

Taktisches Ad-Hoc Satcom System (tAHS)

Erläuterung der Problemstellung, die mit der Idee gelöst werden soll:

Die Koordination und Steuerung der verschiedenen Einheiten in weltweiten Einsatzgebieten zu Land, Wasser und in der Luft erfordert eine mobile, schnell aufzubauende, zuverlässige und abhörsichere Kommunikationstechnik zwischen den Einheiten und der Führung bis hin zum Lagezentrum. Neben Sprachübertragung werden auch Daten- und Bild- und Filmübertragungen benötigt. Mit Blick auf zukünftige Einsatzszenarien müssen in Sekunden mehrere hundert bis tausend Knoten verbunden werden oder gegen Angriffe solcher Verbünde durch entsprechend hohe Redundanz der Verbindungen resistent sein.

Hierfür eignen sich mobile ad-hoc-Netzwerke (MANETs). Deren Nachteile sind allerdings die relativ kurze Reichweite von wenigen 100 bis 1.000 Metern, die die Größe des Einsatzgebiets und der räumlichen Trennung zum Lagezentrum entsprechend einschränkt. Zum Zweiten lassen sich nur wenige 100 Knoten verbinden, was insbesondere für "Internet of Battle Things (IoBT)" -Netzwerke bzw. für Netzwerke mit hoher Verbindungsredundanz (und damit entsprechend hoher Knotenzahl) eine starke Einschränkung ist. Das limitierende Problem ist, dass ab einer Knotenzahl von einigen 100 bis wenigen 1000 das Übermitteln der einzelnen Datenpakete ('routing') entweder viel zu langsam erfolgt, oder die Routing-Tabellen viel zu groß werden (mehrere 100 MB bis GB) und zudem wegen der sich ändernden Topologie bei mobilen Ad-hoc-Netzen permanent aktualisiert/ausgetauscht werden müssen.

Durch den nachfolgend beschriebenen Ansatz wird das Reichweitenproblem sowie das Routingproblem bei größeren bis globalen Ad-Hoc Netzen gelöst. Eine hohe Knotenzahl ermöglicht außerdem eine hohe Redundanz, wodurch solche Netzwerke nur schwer von außen ausgeschaltet werden können. Durch einfaches Ausbringen (z. B. luftgestützt, in Fahrzeugen platziert oder als man-pad) und sensorbasiertes automatisches Aktivieren der Knoten, kann ein solches Netzwerk auch in Gegenden ohne jegliche Infrastruktur eingerichtet und betrieben werden. Die Verfügbarkeit des Netzwerkes ist ohne weitere Fremdeinwirkung nur durch die Energieversorgung eines Terminals (Akku, Solar, etc.) begrenzt. Das Netzwerk lässt sich zudem flexibel durch unbemannte Knoten ('Relais-Stationen') erweitern.

Beschreibung der Idee und wie sie das Problem lösen soll:

Der Ansatz ist, die Modems der tAHS-Knoten auch mit Satellitenlinks zu versehen, die topologisch äquivalent zu den terrestrischen Verbindungen sind. Jeder Knoten ist hierbei auch gleichzeitig 'Router' (solange es seine Energieversorgung erlaubt). Hierdurch unterscheidet sich dieser Vorschlag von bisher untersuchten MANETS.

Durch ein neues AHS-Protokoll und einen neuartigen AHS-Routing-Algorithmus werden in Abhängigkeit von Verbindungsqualität und weiteren Diensteparametern (Redundanz, Latenz) ein oder mehrere Wege durch die tAHS-Knoten (einschließlich Satelliten) ad-hoc ermittelt. Dies geschieht nach Aktivierung eines Knotens in Sekundenbruchteilen, so dass auch eine sich ändernde Topologie (durch Bewegung oder Abschaltung von Knoten) mit nur sehr geringer

Verzögerung bewältigt werden kann, und dies weltweit. Voraussetzung für den AHS-Algorithmus ist allerdings eine direkte oder indirekte Satellitenverbindung, da er auf Systemebene ausgeführt wird (dadurch aber auch nur schwer angreifbar ist).

Die topologisch äquivalente Einbindung von Satelliten behebt das Reichweitenproblem, der AHS-Algorithmus behebt das Routing Problem.

Für die sichere Datenübertragung enthält das AHS-Protokoll zwischen der Routing- und der De-/paketierungsschicht eine Verschlüsselungsschicht, sowie in der physischen Schicht eine weitere Verschlüsselung für ein wählbares Verfahren. Die einzige Einschränkung liegt eventuell in einer vorgegebenen Latenz, die im Falle eines aufwendigen Verschlüsselungsverfahrens entsprechend groß ausfällt.

Grundsätzlich laufen alle bis auf die physische Schicht des AHS-Protokolls aus der Sicht anderer Übertragungsprotokolle auf der Anwendungsschicht. Damit kann tAHS prinzipiell auf bereits vorhandenen - auch proprietären - Protokollen aufsetzen. Somit kann die Konvergenz zu bestehenden Systemen in der Bundeswehr gewährleistet werden.

Zu berücksichtigende Akteure wären aus heutiger Sicht die entsprechenden F&T-Stellen der Bundeswehr, (incl. WTD und Frequenzkoordinator), UniBw sowie Thales.

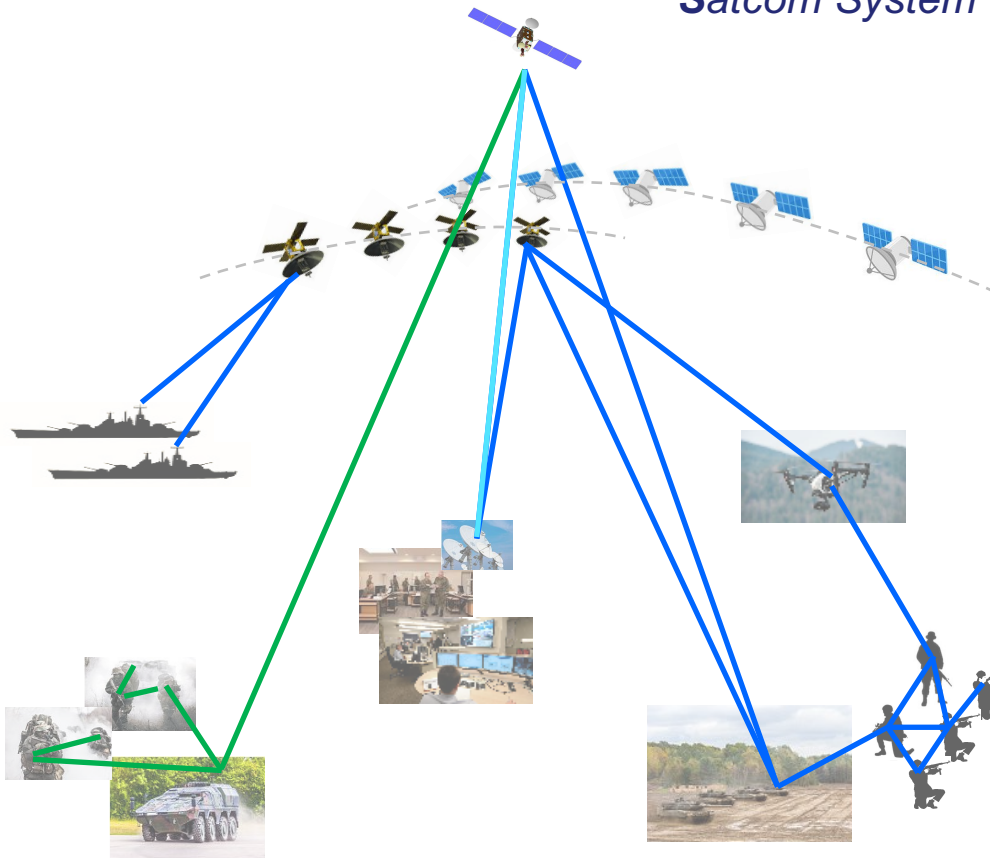
Ziel ist es, in enger Abstimmung mit den o.g. Akteuren einen Demonstrator für ein Proof-of-Concept zu entwickeln. Dabei wird weitestgehend auf die Verwendung von bereits vorhandenen Komponenten wo möglich zurückgegriffen.

tAHS – taktisches Ad Hoc Satcom System

CODE 2019, Innovationstagung, 10.Juli 2019



Vom MANET zu tAHS — *taktisches Ad Hoc Satcom System*



/// Mobile Ad-Hoc Netzwerke

Sehr flexibel und schnell einsatzbereit, aber:

- / Reichweiten-Problem („WLAN“-artig)
- / Routing-Problem (~ wenige 100 Knoten)

tAHS: Ad-Hoc Satelliten Verbindungen ermöglichen ohne Anwendungs-Bodeninfrastruktur zusätzlich:

- ... Verbindung zum Lagezentrum,
- ... zu weiteren Einheiten,
- ... oder zu Drohnen,
- ... auch zur Marine.

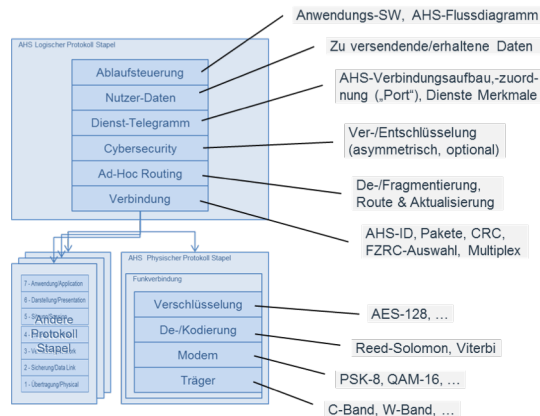
/// tAHS ermöglicht:

- / Großflächige mobile Abdeckung
- / Hohe Knoten-&Verbindungszahl → vielfache Redundanz
- / Separate Einsatzgruppen
- / Datenraten für Text, Sprache, Video (5Mbps)

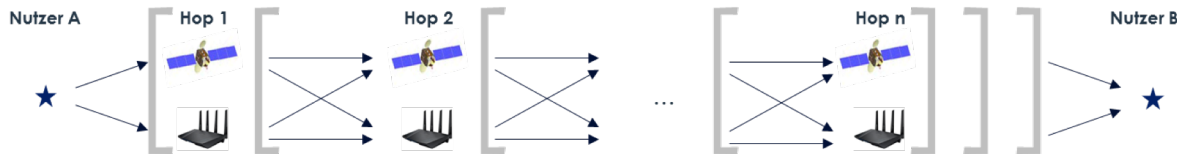
Auslegung

/// Skalierbar (Satelliten, Knoten, Bereich, Dienste) → Stufenweiser Aufbau

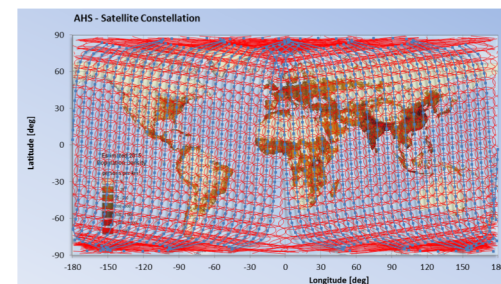
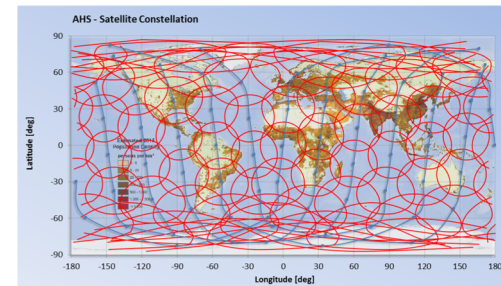
/// Protokoll-Stapel
→ Kompatibel mit
anderen Funkverfahren



/// Topologie → Jeder Knoten gleichwertiger Router, AHS-Routing Algorithmus



/// Zwei Modem-Typen
→ Kostenoptimierung



Satelliten erlauben weitreichende Ad-Hoc Vernetzung & AHS Algorithmus erlaubt eine hohe Knotenzahl/Robustheit
ABER: Angreifbar → Zusätzliche Maßnahmen notwendig ...

Angreifbarkeit

/// Physisches Ausschalten von Knoten

→ Hohe Verbindungsredundanz

/// Störsender

→ Frequenzhopping, Beamforming/Cognitive Radio

/// Funksignale Mithören

→ Verschlüsselung, Schlüsselmanagement, asymmetrische Verschlüsselung

/// Feindliche Übernahme eines Knotens: Mithören, Netz aufklären

→ Knoten stummschalten

/// Feindliche Übernahme eines Knotens: Manipulation von Daten oder Topologie

→ Vitaldaten-/Verhaltens-/Topologieprüfung, Selbst-Deaktivierung/Notsignal, Knoten stummschalten

tAHS besitzt inhärente Robustheit

Komplexere Angriffe durch zentrale (automatisierte) Datenauswertung erkennbar und erschwert oder abwehrbar

Vielen Dank für Ihre Aufmerksamkeit !

Kontakt:

Patrick Rosenthal

📞 +49 7156 353 28410

✉️ patrick.rosenthal@thalesaleniaspace.com

Mario Scaramuzzino

📞 +49 7156 353 43805

✉️ mario.scaramuzzino@thalesaleniaspace.com