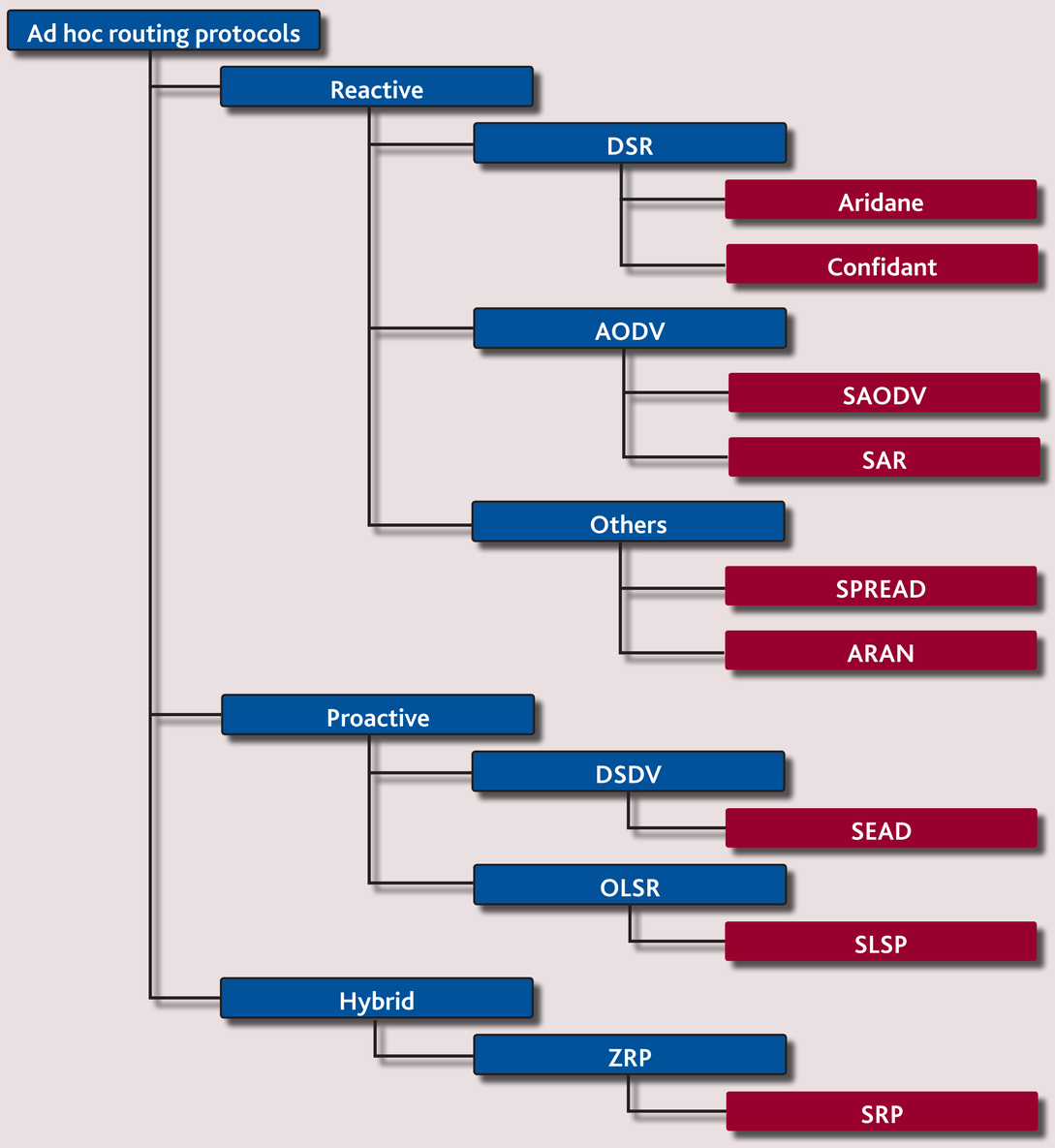
Security Challenges in Mobile Networking: Mobility Management and Routing

Kaj Grahn, Jonny Karlsson, and Göran Pulkkis, Arcada University of Applied Sciences

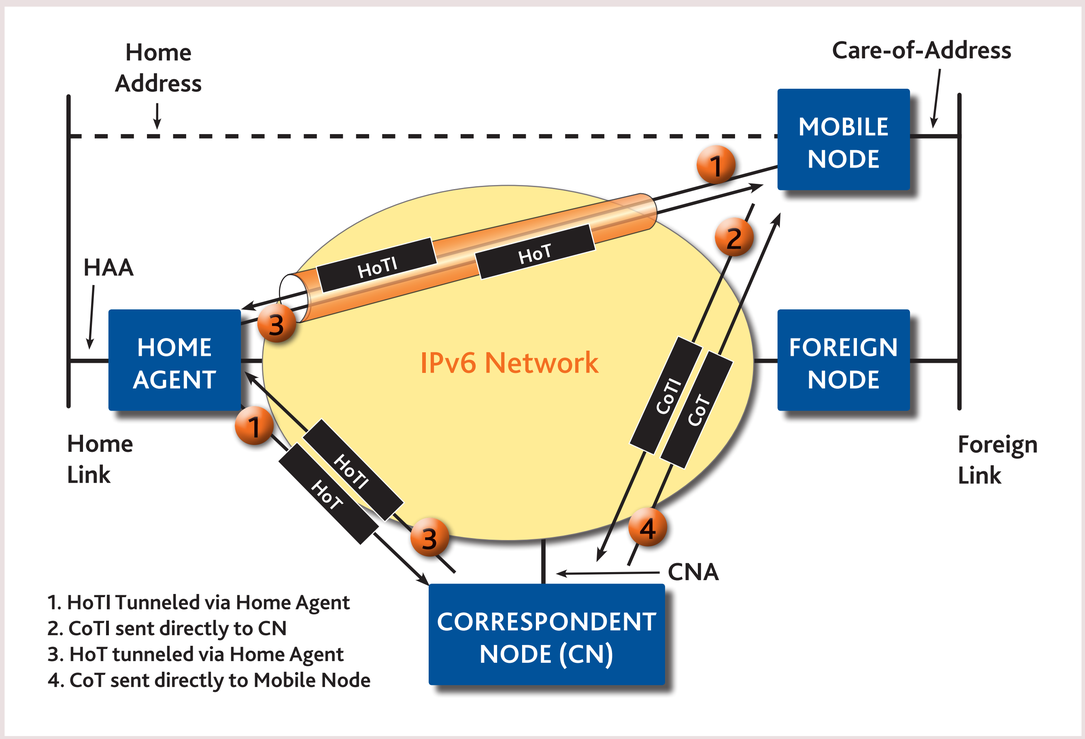
SEAMLESS ROAMING, VERTIVAL HANDOVER AND MOVING NETWORKS IN RELEVANT PROTOCOLS

- Mobile ad-hoc networks (MANETS)
- Mobile Internet Protocol (MIP)
- Network Mobility (NEMO)
- Mobile Internet Key Exchange (MOBIKE)
- Host Identity Protocol (HIP)
- Mobile Stream Control Transmission Protocol (mSCTP)
- Datagram Congestion Control Protocol (DCCP)
- Session Initiation Protocol (SIP)

Security extensions have been proposed for several MANET routing protocols. A proactive protocol periodically updates routes for immediate use. A reactive protocol starts route determination on demand. A hybrid protocol combines the best features of proactive and reactive protocols. Security extensions are based on authentication of routing messages (Ariadne, SAODV, SAR, SPREAD, ARAN, SEAD, SLSP, SRP) and on reputation (Confidant)



The Return Routability procedure



Identified SIP threats/attacks, their impact on security, and protection solutions

Attacks	Impact	Solutions
Eavesdropping: Unauthorized interception and decoding of signalling messages.	- Loss of privacy and confidentiality	Encryption of transmitted data using TLS or IPSec.
Viruses and Software bugs (Malformed Packet).	- DoS - Unauthorized access	Install antivirus applications. Apply software patches.
Reply attacks: The retransmission of a genuine message so that the device receiving the message reprocesses it.	- DoS	Encrypt and sequence messages (Cseq and Call-ID headers)
Spoofing: Impersonation of a legitimate user sending data.	- Unauthorized access	Send address authentication between call participants.
Message tampering/integrity: the received message is the same as the sent message .	- Loss of integrity - DoS	Encrypt transmitted data using encryption mechanisms like IPSec, TLS and S/MIME.
Prevention of access to a network service by bombarding SIP proxy servers/registrars or voice-gateway devices on the Internet with inauthentic packets (SPAM and its variants: Spam over Instant Messaging (SPIM) and Spam over Internet Telephony (SPIT)).	- DoS	Configure devices to prevent such attacks.
SIP-enabled IP phones: Trivial File Transfer Protocol (TFTP) Eavesdropping, Dynamic Host Configuration Protocol (DHCP) Spoofing, Telnet.	- Loss of Confidentiality - Unauthorized access - DoS	SIP phones make TFTP requests to update configuration and firmware files. TFTP is insecure since files are sent unencrypted. Disable TFTP and allow Telnet in configuration updates only to administrators.

Traditional IP (left) and HIP enhanced TCP/IP protocol stacks