Security Analysis of DTN Architecture and Bundle Protocol Specification for Space-Based Networks

William D. Ivancic
NASA Glenn Research Center
21000 Brookpark Road
Cleveland, OH 44135
216-433-3494
william.d.ivancic@nasa.gov

A*bstract*—A Delay-Tolerant Network (DTN) Architecture (Request for Comment, RFC-4838) and Bundle Protocol Specification, RFC-5050, have been proposed for space and terrestrial networks. Additional security specifications have been provided via the Bundle Security Specification (currently a work in progress as an Internet Research Task Force internet-draft) and, for link-layer protocols applicable to Space networks, the Licklider Transport Protocol Security Extensions. This document provides a security analysis of the current DTN RFCs and proposed security related internet drafts with a focus on space-based communication networks, which is a rather restricted subset of DTN networks. Note, the original focus and motivation of DTN work was for the 'Interplanetary Internet'. This document does not address general store-and-forward network overlays, just the current work being done by the Internet Research Task Force (IRTF) and the Consultative Committee for Space Data Systems (CCSDS) Space Internetworking Services Area (SIS) - DTN working group under the 'DTN' and 'Bundle' umbrellas. However, much of the analysis is relevant to general store-and-forward overlays.

TABLE OF CONTENTS

1. INTRODUCTION

The Delay-Tolerant Network Architecture, as described in RFC-4838 [1], is a generalized store-and-forward network overlay. Its origins are from NASA JPL's experiences with high delay, store-and-forward networks for deep space, and their experience gained in the development of the CCSDS File Delivery Protocol (CFDP) [2, 3].

"To provide store-and-forward services, the Bundle Protocol (BP) sits at the application layer of some number of constituent internets, forming a store-and-forward overlay network. Key capabilities of the BP include:

- Custody-based retransmission, a willingness to take responsibility for forwarding a received bundle, thereby allowing the transmitting system to release storage buffer space.
- Ability to cope with intermittent connectivity.
- Ability to take advantage of scheduled, predicted, and opportunistic connectivity (in addition to continuous connectivity)
- Late binding of overlay network endpoint identifiers to constituent subnetwork addresses, thereby enabling a bundle to move closer to its endpoint without complete knowledge of the endpoint physical address until perhaps even the last hop." [4]

Successful end-to-end transmission of bundles depends on the operation of underlying protocols, known as "convergence layers". These convergence layers may have extremely different characteristics (e.g. addressing, security, routing) and may even be associated with completely different network types. Furthermore, the convergence layer is a functional network stack in its own right that includes a transport protocol and a network protocol. For example, bundle communication may utilize a TCP or UDP convergence layer to ride on top of an Internet Protocol network. Or, it may utilize LTP over CCSDS packets or LTP over UDP over IP or run directly on top of a Bluetooth network or even directly to a removable storage device. Each convergence layer protocol adapter is expected to, at a minimum, be able to send a bundle to all bundle nodes and to deliver to the local bundle protocol agent a received bundle, that was sent by a remote bundle node via the convergence layer protocol.

2. NETWORK SECURITY

Traditionally, a space system has been designed more or less as a direct data link between Mission Operations and the in-space asset. There are a number of reasons for this. The primary reason is that networking technology did not exist and most communication was via direct circuits and circuit switching; this was the way space communications had always been done. Techniques and technologies such as the CCSDS Space Link Extensions for Transfer Services

[1] 978-1-4244-3888-4/10/$25.00 ©2010 IEEE
[2] IEEEAC paper#1057, Version 4, Updated 2009:10:27

(SLE-TS) [5] have been developed to allow legacy systems to extend the space link over Internet Protocol networks using TCP/IP protocols.

Traditional space-based point-to-point datalinks have been secured using bulk encryption. This is a very simple way to secure a datalink, but is extremely inflexible and is only good for a single datalink. Bulk encryption is not meant for transition over a multi-hop system. When deploying bulk encryption of datalink over a network, special hardware and techniques are required to encapsulate the bulk encryption into packets that can transition the network. Those encapsulating packets need to be time-stamped and sequenced in order for the encrypted circuit to be reconstructed at the other end of the network.

Networking using packet-based (or bundle-based) techniques allows for communication over multiple hops. Each network packet (or bundle) can be encrypted (or simply digitally signed for authentication) and routed through a multi-hop system. The Bundle Protocol recognizes layering by its use of convergence layer adapters.

Network security is extremely flexible; but, with that flexibility, comes complexity. The complexity depends on the granularity and fidelity of how one may wish to secure the network.

Note, in some ways, it is much easier to secure a network, by considering at which layer security is required, and should be applied.

Keys and Policy

Both bulk encryption and network security require distribution of keys. However, for a point-to-point datalink, those keys are limited. In addition, for bulk encryption, only keys need be distributed and managed.

For network security, not only do keys have to be distributed, but there is also security policy that accompanies those keys. In addition, security is directional – that is one may be permitted to send to a source, but not to receive from the source, or vice versa. Furthermore, the keys may have lifetimes associated with them, requiring refresh or replacement upon expiry. These keys and policies must be managed and there must be a mechanism to distribute, refresh, and revoke the keys and policies. Furthermore, those keys and policies are only as secure as the mechanism used to distribute them.

Key management is critical for network security. Key and policy distribution is extremely difficult in a always connected network. For a disconnected or ad-hoc network such as a DTN, this becomes even more difficult. Currently, no key management mechanisms have been identified for DTNs. This is considered a major area of research.

The following are some examples of a combination of keys and policy:

(1) Internet protocols: Machine A on network *a* may communicate with Machine B on network *b* using UDP protocol and Port 5349 with key XYZ where key XYZ is valid for the next month. Machine B may not Communicate with Machine A. Thus, unidirectional communication is defined here

(2) Internet Protocols: any machine on Network A may communicate with any machine on network B and *vice versa*, using any protocol and any port with Key ABC, where Key ABC is valid for 20 years.

(3) Internet Protocols: Machine A and Machine B may communicate using a session key. They validate each other via certificates and then securely establish the session key using protocols such as IKEv2 (Internet Key Exchange version II). Each of those certificates has a lifetime. Each of those certificates has been signed by a trusted third party and can be verified – though the connectivity required for verification of the certificate may not be available, and verification may be cached and itself subject to expiry. Generally, in order to utilize session keys, the communication links need some reasonable bandwidth and relatively low delay – less than a few seconds. Otherwise, it is very difficult to negotiate session keys. One should not expect to be able to negotiate in many or most DTNs. In fact, one may only have one-way-communications and DTN should still be usable. Thus session keys only make sense for DTN networks where it is possible to negotiate in a reasonable time relative to the type of communication taking place.

(4) DTN: Bundle Agent B authenticates bundle Agent A, the previous hop forwarding agent, using key DEF. Key DEF may have a lifetime. Key DEF may have been sent to Agent B from Agent A encrypted using Bundle Agent A's private Key where Bundle Agent B has Bundle Agent A's public certificate. Agent A's key has been signed by a trusted third party and cached locally. (Note, in a DTN network, one should not expect to be able reach any type of system to validate certificates and keys in a timely manner). This type of authentication may be useful for authenticating routing protocols communications in order to thwart denial of services attacks where a rogue bundle agent wishes to inject false routing information into the network.

(5) DTN: Bundle Agent D authenticates the source that generated a particular bundle. The local DTN policy may state that Bundle Agent D only stores or forwards bundles from particular sources with pre-existing service agreements. This may be done to limit the amount of resources used by various individuals or organizations.

- This is likely the most useful form of DTN security that will be deployed in space-based networks because allocation of resources (storage, transmission, battery life, etc) is critical for a space-based DTN node.

(6) DTN: Bundle is encrypted with Key PCB. In addition, the bundle has 5 pieces of meta-data. Each meta-data block has a different fidelity of information regarding the payload (e.g map, map of Middle East, map of Iraq, map of streets of Baghdad, map of street of Baghdad with ammunition stores). Each piece of meta-data is encrypted with a different key, Key 1 – 5. This type of encryption is envisioned for use by DARPA (Defense Advanced Research Program Agency) to perform a type of secure content-based storage and delivery, whereby the URI of a DTN packet may be more in the form of request for some type of content (e.g. dtn:exec:return:middle_east.ammunition_stores)

- Key and policy management in such a system is EXTREMELY difficult and may not be realizable on a large scale.

- The applicability of this example for a space-based network is questionable due to the large amount of keying material and the complex management of such material.

Shared Keys (Group Keys)

One may wish to utilize group keys and shared keys among a large group of users in order to reduce the complexity of management of keys. However, if a key falls into the wrong hands or is compromised, notifying the group, revoking the shared key and rekeying is problematic in a disconnected network.

Utilizing group keys across multiple agencies may not be acceptable as the larger and more diverse the group, the harder it is to control the key. This, of course, is a "Rules of Engagement" decision – "How does one want to operate? How is one permitted to operate?"

Cross Enterprise Security and International Interoperability

Cross-organization security is a "Rules of Engagement" issue. There are technologies and techniques in place to enable security, depending on what type of trust relationships the various organizations have.

One technique is to have a trusted third party be the root signer of certificates in a chain of trust. If one can validate back to the root authority, the certificates are accepted.

For international interoperability with regard to a space network (consisting of both space and ground assets), technologies for generation and distribution of security keys/certificates and security policy for either Internet Protocols or DTNs is likely to fall under International Traffic in Arms Regulations (ITAR). This is a difficult, critical area that must be addressed internationally.

3. THREATS

General Security Threats for Overlay Networks

An overlay network inherits all of the good and all of the bad of the underlying networks upon which it resides. For example, if an overlay network passes over three different concatenated underlying networks, then the overlay network is vulnerable to all of the insecurities of any of the underlying networks (e.g. denial of service, man-in-the-middle, masquerading,). This makes overlay networks much more difficult to secure as one has to secure each underlying network in addition to applying proper security to the network overlay itself. On the other hand, if an overlay network resides on a very secure underlying network, one may be able to simply secure the overlay network by securing the underlying network. For example, if one already has a closed, secure Internet Protocol (IP) network and is running an overlay network such as DTN on top, one may be willing to simply allow IP security to handle the overlay network's security needs.

Understanding Protocol Layers

There are six basic areas from which security can be compromised in a DTN network: Physical Access, Physical Link, Data-Link, the Network Layer, the DTN Overlay, and the Applications.

For space-based networks, physical access is usually not an issue. One has highly controlled physical security at Mission Operations centers and ground centers and one will know who is residing on any space-base platform. Thus physical security is no different than for any other network.

Physical Media is either the wire, fiber, or radio link that data travels over. For space-based networks between the Mission Operations centers and the ground station one could do bulk encryptions over wire or fiber lines. However, it is much easier to simply encrypt at the network layer if one has either designed the system as an IP-based network or if one is capable of tunneling the datalink over an IP network. The later can become quite expensive and complex – particularly for high-speed networks.

Radio links may also be encrypted. Radio links are subject to jamming and some type of anti-jam radio system many be required. For space-based systems, if someone is jamming, they are likely in violation of international law. It is probably fairly easy to identify a jammer as they require significant equipment and knowledge of your system in order to jam you. As far as deep space is concerned, few people own and operate thirty-meter dishes.

The ***Data-Link layer*** is responsible for node-to-node (hop-to-hop) frame delivery on the same link. The Data-Link

layer contains the Media Access Control (MAC) and the Logical Link Control (LLC). It ensures that an initial connection has been set up, divides output data into data frames, and handles the acknowledgements from a receiver that the data arrived successfully. It also ensures that incoming data has been received successfully by analyzing bit patterns at special places in the frames. Some examples of data links include Ethernet, HDLC, and CCSDS Space Packet Protocol.

For space-systems, the data-link is often secured using bulk encryption immediately before entering the radio and bulk decryption immediately after exiting the radio. Special wrapping techniques exist where this encryption may occur at the mission operation center and the encrypted data sent over the network.

The ***Network Layer*** is responsible for source to destination "packet" delivery. The network layer is where addressing occurs and where routing is performed. For IP networks, the addressing occurs at the network layer and is hierarchical. IP networks are secured using IP security protocols (IPsec). IP security is tied to the interface address. Since IP security is address-based and the address can be hierarchical, IPsec can be hierarchical thereby enabling aggregation of addresses into sets to which security policies can be applied.

The ***Transport Layer*** is responsible for delivering data between appropriate application processes on two or more separate end systems via the underlying network (or datalink if no network exists). Some examples of transport protocols include the TransMission Operations Protocols (TCP) and the User Datagram Protocol (UDP) in IP networks, and the Licklider Protocol for long-delay space links. The Licklider protocol is intended to interface directly to the data-link layer in space-based implementations.

In IP networks, the transport layer is often secured using the *Transport Layer Security (TLS*) protocol. TLS provides security and data integrity across IP networks. It allows client/server applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS requires low-delay control loops and continuous or nearly continuous connectivity and therefore is of little utility in many, if not most, DTNs.

The *Licklider Transport Protocol (LTP)* is intended to serve as a reliable convergence layer over single-hop deep-space radio frequency (RF) links. LTP does Automatic Repeat reQuest (ARQ) of data transmissions by soliciting selective-acknowledgment reception reports. It is stateful and has no initial negotiation or handshakes. Hence, LTP is designed for use in and favored as the transport protocol of choice for deep space communications. There is a security specification for LTP [4] which defines security extensions for LTP generally intended to help thwart DoS attacks. However, such attacks in a space-based network are highly unlikely.

In general, a ***DTN*** is any delay-tolerant network; however, this term has been appropriated to mean a store-and-forward network overlay using the Bundle Protocol. The overall DTN is responsible for source to destination "bundle" delivery. Since data is at rest and can live for very long periods of time, this data is more vulnerable than data that simply passes through a system in the form of packets. An end-to-end control loop for resends of data may be absent, due to the disconnected nature of the underlying network.

A DTN as described in RFC 4838 [1] can be thought of as a network of application-layer gateways. This type of DTN does not really have an addressing scheme per se. Rather, it operates over Convergence Layers which are underlying protocols that accomplish communication between DTN entities using the Bundle Protocol (BP) communications. A DTN resides above the transport layer, whereas an IP network generally resides below the transport layer. A DTN can bridge between dissimilar lower-layer networks and can operate simultaneously over heterogeneous networks (i.e. CCSDS, IPv4, IPv6 and Bluetooth) or even directly over a datalink protocol. DTNs can be attacked via any networks and links they reside on at any layer.

DTNs as specified in RFC's 4838 and 5050 are name-based. To date, DTN naming is an open issue and a difficult one. How names are to be used in routing, and how this will be mapped to the underlying routing of each convergence layer network, is unclear. A naming system that allows for aggregation has the potential to greatly simplify both routing and security. For security reasons and resource allocation, one would like to be able to uniquely identify a source as well as be able to determine which group or groups this source may belong to. A properly constructed naming scheme will help considerably with this.

The ***Application Layer*** contains all protocols and methods that fall into the realm of process-to-process communications. The application layer sits on top of the DTN network layer and above the IP transport layer.

4. PRACTICAL EXPLOITATIONS

Past history has shown that four areas are generally most likely to be attacked: the network, transport and application layers, and imperfections in the code.

Network Layer Exploits

One can attack a network to either attempt to redirect traffic or to create denial of services (DOS) or disrupt the network. The implications of this regarding military networks is obvious. DOS attacks may also cause great economic impact on private enterprise, or nations. Another exploit is to simply be able to enter a closed network and cause problems elsewhere.

The DTN Bundle Security Specification defines a Bundle Authentication Block (BAB), a Payload Integrity Block

(PIB), and a Payload Confidentiality Block (PCB) to help thwart network layer exploits.

Transport Layer Exploits

The transport layer has been exploited in the Internet to create denial of services or connection hijacking. Example include: TCP SYN-flood attacks, man-in-the-middle attacks and UDP flooding.

The *Licklider Transport Protocol* defines security extensions for LTP generally intended to help thwart DoS attacks. These include options for implementing cookies and /or cryptographic authentication of a segment.

Application Layer Exploits

The Application Layer appears to be the layer of choice to exploit a system – at least within the internet – as evidenced by the vast amount of anti-virus and anti-spyware software. Most likely this is because it provides the biggest monetary payoff (e.g. identity theft, information theft). Furthermore, it may be the easiest area to attack due to the vast number of applications and ease in exploiting human behavior. One should anticipate similar exploits in DTNs.

Code Implementation Exploits

History has shown that it is often possible to exploit code implementations. The nature of the bundle protocol adds additional potential vulnerabilities that should be addressed.

Due to many variable-length fields, text-field parsing, and other bundle-processing operations, there may be risk due to implementation bugs (e.g. buffer overflows) that don't exist with fixed-width fields and binary formats (e.g. IP). There may be possibly attacks on host, CPU and memory by sending maliciously-crafted bundles and administrative records.

Implementations need to carefully consider the resources they expose and the algorithms for managing them, including local storage, link access, and memory for management of contacts, in-memory bundle-metadata, timers, etc. Internet experience shows that it's often possible to exploit implementation decisions about these things if the protocol doesn't protect them (witness TCP SYN-flood attacks which Internet community learned from and corrected in SCTP by deploying a 4-way handshake instead of a 3-way).

5. Security Assessment for Space-Based DTNs

Closed versus Open Networks

In general, space networks are closed networks. Closed networks, in theory, eliminate many of the exploits above from ever getting an opportunity to entering the system. However, once one starts interconnecting networks as would be the case for international interoperability, then one enters a gray area somewhere between closed and open.

Architectures and Security

It is generally agreed upon by security experts that the simpler the network architecture the better. The notion is that one can better understand the flow of data and the potential places the network can be exploited. One can then put security mechanisms in place to shore up any weakness.

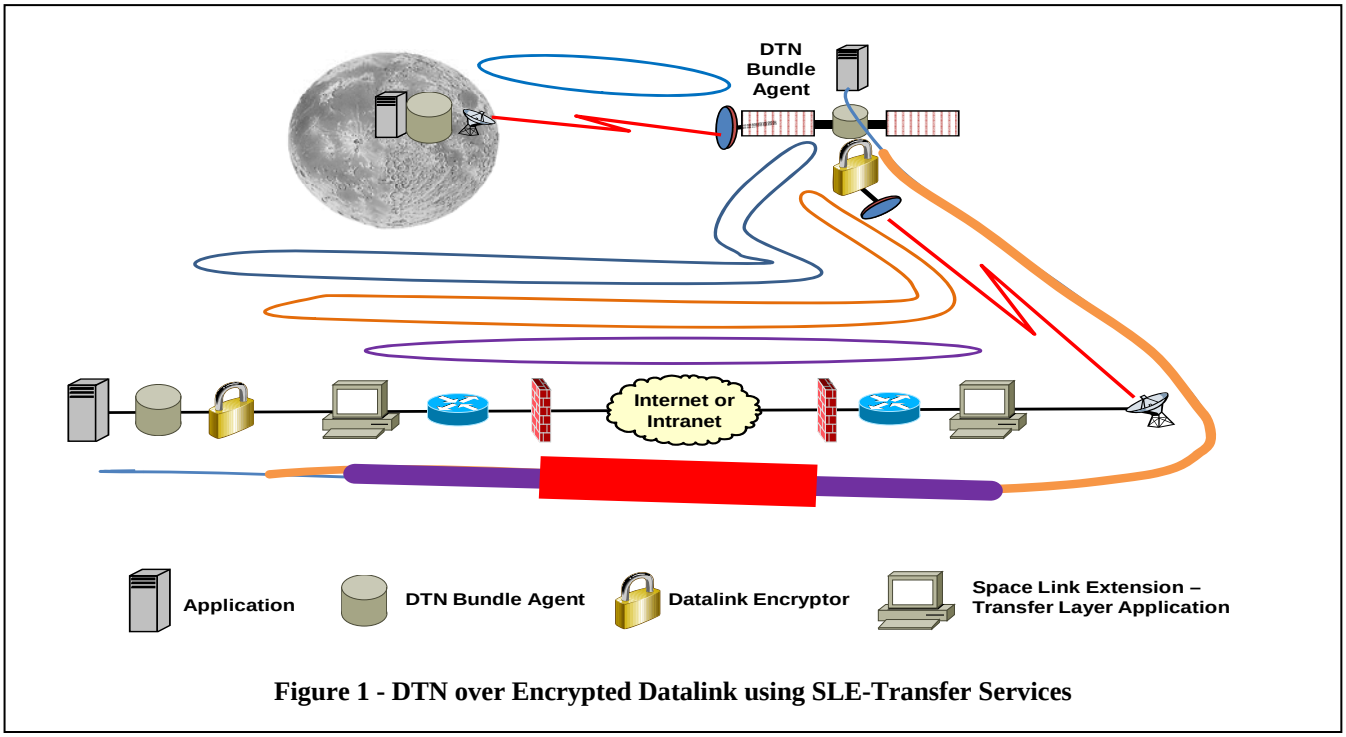

Figure 1 - DTN over Encrypted Datalink using SLE-Transfer Services

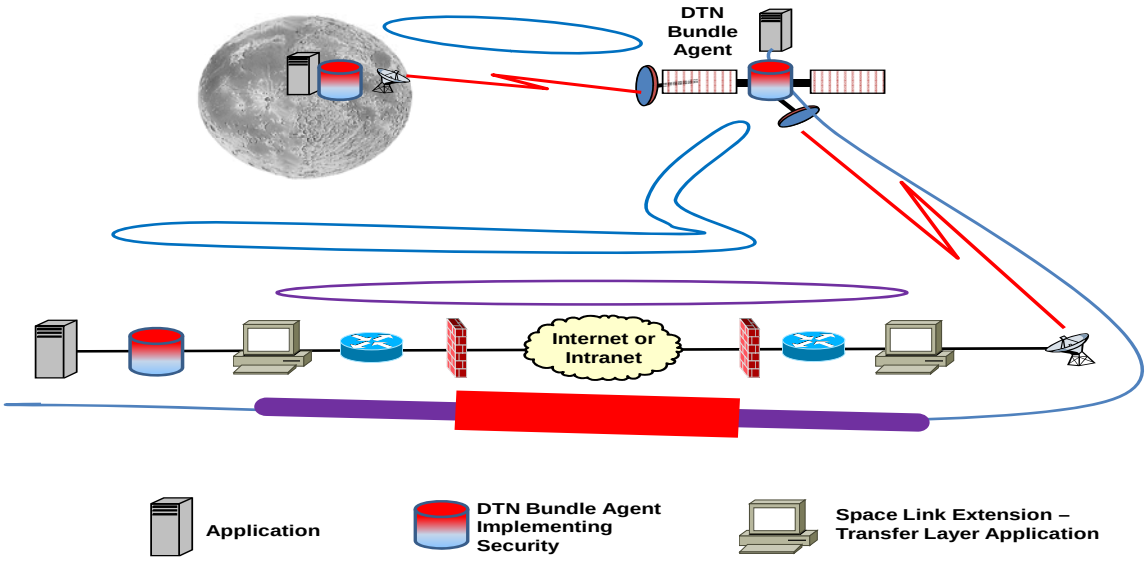

Figure 2 - Secure DTN using SLE-Transfer Services

Three simple architectures are shown in figures 1, 2 and 3. An analysis of the pros and cons of each is provided. Two have a DTN bundle agent at Mission Operations and the next hop bundle agent on the spacecraft. The third has a DTN bundle agent at each ground station. For these architectures, we assume that one would be operating via an international internetworked system as this is the most general case. Thus, assume that the Mission Operations center is sending data through a third-party ground station. In such a case, it would be unlikely that one would be encrypting the uplink at the ground station. Therefore case 1 and 2 have the datalink encrypted at the Mission Operations center and decrypted at the spacecraft. These scenarios also assume that one has to, at a minimum, encrypt the uplink at the datalink layer or network layer – here, the DTN layer. For these scenarios we assume Internet Protocols stop at the ground and CCSDS protocols are used for the space/ground communication link. One could run DTN over an IP network and use IPsec or a combination of IPsec and DTN security to secure the system

Figure 1 illustrates a scenario where a DTN node is at Mission Operations and the next hop DTN node is on the spacecraft. We assume that encryption is required and that a third party ground station is used. Thus, the datalink must be encrypted/decrypted between Mission Operations and the spacecraft. In order to synchronize bit-stream data, special datalink encryptor/decryptor is required at Mission Operations.[3] The encrypted data passes through the Space Link Extension – Transfer Services Application and an application-layer tunnel and control loop are established. The data is forwarded from Mission Operations to the appropriate ground station via a secure IPsec tunnel established between the Mission Operations and ground station firewalls. At the ground station, the datalink data is extracted from the SLE-TS tunnel and forwarded to the spacecraft. At the spacecraft, the DTN bundles can be extracted and forwarded on to the next appropriate bundle agent (here, the moon).

Figure 2 is similar to Figure 1 in that it illustrates a scenario where a DTN node is at Mission Operations and the next hop DTN node is on the spacecraft. However, here DTN bundle security replaces the secure datalink (albeit both can be utilized). Again, we assume that encryption is required and that a third party ground station is used. Here, the "bundles" are secured between Mission Operations and the appropriate endpoint – be it the spacecraft of the lunar node. The encrypted bundles pass through the Space Link Extension – Transfer Services Application and an application-layer tunnel and control loop are established. The data is forwarded from Mission Operations to the appropriate ground station via a secure IPsec tunnel which has been established between the Mission Operations and ground station firewalls. At the ground station, the datalink data is extracted from the SLE-TS tunnel and forwarded to the spacecraft. At the spacecraft, the DTN bundles can be extracted from the datalink stream and forwarded on to the next appropriate bundle agent.

3 For extremely high-rate downlink data, an additional bitstream multiplexer (not shown in figure 1) may be required at each receiving ground station to multiplex and time-stamp the encrypted downlink bitstream prior to sending back to Mission Operations. This can become quite expensive as such equipment has to be duplicated at each receiving ground station. In addition, it makes international interoperability problematic due to concerns of sharing cryptographic related technology.

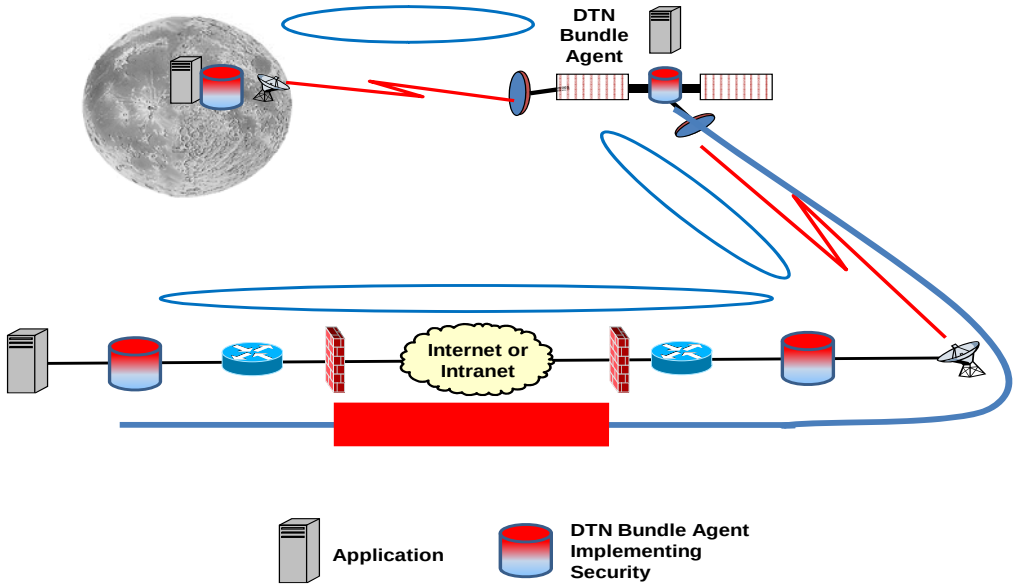

Figure 3 – Secure DTN without the need for SLE-Transfer Services

In figure 3 a DTN bundle agent is placed at each ground station. Since communication is hop-by-hop, there is no need to extend the space-link. Thus, the SLE-Transport Service Application gateways can be removed. Furthermore, the links can be optimized between each bundle node via the proper choice of convergence layers. For example, instead of running LTP between the lunar relay satellite and Mission Operations and one might have to do for scenarios 1 and 2, one can run TCP convergence layer between Mission Operations and the ground station and LTP between the ground station and the relay, thereby optimizing the transport protocol for each DTN link.

Two important items to note from the three scenarios:

(1) The complexity of the architecture goes down dramatically if one is willing to allow DTN to handle the security. Simplifying architecture allows one to better understand and address weaknesses in the network and results in less areas that can be exploited and a more secure system.

(2) The number of control loops is dramatically reduced. Each security mechanism has to be able to function within the characteristics of the underlying transport protocol and tunneling mechanism and each transport protocol has to be able to handle the idiosyncrasies of the embedded control loops. The interactions between transport protocols and security mechanism can be quite subtle. Thus, reducing the number of encapsulations is highly beneficial.

6. CONTACT GRAPH ROUTING AND SECURITY

Contact graph routing (CGR) is a method for routing that applies to scheduled networks such as a space backbone. CGR is currently the routing method of choice for the space backbone. For space-based networks, CGR requires contact start/stop times and data rates, together with the distances [in light seconds] between the nodes. For the communication paths to physically exist, the antenna systems must be pointed accordingly and all modulation and coding must also match on both ends of the communication link. If CGR is to be used between systems owned and operated by different organizations (e.g. NASA, ESA and JAXA) then the contact information, orbital information, modulation and coding must be shared. Thus, a reasonably strong trust relationship is required between organizations – almost to the point where the network looks like a closed network, open only to trusted parties.

Currently, a specific routing protocol has not been developed to distribute the information that is required to configure contact graph routing. Furthermore, this information is likely to be sourced from a central location such as a Mission Operations or network control center, not from the next neighbor. Such information is likely to be delivered over the network management system.

The bundle security protocol (BSP), Bundle Authentication Block (BAB) is used to thwart DOS and to ensure routing information exchange between "neighboring" DTN nodes is authenticated. However, with the pre-established trust relationship required for CGR, there appears to be little need to implement the BAB in a space-backbone running CGR as it adds overhead and processing while providing little or no additional protection.

On the other hand, routing information for CGR will likely be sourced from a DTN node many hops away. In order to validate such information, one could utilize the Payload Integrity Block (PIB) or application-layer security. Furthermore, if one wishes to hide routing information residing in the payload, one could utilize the Payload Confidentiality Block (PCB).

7. NETWORK MANAGEMENT

Network Management consists of configuring bundle agents and monitoring network performance in order to both optimize performance and determine when something has failed either entirely or partially.

Network management can be performed out-of-channel for some DTNs. However, out-of-channel network management requires a direct link to the bundle agent and is therefore limiting. For multi-hop DTNs where some bundle agents are only reachable via DTN technology, DTN protocols will be required to perform network management.

Configurations may include the following: distribution of contact graph routing information, configuration of radios (e.g. modulation, coding, data rates), security policy, security keys, and reporting. If the network management system were compromised, it could lead to serious performance issues relative to the entire DTN network – even if only a single critical node where compromised.

8. IRTF DTN SECURITY PROTOCOLS

The following section addresses security issues related to specific RFC and internet drafts.

As of November 2009, there are currently two documents specifically related to DTN security (e.g. the DTN Security Overview and the Bundle Security Protocol) and one additional document that utilizes the Bundle Security Protocol (Reliability-only Ciphersuites for the Bundle Protocol). There is one additional document specifying Bundle-in-Bundle Encapsulation that will likely be used in conjunction with the Bundle Security protocol to perform secure tunneling – the equivalent of “tunnel mode” in IP security. RFC 5050 and the DTN URI Scheme have some security related issues although they do not specify security protocols.

Bundling Protocol RFC 5050

The Bundle Protocol, RFC 5050, requires that all communicating bundle nodes share a common, simultaneous, synchronized, conception of Universal Time Coordinated (UTC). When a bundle is generated, an “absolute” creation time is included in the header. This creation time is user as a time to live counter to keep bundle from continuously looping in a network and to allow bundle to expire and be removed from the network. In addition, this timestamp is used to uniquely identify the bundle.

For network-centric operations involving diverse organizations, it may not be possible from a security standpoint to accept time reference data from nodes operated by a different organization, even though data communications with that organization are deemed acceptable [7].

Because this timestamp is absolute time, it may be possible to cause inadvertent or intentional problems in the network by sending improper timestamps such as to make bundles look like they came from the future. Of course, if your system is not properly synchronized you may be living in the past and the bundles are actually OK. This is likely a network policy configuration option to determine what to do with such a bundle.

One can also send legitimate, extremely long-lived bundles that may not have a legitimate destination. This could quickly consume system resources (storage). What one does with such bundles is a local or organizational policy issue. Implementations should be able to react to such policy.

The DTN Universal Resource Identifier Scheme

The DTN Universal Resource Identifier (URI) Scheme, draft-irtf-dtnrg-dtn-uri-scheme-xx, represents early thinking on this naming syntax. The scheme described is very likely to change in many respects as additional input is received from the Internet community. In general, the proposed scheme-specific part (SSP) of a "dtn" URI is comprised of one or more dtn URI elements, each of which comprises an optional operation name followed by a URI. The operational name enables flexibility to the point of perhaps actually specifying code to be run. The proposed opnames identified in this document (e.g. next, push, pop, flood, exec) are purely notional at this point.

“DTN URIs whose URI elements lack operation names or are confined to operation names "push" and "next" raise no security considerations beyond those addressed in RFC 5050.

The "pop" operation could be used to circumvent firewall rules that accept Bundle Protocol traffic but reject traffic destined for endpoints of the popped Internet application protocol.

Attacks built on the "flood" operation could exploit the possible side effects of evaluating selection expressions.

Attacks built on the "exec" operation could modify bundle node state in a limitless variety of ways.

Bundle protocol implementations that support these more dangerous operations will need to exercise extreme care [7].”

Delay-Tolerant Networking Security Overview

The "Delay-Tolerant Networking Security Overview", draft-irtf-dtnrg-sec-overview-xx, provides an overview of the security requirements and mechanisms considered for delay tolerant networking security for general DTNs. It discusses the options for protecting such networks and describes reasons why specific security mechanisms were (or were not) chosen for the relevant protocols. The entire document is informative, given its purpose is mainly to document design decisions. Many of the threats identified in the DTN Security Overview document can be mitigated in space-based backbones. Most have been address in the preceding "Threats" section, section 3.

One of the most critical threats for space-base DTNs is unauthorized use of resources – particularly storage and battery power.

This document includes a good explanation of policy-based routing. "It is a requirement that DTN protocols and implementations support mechanisms for policy-based routing. In other words each DTN protocol specpolification should state the security-relevant policy variables upon which routing and forwarding decisions can be made. . . . In particular, since forwarding even a single bundle will consume some network resources, every DTN node must implicitly incorporate some element of policy-based routing [8]."

Bundle Security Protocol Specification

The "Bundle Security Protocol Specification", draft-irtf-dtnrg-bundle-security-xx, defines the bundle security protocol, which provides data integrity and confidentiality services. Note, this is a very complex document and has gone through a number of revisions. The latest have been related to adding multi-layer security to meta-data blocks [9].

There are four basic security blocks: the bundle authentication block (BAB), the Payload Integrity Block (PIB), the Payload Confidentiality Block (PCB) and the Extensions Security Block (ESB).

Bundle Authentication Block

The bundle authentication block (BAB) is used to assure the authenticity and integrity of the bundle along a single hop from forwarder to intermediate receiver. The BAB protects a bundle on a "hop-by-hop" basis while other security blocks may provide protection over several hops or end-to-end. Thus, whenever both are present the BAB must form the "outer" layer of protection.

Currently (as of November 2009) only a share-key Hash Message Authentication Code (HMAC) is defined for the BAB, HMAC-SHA1. This ciphersuite could be used for group keying. The key is not required to be one-to-one unique, just shared between the nodes that need it. If it is one-to-one unique then it can serve as additional validation of the node, but that's not required for bundle authentication.

Note, there is no requirement to do bundle authentication using HMAC. One could create a new ciphersuite and define it to use a different keying scheme. For example, one could use an ephemeral key for HMACing and then encrypt that with the public key of the intended recipient. Only the recipient can decrypt the key and then verify the bundle. One could also establish short-term shared keys for HMAC-SHA1 similar to a session key in IPsec. However, exactly how to do that is not addressed in any current specification – that is, key management and distribution is yet to be defined.

Payload Integrity Block

"The Payload Integrity Block (PIB) is used to assure the authenticity and integrity of the payload from the PIB security-source, which creates the PIB, to the PIB security-destination, which verifies the PIB authenticator. The authentication information in the PIB may (if the ciphersuite allows) be verified by any node in between the PIB security-source and the PIB security-destination that has access to the cryptographic keys and revocation status information required to do so."

The PIB may be of greatest use in space-based networks as operationally one may not care what the previous hop source's unique identity is (that is probably known or implied via scheduling information). Rather, one needs to know if the bundle originates from a trusted community as this is likely to be the filter for policy-based routing. Policy may state that one is willing to store and forward bundles from various communities, but not from others.

For contact graph routing, where distribution of contract graph information originates from a central source, the Payload Integrity Block (and perhaps the payload confidentiality block) are the proper security mechanisms to use if security is to be performed at the bundle layer.

Payload Confidentiality Block

"The Payload Confidentiality Block (PCB) indicates that the payload has been encrypted, in whole or in part, at the PCB security-source in order to protect the bundle content while in transit to the PCB security-destination.

It is STRONGLY RECOMMENDED that a data integrity mechanism be used in conjunction with confidentiality, and that encryption-only ciphersuites NOT be used."

Extensions Security Block

"The Extension security block (ESB) provides protection for non-payload-related portions of a bundle. They MUST NOT be used for the primary block or payload, including payload-related security blocks (PIBs and PCBs). . . .

The ESB is placed in the bundle in the same position as the block being protected. That is, the entire original block is processed (encrypted etc) and encapsulated in a "replacing" ESB-type block, and this appears in the bundle at the same sequential position as the original block. The processed data is placed in the security-result field."

The ESB is likely to be used to protect Meta-data blocks. Meta-data blocks are described in the internet draft entitle "Delay-Tolerant Networking Metadata Extension Block." [10] The Metadata Extension Block is designed to be used to carry application-level information that DTN nodes can use to make DTN-level processing decisions regarding bundles, such as deciding whether to store a bundle or determining to which nodes to forward a bundle.

General Notes Concerning the Bundle Security Protocols—PIB and PCB protect the payload and are regarded as "payload-related". Other blocks are regarded as "non-payload" blocks.

The ESB provides security for non-payload blocks in a bundle. ESB therefore is not applied to PIB or PCBs, and of course is not appropriate for either the payload block or primary block.

Bundles protected using PCB must be processed in order. Great care must be taken to ensure that security zones do not overlap. One may have nested security zones (DTN tunneling), but one may not have overlapping security zones. A detailed discussion on security zones is provided in the bundle security specification [9].

The Defense Advanced Research Projects Agency (DARPA) has a significant research effort in DTN directed toward military applications. Much of the complexities of the security protocol appear to be related to the potential to utilize DTN bundling as a method to perform secure content storage and delivery which is applicable to content-base routing or content-based distribution. Items continue to be developed and added to the bundle specification such as meta-data blocks and the corresponding Extension Security Block. Indications are that these items can be combined to enable a type of multi-layer security for content storage, discovery and distribution.

Implementing security with fragmentation is quite complex. Implementing reactive fragmentation is often not possible depending on the security policies and ciphersuites used. Thus, it is highly recommended that one avoid fragmentation if at all possible. A detailed discussion is provided in the bundle security specification [9].

DTN Bundle-in-Bundle Encapsulation

The Delay-Tolerant Networking Bundle-in-Bundle Encapsulation draft, draft-irtf-dtnrg-bundle-encapsulation-xx, defines an encapsulation-specific application agent capability and a bundle payload format for use with the Bundle Protocol. It defines the capability and format for placing one or more bundles inside of the payload field of an encapsulating bundle's Bundle Payload Block [11].

Bundle-in-Bundle encapsulation can be used for security purposes. One or more bundles can be placed inside of the payload of another bundle and then the payload of the encapsulating bundle can be encrypted. The encapsulating bundle is then sent from the encapsulating security gateway to the de-encapsulating security gateway forming a security tunnel. This security tunnel protects the entire contents of the encapsulated bundle(s) from being disclosed, so that even the confidentiality of each bundle's source EID and destination EID are maintained on the portion of the network that is spanned by the tunnel. One may anticipate that this technique will be applied in a similar manner to IPsec tunnel-mode to effectively hide traffic from one DTN network inside another.

Reliability-only Ciphersuites for the Bundle Protocol

The Reliability-only Ciphersuites for the Bundle Protocol, draft-irtf-dtnrg-bundle-checksum-05, defines new ciphersuites for use within the existing Bundle Security Protocol's Payload Integrity Block to provide error-detection functions. The reliability ciphersuites do not require support for other, more complex, security-providing ciphersuites that protect integrity against deliberate modifications. This creates the checksum service needed for error-free reliability, and does so by separating security concerns from the few new reliability-only ciphersuite definitions. The reliability-only ciphersuites are intended to protect only against errors and accidental modification; not against deliberate integrity violations.

"The Delay-Tolerant Networking Bundle Protocol includes a custody transfer mechanism to provide acknowledgements of receipt for particular bundles. However, no checksum is included in the basic DTN Bundle Protocol. Therefore, at intermediate hops, it is not possible to verify that bundles have been either forwarded or passed through convergence layers without error. Without assurance that a bundle has been received without errors, the custody transfer receipt cannot guarantee that a correct copy of the bundle has been transferred, and errored bundles are forwarded when the destination cannot use the errored content, and discarding the errored bundle early would have been better for performance and throughput reasons. The reliability-only ciphersuites provide the checksum function required to alleviate this problem [12]."

There are two negatives regarding using the BSP to implement checksums. The first is that the complex bundle security protocol must be implemented by all nodes wishing to perform reliability checks. This may be a rather extreme processing requirement for a low-end DTN node such as simple sensor webs. The second is purely a human factors issue. One may be implementing reliability and believe that

they are also secure because they are implementing a portion of the security specification.

9. OPERATIONS CONSIDERATIONS

There are four basic security tools currently developed for DTN bundle security, all are defined in the Bundle Security Protocol document. These are: authentication of neighbors (BAB), integrity (PIB), confidentiality of the payload (PCB) and confidentiality of other bundles such as meta-data (ESB).

For space-based DTNs which are highly scheduled such that contact times, modulation, coding, media access, antenna pointing , etcetera are know, the usefulness of the BAB is questionable as there is already a strong trust relationship in order to establish communication at the physical layer. The added complexity, added key distribution and management and potential for lockout versus the risk of not authenticating you neighbor must be considered. Furthermore, if one is operating across organizational domains, a shared key (HMAC) is probably not acceptable. Rather, asymmetric keys based on certificates are likely to be acceptable as this is easier to control and validate across organizational boundaries.

One will likely have security policies in place that control and limit the use of system resources. This policy should require one to identify the source of data and determine what organization that source belongs to. The PIB would likely be used here. If the keys are certificate-based, one could validate the certificate against an organizational certificate that has been cross certified thereby identifying the source as belonging to a particular organization. For DTNs this requires cross-organizational certification of signing certificates and sharing of public certificates. Certificates would also have to be cached locally as one must assume that the DTN Bundle Agent cannot reach a certificate server and revocation list in a timely manner except for DTN where the 'D' implies short term disruption, a very specific case of DTN.

Common practice today is that the network is run by one group and the applications are run by another. For example, in NASA Mission Operations does not run the ground infrastructure or radio and ground stations. That is the responsibility of the Space Communication and Navigation (SCaN) Program, the IP Operation Network (IONET) group, the Space Network group and the Deep Space Network group. Mission Operations is responsible for the spacecraft control and the applications. The management of security of the mission systems and the communication infrastructure is currently separate and likely to continue – particularly if one considers tying communication networks together with international partners. Thus, one should anticipate the key and policy management of applications will be performed and controlled by a different group than that which controls key and policy for the communication network.

An example of Mission Operations managing application security can be seen in the NASA Constellation program. Here, the Constellation Communication Framework structure has a security element very similar to bundling to enable authentication, integrity and confidentiality. Here, authentication may be used to authenticate commands and confidentiality may be utilized to encrypt crew medical data. This application layer security most certainly is managed by Mission Operations, not by network security.

From the above observations, for space-based networks or any DTN network, encrypting bundles is probably only useful for bundles related to networking and not bundle related to application. The application data should be protected by those responsible for the applications. Such an approach should make security management easier. Applications are protected end-to-end whereas the network is protected at all points of the communication chain using a variety of tools. This may be contrary to what DARPA is considering where they mix Bundle Security, a network layer, with secure content storage, distribution and delivery, an application.

One area that needs special consideration regarding encryptions is DTN network management. Who will control this security layer is not clear. Network Management is an application, but it is also likely to be managed by the communication network group. Thus, it may be appropriate to allow bundle security to be used to protect the network management application data.

The need to protect metadata versus the complexity of key and policy management is and open issue for space-based networks as is how one might use meta-data blocks for space-based applications.

10. ACKNOWLEDGEMENTS

The author wishes to thank the many people who have responded to questions via direct conversation of via DTN email lists to clarify documents and concepts and provided feedback on the draft of this paper.

The information regarding the Internet Request for Comments of the Internet Drafts has been summarized, paraphrased or, in some cases, taken verbatim. In such cases, an attempt was made to quote that information. The authors and research community responsible for these documents are commended for the time and effort taken to develop and document their work.

REFERENCES

[1] V. Cerf et al., "Delay-Tolerant Network Architecture," IETF RFC 4838, informational, April 2007.

[2] CCSDS File Delivery Protocol (CFDP), Consultative Committee for Space Data Systems Blue Book, Issue 4, January 2007.

[3] S. Scott Burleigh, Licklider Transmission Protocol (LTP): An Overview, IETF 69 Transport Area Meeting, July 2007, http://www.ietf.org/proceedings/69/slides/tsvarea-0/sld1.htm

[4] K. Scott and S. Burleigh, "Bundle Protocol Specification," IETF RFC5050, experimental, November 2007

[5] Space Link Extension—Application Program Interface for Transfer Services—Summary of Concept and Rationale. Green Book. Issue 1. January 2006. CCSDS 914.1-G-1

[6] S. Farrell, M. Ramadas: "Licklider Transmission Protocol - Security Extensions," RFC 5327, Category: Experimental, September 2008

[7] L. Wood, W. Eddy, P. Holiday: "A Bundle of Problems," IEEE Aerospace conference, Big Sky, Montana, March 2009.

[8] K. Fall, S. Burleigh, A. Doria, J. Ott, D. Young: "The DTN URI Scheme," draft-irtf-dtnrg-dtn-uri-scheme-00, Expired: September 29, 2009, work-may-be-in-progress

[9] S. Farrell, S.F. Symington, H. Weiss, P. Lovell: "Delay-Tolerant Networking Security Overview," draft-irtf-dtnrg-sec-overview-06, Expired: September 9, 2009, work-may-be-in-progress

[10] Symington, S., Farrell, S., Weiss, H., and P. Lovell: "Bundle Security Protocol Specification", draft-irtf-dtnrg-bundle-security-09.txt, October 2009, work-in-progress

[11] S. Symington: "Delay-Tolerant Networking Metadata Extension Block,"draft-irtf-dtnrg-bundle-metadata-block-04, Expires: April 11, 2010, work-in-progress

[11] S. Symington R. Durst K. Scott: "Delay-Tolerant Networking Bundle-in-Bundle Encapsulation," draft-irtf-dtnrg-bundle-encapsulation-06, Experimental, Expires: February 13, 2010 , work-in-progress

[12] W. Eddy, L. Wood, W. Ivancic: "Reliability-only Ciphersuites for the Bundle Protocol," draft-irtf-dtnrg-bundle-checksum-06, experimental, Expires: April 28, 2010, work-in-progress

BIOGRAPHY

William Ivancic has over twenty-five years of experience in network and system engineering for communication applications, communication networking research, state-of-the-art digital, analog and RF hardware design and testing. He currently is a senior research engineer at NASA's Glenn Research Center where he directs the hybrid satellite/terrestrial networking, space-based Internet, and aeronautical Internet research. He has lead research efforts to deploy commercial-off-the-shelf (COTS) technology into NASA missions including the International Space Station and Shuttle. Mr. Ivancic has recently performing research on advance routing research for space-based and aeronautic-based networks. Of particular interest is large scale, secure deployment of mobile networks including mobile-ip and mobile router technology.

Mr. Ivancic is also principle of Syzygy Engineering, a small consulting company specializing in communications systems and networking as well as advanced technology risk assessment. Mr. Ivancic is currently performing research and development on Identity-based security and key and policy management and distribution for tactical networks - particularly mobile networks.