



PIGEON

PACKET INTERCHANGE GATEWAY FOR ENCRYPTED OVERLAY NETWORKING

ENCRYPTED NETWORKING FOR THE DIGITAL BATTLESPACE

PIGEON forms a single self-organizing network across the tactical radio, cellular and satellite links, partitioned into separate encrypted communities over shared physical links. Uncrewed platforms, sensors, crews and command nodes exchange machine-to-machine data to enable dynamic missions in contested environments.

CORE CAPABILITIES

Single Network Across Dissimilar Bearers

Tactical radio, cellular and satellite links carry one routed network, with traffic following the links available at the time. Bearer optionality provides mission and supply chain flexibility, with no dependency on a single radio supplier or waveform.

Cryptographic Need-to-Know Over Shared Links

Each community is a separate encrypted overlay network, providing connecting coalition partners, sensor cohorts or mission participants. A node may provide transport or access to several communities concurrently.

Direct Distribution of Sense, Decide, Effect Mission Data

Tracks, markers and sensor detections transit node to node to the crews and dismounted users that act on them, and operator position is independent of the data path.

PLATFORM CLASSES

Uncrewed and attritable

Ground and maritime uncrewed systems, reconnaissance air vehicles and unattended sensors: platforms fielded where recovery is not assumed.

Crewed platforms and command

Armoured and protected vehicles, mobile command posts and field headquarters, where custody is held by the crew for the duration of the mission.

Dismounted and gateway

Tactical end-user devices, soldier-worn radio gateways, and vehicle or site switches presenting several networks to one node.

Demonstration available against a customer-supplied bearer mix and platform set.

SPECIFICATION	
Host	Software on the Linux mission compute already carried by the platform (ARM64, x86_64), or supplied as a self-contained node. An IP transport layer only: mission data is carried, not interpreted, and no proprietary interface is presented to a battle management system.
Beareres	Tactical radio and MANET waveforms, cellular, satellite and Ethernet, concurrently on one node. Any bearer presenting an IP or Ethernet interface.
Network	Self-organizing encrypted mesh with no network controller and no route server. Routes re-converge as links change and following a partition.
Traffic	Any IP payload, unicast and multicast, with multicast preserved end to end within a community. Built for ISR, BMS and M2M protocols like RTP, CoT, SAPIENT, Asterix and DDS.
Security	Traffic is encrypted node to node and remains opaque to the bearers carrying it. Keys are derived per node, rooted in a removable hardware token, and rotate on a schedule without dependence on a reachable server.
Sustainment	A node retains no mission state and is not bound to its chassis; replacement consists of fitting the token and credential to a new unit. Provisioning, connection and power-on require no per-link configuration and no route planning between sites.

CONTACT:

Adam Henrichs

Director Advanced Development

adam.henrichs@rheinmetall.com.au

Rheinmetall Defence Australia

MILVEHCOE · 111 Robert Smith Street · Redbank QLD 4301 · Australia · www.rheinmetall.com.au