DELAY TOLERANT NETWORK (DTN) SECURITY

by

Mohaymen Aljarrah
A Thesis
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
The Requirements for the Degree
of
Master of Science
Information Security & Assurance

Committee:

Duminda Wijesekera ____ Dr. Duminda Wijesekera, Thesis Director

____ Dr. Angelos Stavrou, Committee Member

____ Dr. Paulo Costa, Committee Member

Sanjeev Setia ____ Dr. Sanjeev Setia, Department Chair

Kenneth S Ball ____ Dr. Kenneth S. Ball, Dean, Volgenau School of Engineering

Date: ____ Summer Semester 2014
George Mason University
Fairfax, VA

Delay Tolerant Network (DTN) Security

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at George Mason University

by

Mohaymen Aljarrah
Master of Business Administration
Georgetown University, 2009
Bachelor of Arts
George Washington University, 2004

Director: Duminda Wijesekera, Professor
Department of Computer Science Department at The Volgenau School of Information Technology and Engineering, George Mason University

Summer Semester 2014
George Mason University
Fairfax, VA

Dedication

This is dedicated to my grandmother Lutfia Jarrah, her constant love have sustained me throughout my youth and the rest of my life.

Acknowledgments

I am most appreciative to the members of my ISA committee, Dr. Duminda in particular for his time, inspiration, and proficiency throughout this project.

I could not have done this project without my wife Hiba Jarrah and my precious daughter Sarah Lutfia support and encouragement. Thank you both for your love and support.

Table of Contents

Page

List of Figures

List of Abbreviations and Acronyms

FAT	-	Fragment Authentication Tree
DTN	-	Delay Tolerant Network
TCP	-	Transport Control Protocol
PKI	-	Public Key Infrastructure
CRL	-	Certificate Revocation List
DOS	-	Denial of Service
PCB	-	Payload Confidentiality Block
BAB	-	Bundle Authentication Block
PIB	-	Payload Integrity Block
MAC	-	Media Authentication Code
OBBA	-	Opportunistic Batch Bundle Authentication

Abstract

Delay Tolerant Network (DTN) Security

Mohaymen Aljarrah, M.S.

George Mason University, 2014

Thesis Director: Dr. Duminda Wijesekera

DTNs (Delay Tolerant Networks) or opportunistic networks represent a class of networks in which a continuous end-to-end connectivity in the network may not be quite possible.

Because DTN is a well-recognized networking concept, it has attracted extensive attentions from both the system designers and also application developers.

Security is a major barrier to wide-scale deployment of the DTNs, though it has gained little attention so far. Just like traditional mobile ad hoc networks, the multi-hop transmission and open channel have made DTNs vulnerable to security threats, such as unauthorized access message modification or injection attack. The security characteristics of DTNs include frequent disconnectivity, long round-trip delay, opportunistic routing, fragmentation, as well as limited storage capability and computational delays; make the existing security protocols unsuitable for DTNs. Thus, new security protocols should be implemented; that are stringent and efficient in securing DTNs.

Chapter 1

1.1 Introduction

Delay Tolerant Networking (DTN) is considered an overlay network that is on top of the regional networks. It has a new layer not common with other internet protocol layers called the bundle layer. It is located on top of the Transport layer (TCP). Below is a figure showing the difference between DTN and other internet protocol layers.

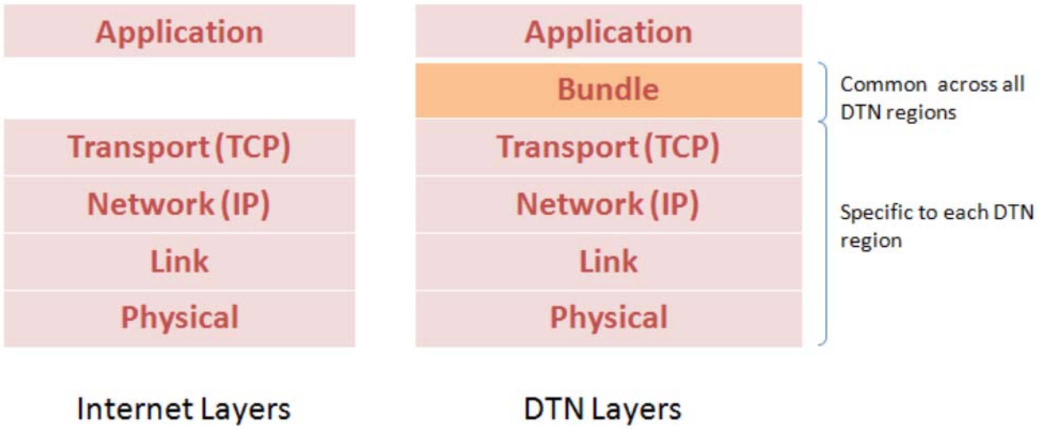


Figure 1: Comparison of DTN and other Internet Protocol Layers

Several protocols have changed to the latest internet protocol suite that supports the DTN architecture. Unlike in the Transmission Control Protocol (TCP) where the communication is end-to-end, DTN uses a store and then forward approach. Here the data is first stored then moved incrementally in the network, hoping that the data will reach its destination. Another way is to send a message over and over hoping that one of the messages will arrive at the destination. Here more bandwidth and local storage is required (Ferrara A. L.). DTN primarily stands for delay in the network. This delay can be of the following three major kinds: delay in propagation through a medium, delay in queuing within the relay points, destination and source; and finally, clocking delays that are associated with the transmitting onto the medium, of an atomic unit of data. The propagation delays experienced over the medium might be long and are caused by speed-to-light delays to cross long distances (e.g., underwater, space). On the other hand, traffic and service rate are affected by queuing delays that are within the relay points. The clocking delays occur when erroneous data is received, though not recognized and resent until when all the right data is received. Vast ranges of environments are covered in DTN researches. Each of the particular entities in these environments has their own features and characteristics. For example, each hub or node in the space network may have a difference in their resource capabilities that govern the way they transmit mostly among each other. They also have to have a balance in the way they conduct their different functions – a mars rover meant to collect samples in the red sandstorm, might not be in a position to relay their findings during that season. Moreover, it is known beforehand the time when the two transmitting entities remain in transmitting sight and for how long they can transmit. In such a case, the transmission might be scheduled beforehand. In other examples like the infamous vehicular DTN (underwater environments), this might not apply. Therefore, the DTN protocol is often application specific (Ferrara A. L.).

DTN has now gone a step further into a new technology of having interplanetary internet that will have the capability of improving the communication by acting by storing data whenever a connection is interrupted in any way. In this technology, after the storage, the data will be transferred to their destination by the use of nodes or relays station. Thus, the main function of the DTN network will be to provide a guaranteed and reliable delivery services.

Security, which is a very important key aspect of reliable internet protocol, is a major concern with the DTN protocol. They are specifically concerned with the authentication, date authenticity, the environment and finally attacks.

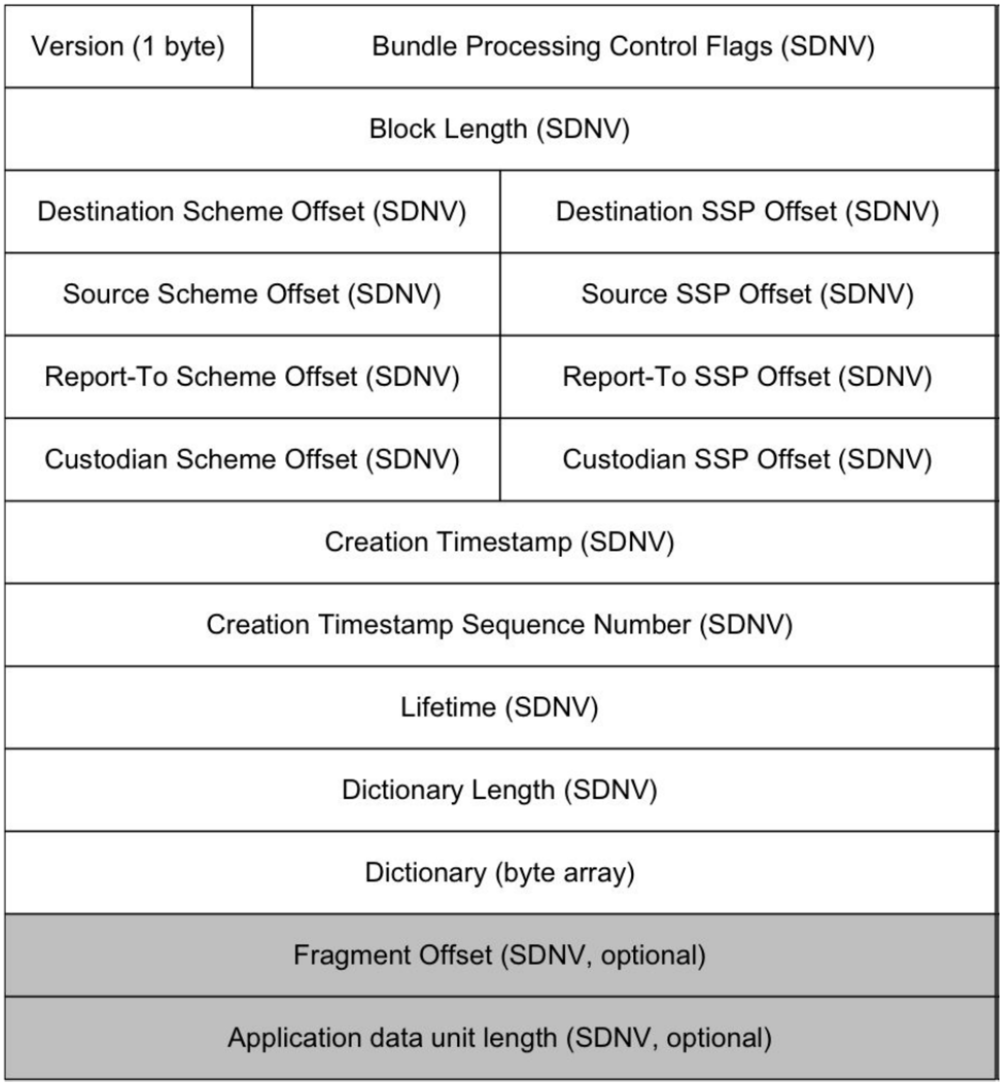
DTN PDUs: BUNDLES

In the DTN architecture, applications operate on messages carried in variable length protocol PDUs called bundles. This name bundle is derived from the consideration of the protocols that attempt to minimize the actual number of round trip exchanges that are necessary to for the completion of a protocol transaction. These date back to the original IPN work. The number of exchanges is reduced when all the information to be communicated is bundled together which in turn gets to be considerable interest in the round trip time is hours, weeks or days.

Bundles are comprised of a collection of typed blocks. Each of these blocks contains meta-data; others also contain application data. For much of the DTN architecture and bundle protocol evolution, meta-data blocks were simply called headers, but after it became real that the bundle security protocol required the ability to attach meta-data to a bundle, the term block was adopted. Just like the extension headers in the IPv6, blocks are chained together.

a) Blocks

The primary (first) block of each bundle illustrated in figure 2 contains the DTN equivalents of the data typically found in the IP header on the internet: version, destination EIDs, length, version, fragmentation information (optional) and source. It also contains some additional fields, more specific to the bundle protocol: report-to EID, current custodian EID, creation timestamp and sequence number, lifetime and a *dictionary*.



Version (1 byte)	Bundle Processing Control Flags (SDNV)
Block Length (SDNV)	
Destination Scheme Offset (SDNV)	Destination SSP Offset (SDNV)
Source Scheme Offset (SDNV)	Source SSP Offset (SDNV)
Report-To Scheme Offset (SDNV)	Report-To SSP Offset (SDNV)
Custodian Scheme Offset (SDNV)	Custodian SSP Offset (SDNV)
Creation Timestamp (SDNV)	
Creation Timestamp Sequence Number (SDNV)	
Lifetime (SDNV)	
Dictionary Length (SDNV)	
Dictionary (byte array)	
Fragment Offset (SDNV, optional)	
Application data unit length (SDNV, optional)	

Figure 2: Bundle architecture

b) Fragmentation

The bundle ability to be fragmented, either whilst in transmission or prior to the transmission, has been an ongoing point of interest since the original IPN. The motivation for bundle fragmentation is similar to that of IP fragmentation: to adapt to relatively large bundles for transport using message oriented protocols. The specific argument that was against fragmentation was because of the interaction of fragmentation with transfer of custody. The key issue in this case was whether the particular granularity of a custody transfer acknowledgement could express a partial bundle and if the fragments needed reassembly while in transit.

Early in the transition from IPN to DTN architecture, and upon the further understanding of the routing requirements, the need for fragmentation became undeniable. In particular it is very important to understand that the routing contact is not measured in terms of bandwidth but instead it is measured in terms of bytes (storage) units (the product of the time window and the bandwidth), a way was needed to divide large bundles into sizeable ones to fill contacts. It is because of this case that the term Proactive fragmentation was adopted. This proactive fragmentation is performed ahead of time and before contact of known duration and time becomes active in the network.

Supporting fragmentation in the basic bundle protocol is not unusually difficult. A special header is used that is similar to that of the IPv6 to describe the fragments offset and length relative to its original position in the bundle when it was first transmitted. As in the IP fragmentation, the bundle fragments are required to be reassembled at the final receiver(s). The custody acknowledgements are expanded to have the capability of describing partial bundles. Bundle fragments are said to have the same originality in a specific bundle by a common identifier comprising of a subset of the primary block (receiver, sender, origination timestamp).

The support of fragmentation in conjunction with encryption, applied along bundles delivery path is very challenging. When using typical cypher text bundle, encryption can expand the size of a clear text bundle when transformed. Fortunately, it is possible to avoid such cases by, for example, encrypting at the source and also using algorithmic alternatives that have equally strong security properties. Counter-mode encryption is an example of such (Dworkin M., 2007). Here the cleartext and cypher text versions of a bundle are of equal length, meaning that the related fragmentation information (length, byte range descriptions and offset) remain accurate whether or not bundles are encrypted.

1.2 Research on DTN Security

1.2.1 Motivations

DTNs are considered to be vulnerable to security threats. They also introduce a number of security challenges to the networking field. Particularly, when open networks are used in the transmission of data, they open up the network to multiple threats and attacks. For example, malicious routers in DTNs can easily insert unwanted and even false information into the messages. If the innocent routers then take up these wrong messages and send them, then large numbers of false and unwanted traffic are generated. As DTNs have scarce resources, the extra traffic may seriously affect the proper functioning of the

DTN (S. Farrell and V. Cahill). Unauthorized access to the DTN resources and their use are also a serious DTN security issue.

Research done on DTN security is more challenging compared to research on the conventional protocols. The unique features of the DTN include long round-trip delays, fragmentation as well as frequent discovery make the conventional protocol designs and architectures irrelevant in these cases. This, therefore, calls for there to be new security protocols in place.

The misbehaving nodes can be classified into two main classes: selfish and malicious. The main objective of malicious is to attract and disrupt the proper and functioning networks without particular self gain from the attack. The selfish nodes, on the other hand, maximize their own needs and gains or those of other nodes that are collaborating with them. Therefore, to ensure there is DTN security, we need to address the malicious and selfish network behavior, as well.

Last but not least, public key management that includes public key distribution issues, as well as revocation issues serves as the most important foundation of any worthy security protocol in any wireless network.

1.2.2 Contributions to DTN research

The basis of this thesis is to develop an understanding of the security constraints faced by DTN networks e.g. malicious nodes, selfish nodes etc. DTN security characteristics and issues.

I proposed an efficient scheme to authenticate bundles in batches. This will help thwart malicious attacks that the DTN networks face.

1.3 Thesis outline

This thesis is in the following order:

Chapter 2

DTN Security: Threat, Characteristics and Challenges Faced

DTN introduces a new networking concept that also brings with it new security challenges. In this chapter, I will discuss the security threats that DTNs face and also give solutions to securing a DTN. DTN security features are considered when discussing the difference between conventional and DTN networks. I will finally conclude the section with a statement of three research issues related to DTN security, which are these thesis study objectives.

2.1 DTN Security Threat

According to (S. Farrell, et al), possible security threats regarding the DTNs can be summarized as follows:

- Bundles (messages) modification: in DTNs, the bundles might traverse underlying heterogeneous networks.

- Unauthorized access: Unauthorized use and access to DTN resources can be very serious concern.

- Bundle interjection attack: Fake bundles might be injected by attackers to consume DTN resources. Because DTN cannot detect misbehavior and unplanned replays, they can be used to amplify resource consumption.

2.1.1 Flood Attack

Disruption Tolerant Networks (DTNs) consist of mobile nodes carried by human beings, vehicles, etc. DTNs enable data transfer when mobile nodes are only intermittently connected, making them appropriate for applications where no communication infrastructure is available. Due to the limitation in network resources such as contact opportunity and buffer space, DTNs are vulnerable to flood attacks. Rate limiting was proposed to defend against flood attacks in DTNs, such that each node has a limit over the number of packets that it can generate in each time interval and a limit over the number of replicas that it can generate for each packet. Here a detection adopted claim-carry-and check Packet Flood Detection To detect the attackers that violate their rate limit L, we must count the number of unique packets that each node as a source has generated and sent to the network in the current interval. The node itself count the number of unique packets that it, as a source, has sent out, and claim the up-to-date packet count (together with a little auxiliary information such as its ID and a timestamp) in each packet sent out. The nodes rate limit certificate is also attached to the packet, such that other nodes receiving the packet can learn its authorized rate limit L. If an attacker is flooding more packets than its rate limit, it has to dishonestly claim a count smaller than the real value in the flooded packet, since the real value is larger than its rate limit and thus a clear indicator of an attack. The claimed count must have been used before by the attacker in another claim, which is guaranteed by the pigeonhole principle, and these two claims are inconsistent. The nodes which have received packets from the attacker carry the claims included in those packets when they move around. When two of them contact, they check if there is any inconsistency between their collected claims. The attacker is detected when an inconsistency is found. Replica Flood Detection Claim-carry-and-check can also be used to detect the attacker that forwards a buffered packet more times than its limit l. Specifically, when the source node of a packet or an intermediate hop transmits the packet to its next hop, it claims a transmission count which means the number of times it has transmitted this packet (including the current transmission).

Based on if the node is the source or an intermediate node and which routing protocol is used, the next hop can know the node's limit l for the packet, and ensure that the claimed count is within the correct range. In the existing system, we can identify only the attackers who exceed the rate limit with the help of rate limit certificate. But if they send packet within the rate limit, they won't be identified in the Disruption Tolerant Networks .So as to identify that kind of attacks we are going to use key. If the original user sends packet less than rate limit value, then they have to generate the key with that packet count. So that key is transferred to each and every node along with the packets. At the receiver side Rate limit certificate and key will be checked. Based on the key, we can easily identify the attackers who sending unwanted packets within the rate limit. The key will be generated based on AES algorithm.

2.2 DTN Requirements

DTNs have four significant security requirements. These are confidentiality, integrity, anonymity and authentication.

2.2.1Authentication

Authentication techniques are used to verify the identity of the DTN nodes during communication and in the process help identify the legitimate DTN users from unauthorized users. In DTNs, it is paramount that intermediate nodes have the capability to verify that data was sent by an authorized node and at a legitimate rate too. Such authentication is provided on a hop-by-hop or the end-to-end basis. This is dependant on the different design goals for the security. Hence, authentication is a vital mechanism that serves to support access control.

2.2.2 Integrity

The integrity of data must be protected. Transmitted messages should not be altered during the propagation process. Message modification, falsification, replay attacks are as a result of lack of integrity protection.

2.2.3 Confidentiality

The purpose of confidentiality is to ensure only the persons we out to send a message to is the only receiving. This confidentiality can be achieved by using end-to-end encryption. The encryption requires that there be mutual authentication and agreement of the key between the destination and the source.

2.2.4 Privacy/Anonymity

The user’s location should neither be revealed by the network, nor the communicating party. The provision of identity and one’s place privacy is of much importance in particular scenarios. However, there is an exception. The Law enforcing agencies are allowed access to this crucial and private information.

2.3 DTN Security Characteristics

The specific DTN security characteristics are discussed in this section.

2.3.1Lack End-to-end Connectivity

The lack of end-to-end connectivity of the DTN network only brings about challenges to routing and also makes conventional network security solutions not admissible in DTN network. For example, traditional encryption mechanisms in end-to-end confidentiality require for there to be multiple round-key agreements between the receiver and the sender, in advance. These might not be feasible in DTN networks as there might be no network connectivity during the particular moment when the information is being sent (N. Asokan et al.).

Therefore, non-interactive one way key distribution is more suitable for the DTN networks. The same applies for the authentication. The non-interactive authentication scheme is more suitable in the DTNs than in conventional networks as the links are highly time-constrained (A. Kate et al.). The lack of end-to-end connectivity also serves to be a challenge to the revocation of the public key. PKI (Public Key Infrastructure), the most used certificate revocation scheme, functions through CRL (Certificate Revocation

List). A CRL is a list of the revoked certificates that are stored in a central repository. In DTNs, however, the nodes might suffer from delays or frequent loss of the connectivity to CRL servers. Therefore, it is preferred in DTNs that the public key is updated periodically and there be distributed CRL.

2.3.2 Fragmentation

Due to high mobility, the network links in DTNs become available only for short periods of time. Therefore if the information is large, the transmission might not occur just at once. The most possible solution to this is for the message to be split into fragments that can be sent over the network as bundles. The sending of the message can be over several links at the most convenient times when the communication is scheduled to take place.

As a result of fragmentation, the most used traditional authentication schemes might not work well. This is because the intermediate receiver usually doesn't have the full information thus cannot be able to verify the entire message. The 'toilet paper' approach was proposed to solve this in (mailman.dtnrg,org). The main idea here is to enable each fragment to self verifies by attaching a special signature at the very end of each fragment separately. This has a negative effect on the computation power of the relaying nodes as they have to spend much time trying to process an increasing number of signatures.

2.3.3 Resource Scarcity

Scarcity in the resources is another main concern in DTN security designs. Due to the limited contact time, nodes need to receive, check and finally, forward a large number of bundles in a limited time. On one hand, authentication and other security operations are regarded as being a necessity in the security of the DTN resources from any unauthorized use and access. Extra computation and overheads will then be presented automatically by the security mechanisms. Denial of service (DOS) opportunities might be presented to the attackers when there is much resource consumption.

2.4 Bundle Security Protocol Specification

Recently the DTNRG (DTN Resource Group) proposed an internet bundle security protocol specification (Farrell et al.) to provide integrity, data authentication and confidentiality services. The foundation of the DTN security research is the specification of the bundle security protocol. Here, I will briefly discuss on its major components and their corresponding functionalities.

2.4.1 Security Blocks

Here, three types of security blocks that are usually included in the bundle are defined by the ‘Bundle Security Protocol Specification’. The Payload Integrity Block (PIB), Payload Confidentiality Block (PCB) and the Bundle Authentication Block (BAB), are used to provide authentication, confidentiality and integrity functionalities. These security blocks are introduced briefly in the next section.

2.4.2 Bundle Authentication Block

This block ensures integrity and authenticity from the forwarder to the intermediate receiver of the bundle along a single hop. BAB is computed at every sending bundle agent and also checked at every receiving bundle agent along the way. This is done from the source all the way to the destination on every hop. This is shown in figure 2.1 below.

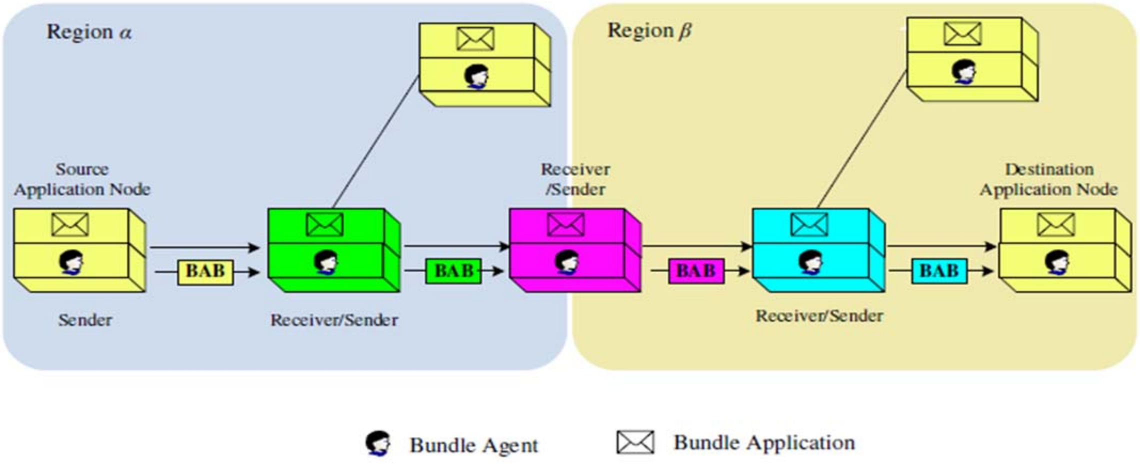


Figure 3: Hop by Hop Authentication

2.4.3 Payload Integrity Block (PIB)

This is used to ensure that the integrity and authenticity of the bundle from the PIB security-source to the PIB security destination are maintained. There are typically two operational modes for the PIB that includes the end-to-end mode and the hop-by-hop mode. As a BAB protects a bundle on a ‘hop-to-hop’ basis, the PAB protects the bundle on an ‘end-to-end’ basis. Its MAC can be verified by any node between the PIB’s security-source and also the PIB’s security-destination. These have access to

Cryptographic keys and revocation status information required to do so.

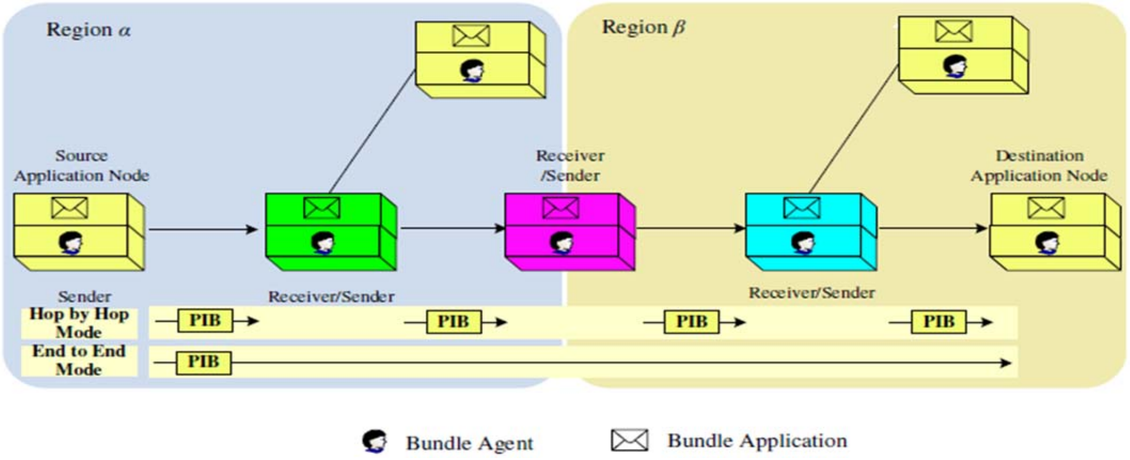


Figure 4: Two Operation Mode for Bundle Integrity Block

2.5 Basic Bundle Protocol Block Formats

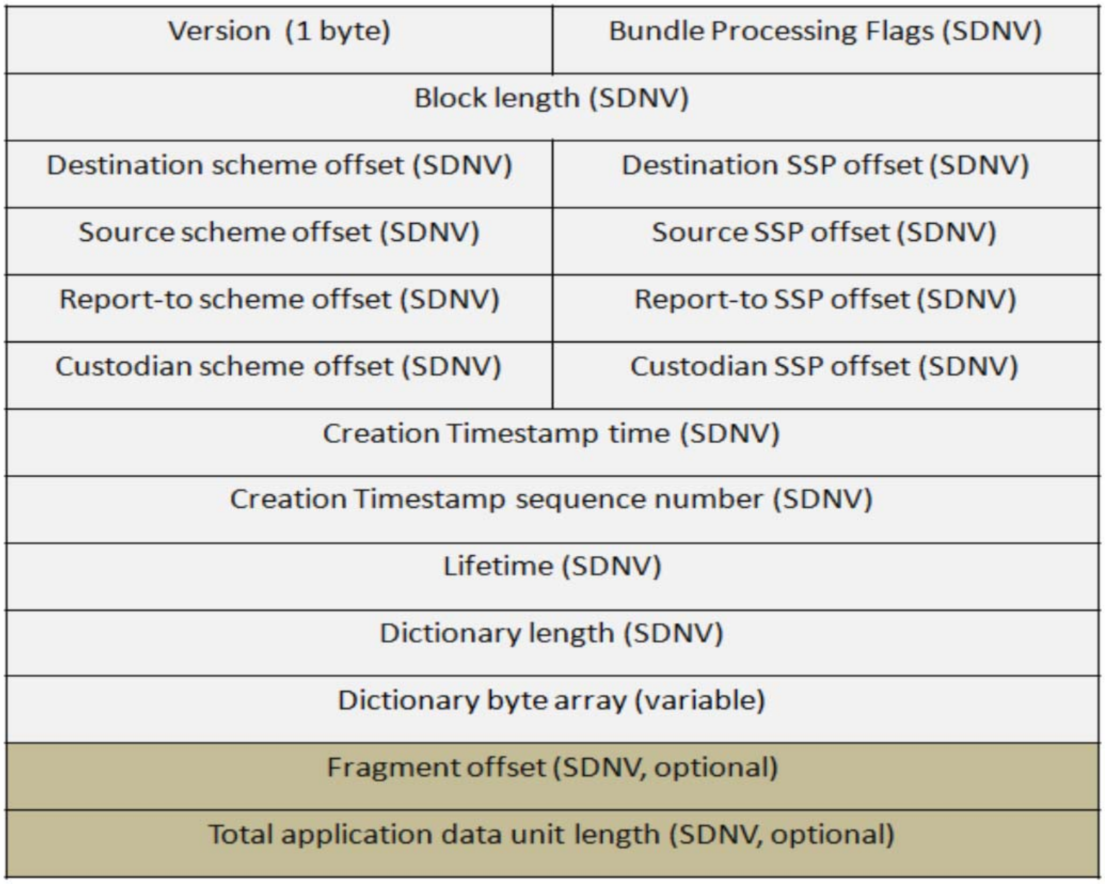
The major functions of the protocol are as summarized below and stated in (K. Scott and S. Burleigh, 2007).

- Retransmission based o custody
- Is able to cope and work with intermittent connectivity
- Able to take advantage of predicted, scheduled, and opportunistic connectivity
- Late binding of the overlay network identifiers (end point) to constituent the Internet addresses.

In this section we introduce the terms associated with the Bundle Protocol mechanism. More information about DTN based space protocols can be found in (NASA, 2010). The Bundle Protocol uses the ‘native’ Internet protocols (not necessarily TCP/IP) to communicate within the Internet. The Convergence Layer Adapter (CLA) forms an interface between the Bundle Protocol and a common internetwork protocol and it offers important functions to the Bundle Protocol Agent (BPA) – a part of the node that provides Bundle Protocol services. More about the CLA services is mentioned in (K. Scott and S. Burleigh, 2007). A bundle node is the one that sends or receives data. It can be a thread running on the system, an object in an object oriented programming environment or may be a special purpose hardware device. The bundle endpoint is a group of such bundle nodes that can offer Bundle Protocol functionalities and they identify them selves with a single string called as the “bundle endpoint id”.

The bundle endpoint can be a single node or a single bundle node can also be a part of many endpoints. Whenever a bundle node decides to forward a bundle it does so and marks the destination as the bundle endpoint. The Bundle Protocol data unit is referred to as a “bundle” and it contains at least 2 or more blocks of protocol data. The first one is called the primary bundle block and it may be followed by sequence of Bundle Protocol blocks that can be used to support Bundle Protocol extensions such as the Bundle Security Protocol (BSP) (S. Symington et al., 2011). Among them there must be at most one block that acts as the payload block. The ending block in the sequence must have the “last block” field set to 1, which will indicate it as the last block.

The Bundle Protocol tries to use as minimum bandwidth as possible while transmission. This has been accomplished with the help of Self-Delimiting Numeric Values (SDNV) encoding technique. In this technique any positive numeric value is encoded into N octets, the Most Significant Bit (MSB) of the last octet is set to 0 while all the other octets have their MSBs as 1. The other 7 bits of every octet contain relevant information. Figure 1 below shows the basic bundle protocol format.



Version (1 byte)	Bundle Processing Flags (SDNV)
Block length (SDNV)	
Destination scheme offset (SDNV)	Destination SSP offset (SDNV)
Source scheme offset (SDNV)	Source SSP offset (SDNV)
Report-to scheme offset (SDNV)	Report-to SSP offset (SDNV)
Custodian scheme offset (SDNV)	Custodian SSP offset (SDNV)
Creation Timestamp time (SDNV)	
Creation Timestamp sequence number (SDNV)	
Lifetime (SDNV)	
Dictionary length (SDNV)	
Dictionary byte array (variable)	
Fragment offset (SDNV, optional)	
Total application data unit length (SDNV, optional)	

Figure 5: Basic Bundle Protocol Block Formats

2.6 Summary

We discussed the threats that DTNs face, their requirements and also characteristic of the DTN security. We also did a review on the bundle security specifications which happen to be DTNs primary security solution. In the following chapter, we discuss two security challenges for the DTN networks.

Chapter 3

Schemes

Opportunistic BBA Scheme for DTNs

In this particular chapter, we will discuss the bundle authentication issue. Although an effort has put, the design of the efficient routing algorithms for the DTNs (Spyropoulos et al., C. Liu and J. Wu) has not done much for the security issues. The security of the bundles as they multi-hop is not assured. Security of the DTN is a serious concern especially because of the unauthorized access and use of the DTN resources (Farrell and Cahill).

3.1 DTN Security and Bundle Authentication

Security is a major problem with the DTN design (Farrell and Cahill). Even though bundle security protocol specification has done much to provide a framework that will ensure the security of the DTNs, frame authentication and fragmentation remain to be an issue.

- Fragmentation: This is a characteristic that is unique for DTNs. When a message to send is large, it might not be possible to send the whole message as one.

- Performance problem: The resource scarcity characteristic of the DTNs is a major problem to the security of the DTNs. Many resources are focused on data bundle authentication, but little attention is given to the security of the bundle. The authentication scheme for the individual bundle that is public key signature based may face expensive transmission and computational costs.

Since the two above issues are closely related, we will address them together.

3.2 Design Goals

The security goal is straight forward: all the relayed messages should be authenticated so that those the bogus ones that might have been inserted by the illegitimate DTN users or external attackers can be efficiently filtered or rejected at the earliest opportunity possible. I am also focused on minimizing the overheads of the security design. These overheads are; computational costs, energy efficiency as well as security design.

3.3 Proposed Scheme

In this particular section, I propose a basic plan referred to as OBBA, which functions to minimize the computational overhead. This is done by exploiting the bundle buffering opportunities. The computational costs for authenticating the bundles origins from the verification of a set of signatures that are issued by different bundle senders. The corresponding certificates for the public key of the signers also require to be verified together. All of the will have to incur a significant verification cost. On the other hand, the ‘Store-Carry-and-Forward’ transmission strategy that DTN uses implies that the bundles do not have to be verified one by one rather they can be verified in a batch.

3.3.1 The Basic OBBA

The major computational cost in the process of data transmission in DTNs is the cost of verification of signatures issued by different bundle senders. The signer’s public key certificates must also be verified together. All will have to incur a verification cost.

ID-based Batch Signature

Recently, batch signature techniques have emerged to permit the signature verifier to verify the signatures of different messages quickly. This batch signature is a signature that allows for batch verification of fragments.

There are few signature techniques that are available, of these we refer (Ferrara et al.) for a comprehensive survey. The benefits of the ID-based batch signature are:

- Inherits the IBC advantage that eliminates that need to have a public key distribution infrastructure. It also relieves the verifier off the duty of checking the authenticity of the public key certificates.

- The batch verification techniques enable the quickly verify several digital signatures by different signers on different messages.

3.3.2 Supporting Fragment Authentication

To carry out this support, the bundle sender has to first split the bundle into multiple base fragments (or proactive fragmentation). A signature is appended to each fragment that allows for every fragment to be self authenticated (toilet paper method). This method might actively increase the fragment signatures required and thus significantly introduce the computation and transmission overhead. Even though the proposed OBBA can act to reduce the verification cost especially at the intermediate nodes as they transfer the bundles, it cannot reduce the transmission costs incurred as the fragment is authenticated.

3.3.3 Utilizing the Fragment Authentication Tree (FAT) to Achieve Efficient Fragment Authentication

In order for the number of signatures to be reduced, and also to provide fragment authentication, the sender might build a Merkle hash tree on them (Merkle). They will then only be required to sign the root of the tree that will thereby generate one signature for all unsigned fragments. The Merkle Hash Tree is also referred to as ‘binary’ hash tree.’

Chapter 4

Conclusion and Future Work

In this particular chapter, I conclude this thesis with a word on future work

4.1 Conclusion

This thesis has brought about major contributions as follows:

- We carried out a study on a series of DTN security features. We noted this features distinguished DTN security from conventional network security issues. The challenges related to DTN security are as follows: an efficient bundle authentication, certificate revocation and self issue.

- For the bundle authentication to be efficient, I proposed a plan that would carry out authentication on bundles as a batch.

4.2 Related Work

The DTN architecture is based most closely on work that originated with the Interplanetary Internet (Cerf et al.) design, but represents a significant generalization to other types of networks suffering from non-Internet-like performance characteristics. It addresses several of the issues raised in the “network survivability” literature (J. Heidemann), especially with respect to networks lacking continuous connectivity.

With respect to store-and-forward routing in other frequently- disconnected networks, a number of recent efforts have arisen. In ZebraNet (Juang, et al.), wireless sensor nodes (attached to animals) collect location data and opportunistically report their histories when they come in radio range of base stations. They explore the case of mobile base stations and sensor devices and the use of a pair of flooding-based routing protocols. In DataMules (R. Shah), low-power sensor nodes can save power if periodically visited by a "mule" that travels among them and provides a non-interactive message store-and-forward service. In these two efforts plus that of Vahdat, mobility models are employed in a simulation to predict the ability of partially connected networks to deliver data eventually.

The use of late binding for names in DTN is shared with, although not directly based upon, the work on Intentional Naming (Adgie-Winoto et al.). Here, names represent a form of query and are used specifically for any cast in order to locate nearby network services. Routing based on names is shared, to some degree, with Internet Content Routing (Gritter & Cheriton). This work focuses on using routing on names to providecontent distribution facility for the Internet, addressing its scalability and performance. It does not use two separate name components as in DTN, but does suggest the viability of the name-based routing mechanism. The generality of the entity portion of names is influenced by (Heidemann et. al), where database-like queries are effectively used as addresses for groups of sensor nodes.

The architectural thinking regarding interoperability and layering is guided by principles of the ARPANET/Internet (Cerf et al.; Clark D.). DTN gateways operate in many ways similar to Internet routers, but are adapted for use in high-delay and disconnected environments by storing messages for potentially long periods of time.

4.4 NASA and DTN

The European Space Agency (ESA) and NASA have successfully used an experimental version of the interplanetary internet to control a rover from the international Space Station. This particular experiment used NASA's DTN protocol to demonstrate technology and transmit messages. This is the technology that is believed will one day enable internet communication between space vehicles and also support infrastructure and also habitats on another planet.

Sunita Williams, a space commander of the Expedition 33 space station, used a NASA developed laptop to remotely drive a small LEGO robot at the European Space Operations Centre, Germany. The experiment was led by the Europeans used NASA's DTN to stimulate a scenario in which an astronaut in a vehicle orbiting a planetary body controls a robotic rover that is on the planet's surface.

The DTN architecture is a new communications technology that enables standardized communications similar to the Internet to function over long distances and through time delays associated with on-orbit or deep space spacecraft or robotic systems. The core of the DTN suite is the Bundle Protocol (BP), which is roughly equivalent to the Internet Protocol (IP) that serves as the core of the Internet on Earth. While IP assumes a continuous end-to-end data path exists between the user and a remote space system, DTN accounts for disconnections and errors. In DTN, data move through the network "hop-by-hop." While waiting for the next link to become connected, bundles are temporarily stored and then forwarded to the next node when the link becomes available.

NASA's work on DTN is part of the agency's Space Communication and Navigation (SCaN) Program. SCaN coordinates multiple space communications networks and network support functions to regulate, maintain and grow NASA's space communications and navigation capabilities in support of the agency's space missions.

The space station also serves as a platform for research focused on human health and exploration, technology testing for enabling future exploration, research in basic life and physical sciences and Earth and space science.

4.3 Future Work

This thesis has provided a layout of the DTN security issues and solutions to better the protocol. More research can be carried out on the subject matter. I propose for more research to be conducted on selfish nodes as these nodes do not relay the data efficiently in DTNs

Works Cited

A.Kate, G. Zaverucha and Urs Hengartner, "Anonymity and security in delay tolerant networks," In Proc. of *SecureComm'07*, Sept. 2007.

A. L. Ferrara, M. Green, S. Huhenberger and M. Pedersen, "On the practicality of short signature batch verification," available in http://eprint.iacr.org/2008/015.pdf, 2008.

A.Vahdat, D. Becker, "Epidemic Routing for Partially-Connected Ad Hoc Networks", Duke Tech Report CS-2000-06, 2000 M. Gritter, D. Cheriton, "An Architecture for Content Routing Support in the Internet", Proc. Usenix USITS, March 2001.

D. Clark, "The Design Philosophy of the DARPA Internet Protocols", Proc. SIGCOMM 1988.

DTNRG. Delay tolerant networking research group: dtn-interest mailing list archive, April 2005. Available from http:// mailman.dtnrg.org/pipermail/dtn-interest/2005- April/.

J. Heidemann et. al., "Building Efficient Wireless Sensor Networks with Low-Level Naming", Proc. SOSP, Oct 2001

J. Sterbenz, et. al., "Survivable Mobile Wireless Networks: Issues, Challenges and Research Directions", WiSe 2002, Sep 2002

K. Scott and S. Burleigh, "Bundle protocol (BP)." http://tools.ietf.org/html/rfc5050, 2007. IETF Request for Comments, RFC 5050.

M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Galois/Counter (GCM) and GMAC," *NIST Special Publication 800-38D*, November 2007.

[Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott and Cheng Luo, “Applicability of identity-based cryptography for disruption-tolerant networking,” In Proc. of *MobiOpp*, June 2007.

NASA, “Rationale, scenarios, and requirements for DTN in space.” http://public.ccsds.org/publications/archive/734x0g1e1.pdf, 2010. CCSDS 734.0-G-1, Green Book.

P. Juang, H. Oki, Y. Wang, M. Maronosi, L. Peh, D. Rubenstein, “Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet”, Proc. ASPLOS, Oct 2002

R. Merkle, “Protocols for public key cryptosystems,” In Proc. of *IEEE S&P*, pp. 122-133, 1980.

R. Shah, S. Roy, S. Jain, W. Brunette, “Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks”, IEEE SNPA Workshop, May 2003

S. Farrell and V. Cahill, “DTN: An architectural retrospective,” *IEEE J. Sel. Areas Commun.*, vol. 26, no. 5, pp. 828-836, June 2008.

S. Farrell and V. Cahill, “Security consideartons in space and delay tolerant networks,” In Proc. of *SMC-IT’06*, July 2006.

S. Symington et al., “Bundle security protocol specification.” http://tools.ietf.org/html/rfc6257, May 2011. IRTF Request for Comments, RFC 6257.

T. Spyropoulos, K. Psounis and C. S. Raghavendra, “Efficient routing in intermittently connected mobile networks: the multiple-copy cast,” *IEEE/ACM Trans. on Networking*, vol. 16, no. 1, Feb. 2008.

V. Cerf et. al., “Interplanetary Internet (IPN): Architectural Definition”, http://www.ipnsig.org/reports/memo-ipnrg-arch-00.pdf

V. Cerf, R. Kahn, “A Protocol for Packet Network Inter- communication”, IEEE Trans. on Comm., COM-22(5), May 1974

W. Adgie-Winoto, E. Schwartz, H. Balakrishnan, J. Lilley, “The Design and Implementation of an Intentional Naming System”, Proc. SOSP, Dec 1999

Biography

Mohaymen Aljarrah graduated from Lamar High School, Houston, TX, in 1988. He received his Bachelor of Arts from George Washington University in 2004, a Master in Business from Georgetown University. He is employed by National Aeronautics and Space Administration as a Head of Network in Washington DC for twelve years, and expected to graduate his Master of Science in Information Technology from George Mason University in the summer of 2014.