm.-Systeme (inkl. VPN)

ThalesAlenia Space
a Thales / Leonardo company

ANGRIFFSPUNKTE & SICHERUNGSMÖGLICHKEITEN

/// System-Ebenen > Angriffsmöglichkeiten > Sicherungsmöglichkeiten

- Sicherstellen von benötigter Verfügbarkeit / Authentifizierung / Vertraulichkeit / Integrität / Nachweisbarkeit für Datenübertragungen
- Maßnahmen: Prävention; Detektion, Reaktion

System – Ebenen ↑ ↓

Zentrale Einheit	> Ausschalten / Manipulieren / Nachahmen	> Redundanz, Zugangskontrolle, Root CA (PKI)
Benutzer	> Missbrauch des AHS-Terminals, Desinformationen	> Authentifizierung (PKI), Statistische Überwachung
Anw.-Software	> Modifikation AHS-SW/-Protokoll, Schad-SW	> Selbstüberwachung, Statistische Überwachung
AHS-Protokoll	> Topologie Aufklärung, Routen-Manipulation, Mithören	> Daten- / Routen-Verschlüsselung, Kooperation
Betriebssystem	> Sicherheitslücken (Viren etc.), offene Schnittstellen	> ‚Härtung', kein routing, kein forwarding
Digitalelektronik	> Sicherheitslücken, offene Schnittstellen	> ‚Härtung', Überwachung durch Anw.-SW
Verbindung	> Stören, Mithören	> ‚Cognitive Radio', Datenverschlüsselung

/// Sicherungsmaßnahmen …

- hängen vom Anwendungsfall ab (öffentlich / kommerziell / BOS / taktisch)
- sind innerhalb eines Knotens, aber auch über mehrere Knoten hinweg notwendig
- gegenüber Rechen- und Netzwerklast, sowie ggf. Energiebedarf abwägen

Date: 13/07/2022
Ref: CODE2022_tAHSD_Rosenthal_V01
Template: 83230347-DOC-TAS-EN-011

MAßNAHMEN tAHSD vs. MANET

/// PKI und Statistische Überwachung sind bei tAHSD im Gegensatz zu anderen MANETs möglich

- Identifikation von schädlichen Knoten anhand von inkonsistenter Netzwerk-Statistik und gezielte Deaktivierung
- Sicherung des AHS-Servers mit bekannten Maßnahmen

/// Unkooperative Knoten können im Gegensatz zu anderen MANETs erkannt und ggf. geduldet werden

- Grad der möglichen Kooperation wird im AHS-Protokoll übertragen und ist der Zentralen Einheit bekannt

/// Verbleibende Punkte

- Nächste Schritte: Erweiterung des Demonstrators um …
  - PKI (Root CA in Zentraler Einheit)
  - SW-Lizenz mit periodischem Selbsttest
  - AHS-Server Redundanz
  - Cognitive Radio (Modem: Mehrkanal-HF-Frontend/SDR)
- Zu untersuchen: Endgerät hat Sicherheitslücke (z.B. eigene, unzureichend gesicherte Internetanbindung)

/// **Fazit:** tAHSD verbessert die MANET-Eigenschaften um Sicherungsmaßnahmen gegen …

- feindliche Übernahme von Knoten mittles PKI und statistischer Überwachung
- unkooperative Knoten mittels flexibler Kooperation und statistischer Überwachung
- physisches Ausschalten mittels hoher Knoten-/Netzwerkredundanz

Vielen Dank für Ihre Aufmerksamkeit !

Kontakt:
Patrick Rosenthal
✉ patrick.rosenthal@thalesaleniaspace.com
✆ 07156 353 28410

BACKUP: ANGRIFFSTYPEN

Quelle:
Ali Dorri and Seyed Reza Kamel, Esmail kheyrkhah
SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS: A SURVEY

International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015

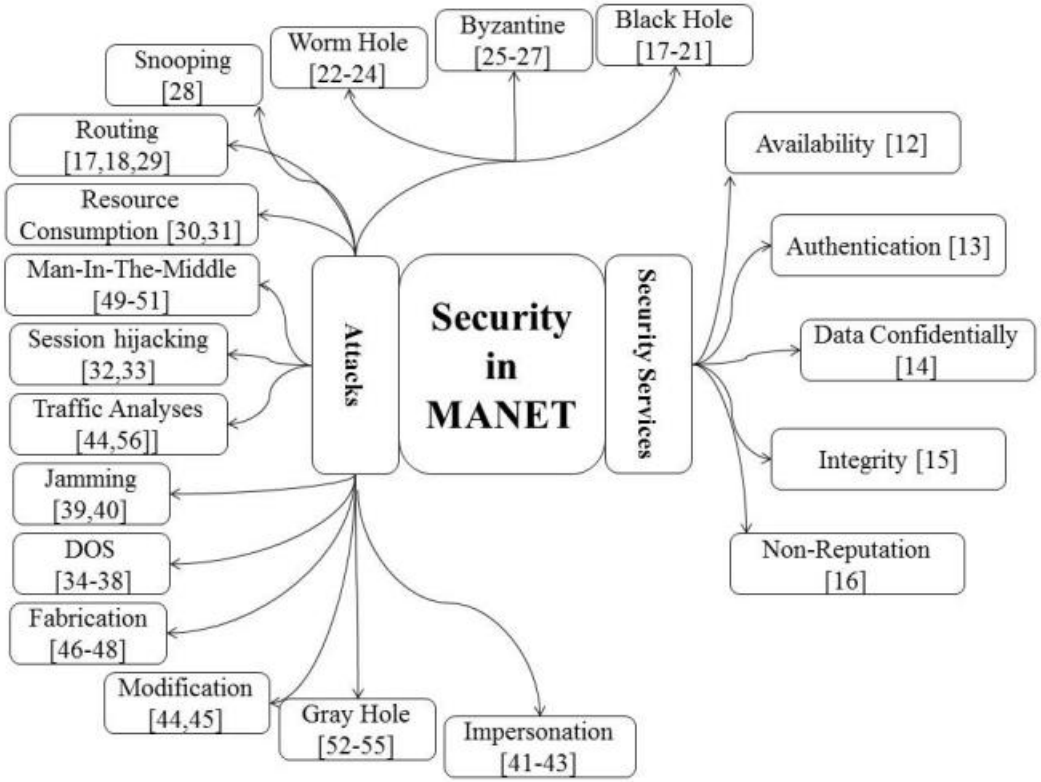


Figure 2. Security Aspects in MANET

Date: 13/07/2022
Ref: CODE2022_tAHSD_Rosenthal_V01
Template: 83230347-DOC-TAS-EN-011