Cross Domain Autonomous Communication Protocol for DTN

Mehmet Yavuz Adalier, Antara Teknik LLC

Scott Burleigh, Jet Propulsion Laboratory, California Institute of Technology

Cybersecurity Track

NAECON 2018

Part of this research was performed at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. Government sponsorship acknowledged.

Motivation

Goal:

Clusters of spacecraft that autonomously communicate among themselves in order to adapt to complex and rapidly changing environments

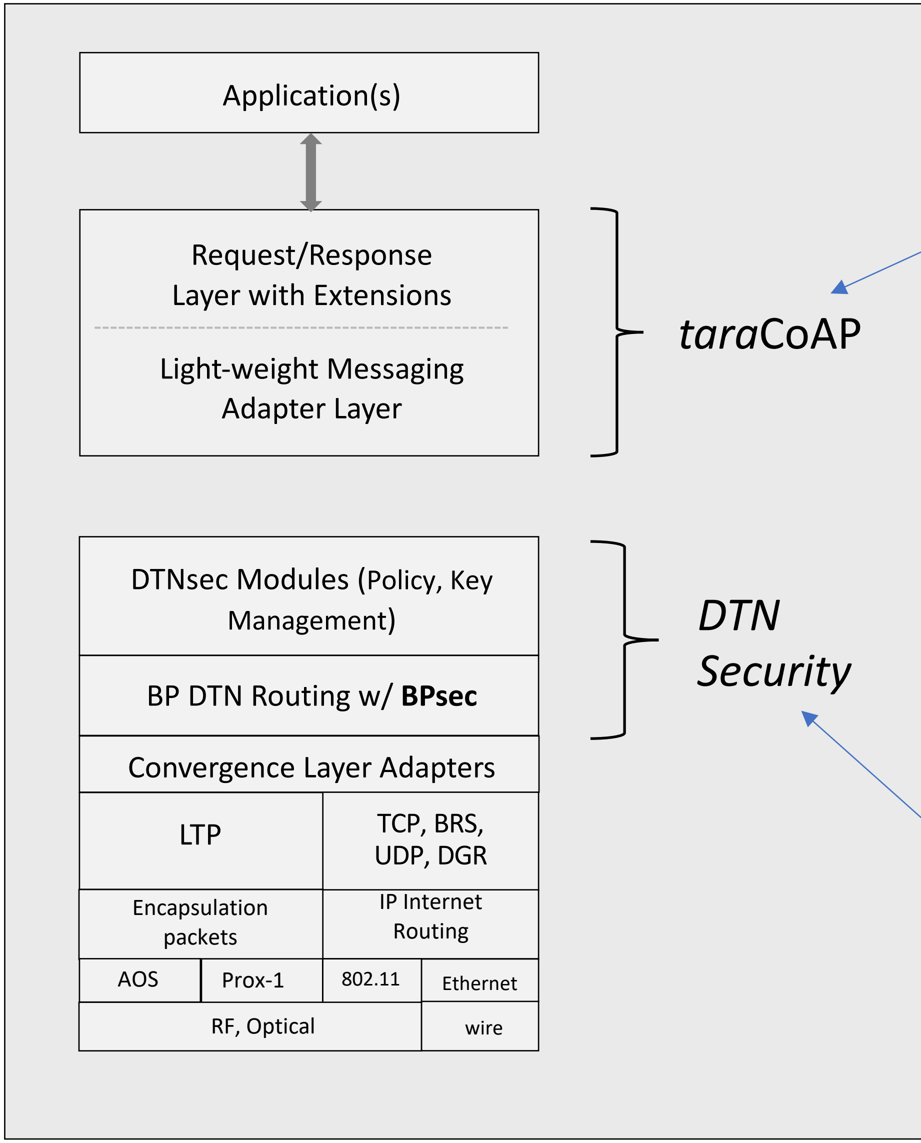
- Habitat Set-up, Support operations, Tear-down
- Rendezvous and Proximity Operations
- Robotic Exploration Teams

Requirements:

1. Scalable, standards-based M2M communication protocol
2. Secure, Interoperable Delay Tolerant Network

Cybersecurity must be an integral component of the solution architecture, not an afterthought

Key Solution Elements



- Converts application intents to:
  - Communication Policies
  - Asset Observation Policies
  - DTN Security Policies
- Provides:
  - RFC7252 Functionality
  - Policy Engines
  - Extensions such as Enhanced Observation, PubSub, etc.

- API for DTN security administration
- Key management (DTKA)
- BPsec functionality
- Multiple Cipher Suite Support

AntaraTek

*tara*CoAP

- Cross-architecture, cross-OS, standard C based SW module
- RFC7252 compliant (except for DTLS and UDP bindings)
  - Provides standard Methods PUT, GET, POST, DELETE
  - Extensible and scalable through Resources and Options Processing
  - Nodes can simultaneously act as ‘clients’ and ‘servers’
  - Support confirmable, acknowledgement and non-confirmable messages
  - Support Separate and Piggybacked Responses
  - Extensible request and response options
- Architectural Enhancements:
  - CoAP Operations Concurrent Execution Manager
    - Manages multiple simultaneous clients and servers
    - Issues multiple requests and/or handles simultaneous requests from multiple nodes
    - Maintains coherency to support indirect requests

Tested with NASA’s Interplanetary Overlay Network (IONv3.6.1)

*tara*CoAP Cyber-Physical Autonomous Asset Observation and Management

- Supports and enhances:
  - RFC 7641, "Observing Resources in the Constrained Application Protocol,"
  - draft-ietf-core-coap-pubsub-02, "Publish-Subscribe Broker for the Constrained Application Protocol"
  - Additional methods: DISCOVER, CREATE, REMOVE, PUBLISH, SUBSCRIBE, UNSUBSCRIBE, READ
  - Sleep-Wake Mode
- Policy Driven Trusted Anchors as brokers
  - Can substantially reduce network traffic while cloaking nodes to conserve power and/or maintain a security posture
  - Utilizes clients' "Observation Trust Level" and server's explicit consent to share with authorized subscribed clients based on rules
  - Observation servers are non-blocking and can be real time configured
  - Uses Intrusion Prevention System to enhance availability

Cross-cutting Cross-architecture Security

- IONsec API and Administration
  - Handles static key generation (symmetric and private/public), secure key storage and access
  - Add/delete/change/get info on security objects including BPsec BIB and BCB Policies

- Enhanced Keying with Delay Tolerant Key Agreement
  - Secure, mission-configurable, dynamic key management and distribution
  - ECC based for efficiency and scalability

- High Performance High Security Implementation of BPsec
  - Low footprint confidentiality and integrity/provenance functionality
  - Seamless support for multiple Cipher Suites
  - Multiple Quality of Service (QoS) Levels
  - Algorithmic optimizations and asynchronous execution methods

AntaraTek

Delay Tolerant Key Agreement

1. Perform Timely Key Provisioning
   - Keys must be available at all nodes in the path before actually needed
   - Node generated public keys must be properly transported to the Key Authorities (KAs) in advance
2. Publish/Subscribe Model
   - Publish public key bulletins to all subscribing DTN nodes
   - Bulletins published on the same link as data bundles
3. Spread Publication over Multiple KAs
   - KAs agree on a bulletin through control message exchanges
   - Each KA publishes overlapping bulletin fragments
   - Receiving DTN nodes assemble bulletins
4. Availability and Security
   - Antara implementation uses approved ECC algorithms

Based on IETF draft "Architecture for Delay-Tolerant Key Administration," draft-Burleigh-dtnwg-dtka-01.txt," S. Burleigh, D. Horres, K. Viswanathan, M. Benson, F. Templin.

AntaraTek

ECC Benefits

High Security Strength and Performance with Shorter Keys

- At security strengths of interest (i.e., 128-bit and 192-bit) ECC keys are substantially shorter than RSA keys
- ECC P-256 provides 128-bit security with 256-bit keys vs RSA's 3072-bit keys.
- ECC P-384 provides 192-bit security with 384-bit keys vs RSA's 7680-bit keys.
- Smaller key sizes result in savings for power, memory, bandwidth, and computational cost that make ECC especially attractive for constrained environments.

Security Strength	Symmetric Key Algorithms	IFC (e.g., RSA)	ECC (e.g., ECDSA)
<=80		*k*=1024	*f*=160-223
112		*k*=2048	*f*=224-255
128	AES-128	*k*=3072	*f*=256-383
192	AES-192	*k*=7680	*f*=384-511
256	AES-256	*k*=15360	*f*=512+

Allowance for applying cryptographic protection on Federal Government information:
Red: Not approved; Yellow: Not in NIST standards for interoperability and efficiency reasons;
Green: Approved for beyond year 2030

AntaraTek BPsec Cipher Suite Criteria

1. Standards Based – Must use NIST defined algorithms that:
   - Can be validated under the NIST Cryptographic Module Validation Program (CMVP);
   - Can be FIPS 140-2 certified;
   - Are included in the CCSDS Crypto Algorithm Recommendations;
   - Support Common Criteria specifications;
2. Suitable for constrained nodes and delay tolerant networks:
   - High security strength without large key sizes;
   - Efficient and high-performance potential on multiple architectures;
   - Support for both pre-shared and dynamic keys;
3. Support for long data lifetime
   - Long key validity (i.e., years)
   - Algorithms must be deemed secure (i.e., security strength acceptable) beyond year 2030 (NIST SP 800-57Pt1)
4. Multiple levels of security to support multiple missions and cross-domain communications
   - Confidentiality and integrity security strength up to Top Secret/SCI;

AntaraTek BPsec Cipher Suite

AntaraTek Cipher Suites			
Confidentiality	**Code**	**Integrity**	**Code**
DTN_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xE0	DTN_ECDHE_ECDSA_WITH_HMAC256_SHA256	0xE8
DTN_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xE1	DTN_ECDHE_ECDSA_WITH_HMAC384_SHA384	0xE9
DTN_ECDHE_ECDSA_WITH_AES_128_CTR_SHA256	0xE2		
DTN_ECDHE_ECDSA_WITH_AES_256_CTR_SHA384	0xE3		
DTN_PSK_WITH_AES_128_GCM_SHA256	0xE4	DTN_PSK_WITH_HMAC256	0xEA
DTN_PSK_WITH_AES_256_GCM_SHA384	0xE5	DTN_PSK_WITH_HMAC384	0xEB
DTN_PSK_WITH_AES_128_CTR_SHA256	0xE6	DTN_PSK_WITH_ECDSA_SHA256	0xEC
DTN_PSK_WITH_AES_256_CTR_SHA384	0xE7	DTN_PSK_WITH_ECDSA_SHA384	0xED

- Confidentiality
  - AES with key sizes of 128 and 256-bits
  - Authenticated Encryption with GCM
  - CTR Mode for truly constrained devices
- Integrity
  - Keyed HASH HMAC-256 and HMAC-384
  - ECDSA with curves P-256 and P-384
- Symmetric Bundle Key Protection
  - AES 128 and 256-bit Key-wrap/unwrap function based on NIST SP.800-38F
- Interoperable with:
  - draft-birrane-dtn-bpsec-interop-cs-00, “BPSec Interoperability Cipher Suites,”
- Compliant with:
  - CCSDS Crypto Algorithm Recommendations

AntaraTek

Cross-Domain Transaction with BPsec

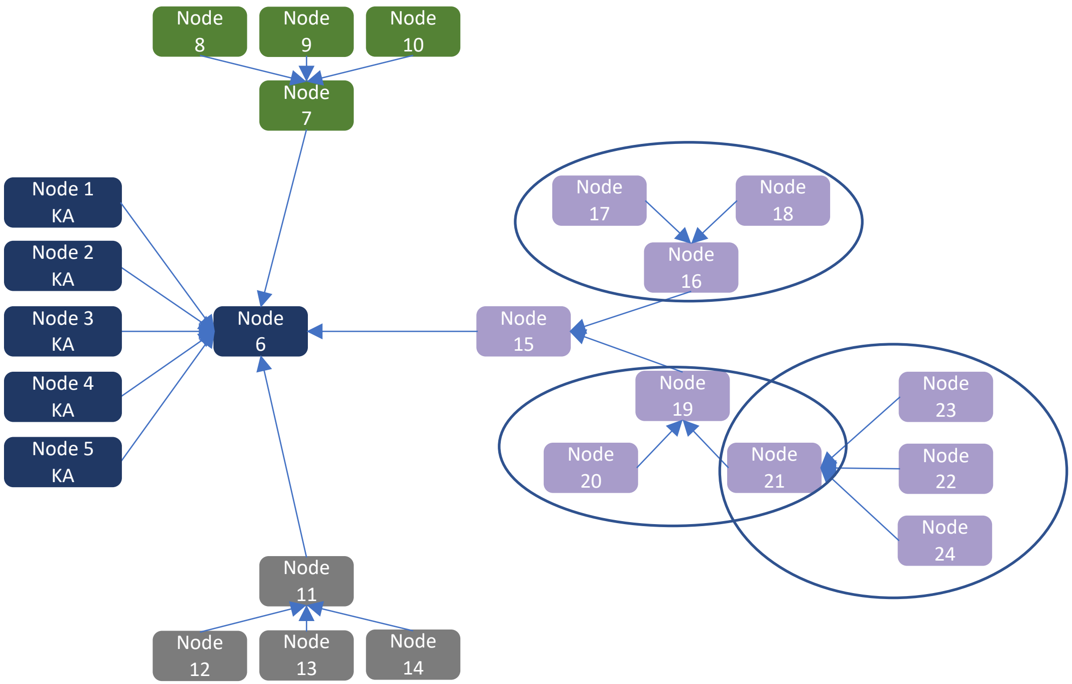
1. Use $PrivKey_{NodeA}$ and $PubKey_{NodeB}$ to derive a Symmetric Key (KEK)
2. Generate a Symmetric Encryption Key (BEK) and a MacKey (BIK)
3. Generate an Integrity Tag (T) on M with BIK
4. Encrypt Message (M) with BEK -> (EM)
5. Use KEK to encrypt BEK and BIK -> EBEK and EBIK
6. Send EM and T with EBEK and EBIK

1. Use $PrivKey_{NodeB}$ and $PubKey_{NodeA}$ to derive the same Symmetric Key (KEK)
2. Use KEK to Decrypt EBEK and EBIK -> BEK and BIK
3. Decrypt Message (EM) with BEK -> M’
4. Generate an Integrity Tag (T’) on M’ with BIK and verify T’ against T

Uses fresh symmetrical keys for each bundle
No hand-shakes required

- Based on Elliptic Curve Integrated Encryption Scheme
    - Semantically secure in the presence of an adversary capable of launching chosen-plaintext and chosen-ciphertext attacks.
- Asserted key info used for all bundles where (creation time > asserted effective time.)

24-Node Topography Tests



1. Multi-hop Message transmit
   - BPtrace encrypted message with integrity from each node to Node 6
   - Verifies Node 6 receives the expected message from each node
2. Send and Receive Secure Large Files
   - Each node produces and transmits an encrypted unique test file to every other node
   - Verifies that each Node Receives a File from Every Other Node

BPsec Security Rules for All Nodes:

BIB Rule: DTN_ECDHE_ECDSA_WITH_HMAC384

BCB Rule: DTN_ECDHE_ECDSA_WITH_AES_256_GCM

AntaraTek

Future Work

- Drive solution to TRL-7+
- Develop test environment with multiple (> 12) physical devices and sensors to analyze and optimize at system level
- Port to High Performance Spaceflight Computing (HPSC) chiplet and optimize
- Identify missions for infusion opportunities

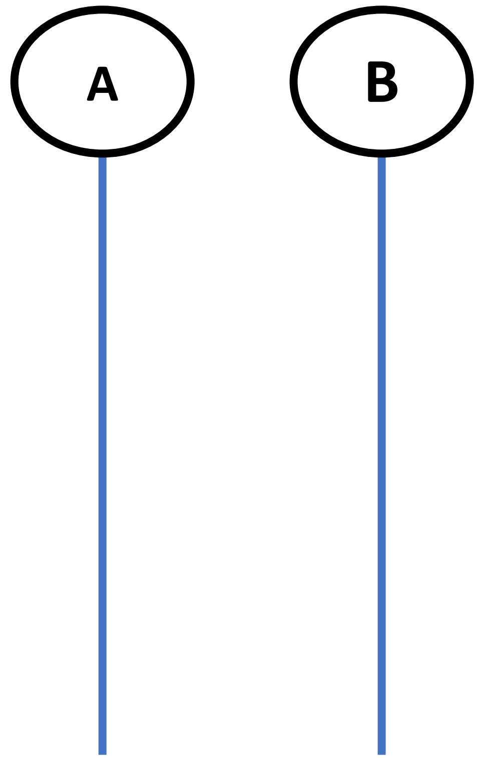
Questions

Backup

Evaluating Key Encryption Key (KEK)

Sending Node

1. Evaluates a shared secret, *Z* with $PrivKey_{NodeA}$ and $PubKey_{NodeB}$
2. Utilizes *Z,* optional “Mission specific Input” and an Aux-function to generate a unique DerivedKeyingMaterial, which is used to generate the KEK
3. The KEK does not need to be transferred



Receiving Node

1. Evaluates a shared secret, *Z* with $PrivKey_{NodeB}$ and $PubKey_{NodeA}$
2. Utilizes *Z*, optional “Mission specific Input”and and an Aux-function to generate a unique DerivedKeyingMaterial, which is used to generate the KEK

All steps done locally without any handshakes.
Aux-function is H(x) = HMAC-HASH(salt, x) where “salt” is pre-determined by the protocol