A Novel Security Architecture for a Space-Data DTN

Nathan L. Clarke[1,2], Vasilis Katos[3], Sofia-Anna Menesidou[3],
Bogdan Ghita[1], and Steven Furnell[1,2]

[1] School of Computing and Mathematics, Plymouth University, Plymouth, United Kingdom
info@cscan.org
[2] School of Computing and Security, Edith Cowan University, Western Australia
[3] Department of Electrical and Computer Engineering,
Democritus University of Thrace, Greece

Abstract. In this paper we reflect upon the challenges and constraints of a DTN infrastructure handling space data and propose a suitable security architecture for offering security services. The security requirements are expressed in terms of architecture components and supporting security processes. The architecture is provided as a point of reference for validating and evaluating future security controls and processes suitable for space data DTN environments.

Keywords. DTN, security DTN, secure communications, security architecture.

1 Introduction

Delay or Disruption Tolerant Networks (DTNs) are becoming popular both in terrestrial and deep space environments as they maintain certain advantages over traditional networking protocols such as TCP/IP. The benefits of adopting DTN technologies are clear in environments where connectivity in terms of end-to-end path availability cannot be guaranteed for the lifetime of a communications session.

Although DTNs by their nature support high availability, they are not short of security issues. This is primarily due to the constraints of the unwelcoming and hostile environment within which the communications take place. The three main limitations composing a typical space-internetworking environment are: the limited bandwidth, the relatively high bit error rates, and the periods lacking connectivity where in some cases open loop communication is the only option.

Security issues therefore arise in how to achieve end-to-end security of communications, with many standardised approaches being ineffective due to the high number of handshaking messages required to setup the secure channel. These would simply be not possible in a delay/disruptive network environment. Furthermore, issues regarding successful polices for enabling authentication, authorisation and accountability services within a Space-Data DTN exist. Indeed, little research has been published demonstrating how this can be achieved in reality.

The purpose of this paper is to propose a novel architecture to support the secure management and delivery of data across a Space-Data DTN. Section 2 describes the current state of the art, highlighting the unique threats present within a DTN and the

Y. Koucheryavy et al. (Eds.): WWIC 2012, LNCS 7277, pp. 342–349, 2012.

advances made on developing a protocol for securing the channel. Section 3 and 4 present the novel architecture and secure data channel models, with a detailed explanation of both being provided. A discussion of these processes follows this, before Section 6 presents the conclusions and future work.

2 Background Literature

The area of security in Delay Tolerant Networks is relatively new and many research challenges remain to date. The DTN Research Group has published Internet-drafts on DTN Security Overview, Bundle Security Protocol Specification and Bundle Security Protocol Specification [1-3]. The Bundle Protocol (BP) exists within the DTN architecture and provides the capability of dealing with particular DTN characteristics, such as intermittent connectivity, custody retransmission and differing types of service delivery (e.g. scheduled, predicted and opportunistic connectivity)[2]. The DTN architecture [4] defines the "bundle layer" that may exist anywhere between the transport and the application layers of the OSI model.

The DTN Security Overview provides a useful insight into the possible threats faced within an DTN-based architecture [1]. The authors have identified the following potential threats: non DTN node threats; resource consumption; amplifying threats via forwarding bundles that were not sent by authorized DTN nodes; denial of service threats; attacks against the confidentiality and integrity of data; traffic storms (i.e. particular bundle protocol configurations allow for the generation of extra bundles) and partial protection (i.e. not all DTN nodes will have the ability to enact all security functionality).

The recently published Bundle Security Protocol Specification (BSP) states that addressing security issues is important for the Bundle Protocol (BP) [3]. The specification defines security features for the BP for use in DTNs. It specifically describes four security blocks to provide different security services. The four blocks, the Bundle Authentication Block (BAB), the Payload Integrity Block (PIB), the Payload Confidentiality Block (PCB) and the Extension Security Block (ESB), are defined in the Abstract Security Block (ASB). However, in the specification key management is not covered and the authors explicitly state that such exclusion is a result of an informed decision.

The author in [5] states some requirements for key management in delay tolerant networks but no solution is yet proposed. The internet draft [1] also provides an overview of the security requirements and mechanisms considered for DTNs security. More recently, two new internet drafts [6-7] extend the specification [3] and specify eight new Ciphersuites for use with the BSP's security blocks. However, until now few solutions have been proposed to address the security in DTNs. The work in [8] provides a security analysis of the RFCs and internet drafts with a focus on space-based communication networks. The author also identifies the problem that the management of security of the mission systems and the communication infrastructure is currently separate.

The authors in [9] introduce a solution based on Identity-Based Cryptography (IBC), a cryptographic method that enables message encryption and signature

verification using a public identifier. In [10], the authors use the non-interactive Sakai-Ohgishi-Kasahara (SOK) key agreement scheme, which is based on Boneh-Franklin IBC scheme. However, such IBC solutions appeared to superficially solve the problem. The work in [11] examines and identifies a number of problems and issues of the BP. They point out the lack of integrity checksums for reliability checks in the BP and the need for network time synchronization in order to increase the performance and reliability of the BP. Finally, a more recent study [12] addresses the key management problem in DTN by using one-pass authenticated key exchange protocol. The authors try to minimize the communication cost by using an adoption of Horsters-Mitchels-Peterson protocol.

To summarize, the Bundle Security Specification Protocol provides a baseline of cryptographic services for the bundle layer. The BSP supports flexibility and extensibility for the cryptographic mechanisms, allowing the relevant header fields to match the constraints and requirements imposed by the underlying environment or application domain. However, key management remains an open issue and would benefit from further research. Furthermore, little research exists on proposing how to achieve various other security requirements required within an operational DTN infrastructure. For instance, with regards to providing authentication, authorization and accountability (AAA) services.

3 Security Architecture

Based upon a set of analyses, which included deploying a stakeholder questionnaire to capture end-user requirements and expert analysis, the following architecture was proposed. The Space-Data DTN also includes an additional requirement beyond normal DTN systems in that it must support the long-term storage of large volumes space data within the DTN itself. The architecture is comprised of the following key components:

- Management Application (MA) – a web application that facilitates end users obtaining space-data. The application provides authentication, authorisation and accountability services
- Data originator (DO) – the original source of space data that is placed within the DTN. These components are assumed to be trusted.
- End-Users (EU) – the final destination of space data
- Trusted DTN nodes (TDTN)– a subset of the DTN nodes that are able to deliver space-data datasets

The term Trusted DTN is used in order to differentiate between the already defined Security DTN. The latter is defined by the Bundle Protocol and provides the communication security between security DTN nodes at the bundle layer. Trusted DTN nodes are security DTN nodes but also include additional functionality:

- Operating above the Bundle layer, they provide the functionality to store (and subsequently forward) complete datasets, rather than simply bundles (as defined by the Bundle protocol)

- Trusted DTN nodes have standard Internet-based communication capabilities with the Management Application – i.e. all management signalling information between the MA and TDTN conforms to standard internet based traffic conditions and is not subject to delay, disruption that a DTN network connection could be.

Fig. 1 illustrates the principal interactions of the key components within the Space-Data DTN. Contrary to typical DTN implementations, this architecture replies upon access to normal network communications in addition to the DTN. This capability permits the use of standard security mechanisms to protect key services – mechanisms whose operation could not be relied upon in a DTN where delay and disruption are present.

For simplicity and ease of understanding some DTN network connectivity between nodes is missing; however node "W" provides an indication of the interconnectivity of nodes within the DTN. The figure presents three different types of network connectivity for illustration. This is not a definitive set of connectivity but merely an example of the interactions between the principal components. Data Originators A, B and C are all storing their datasets within the DTN network – at the Bundle layer within both the Security and Trusted DTN nodes. Complete datasets are stored at the Trusted DTN nodes. Users A, B and C are also downloading datasets from the DTN network from the Trusted DTN nodes. In all three examples, data is sent within the DTN to untrusted DTN nodes with security being maintained between security and trusted DTN nodes (as specified by the Bundle Protocol security). The Management Application provides the mechanism for Trusted Nodes and Users to communicate and request datasets.

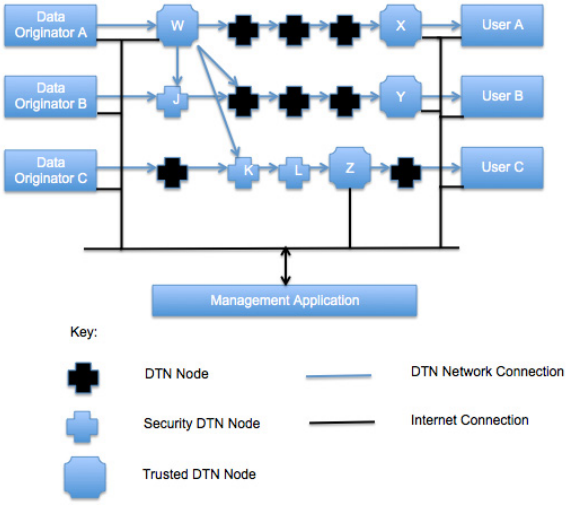

Fig. 1. Security Architecture Overview

Fig. 2 illustrates the network interactions that are sent when downloading space data from the DTN. A user requests a dataset by logging into the Management Application and clicking upon the available datasets. A one-time URL (with sufficiently long

freshness) is generated by the Management Application and sent to the most appropriate (frequently this would be geographically nearest) Trusted DTN nodes that is currently storing the dataset alongside additional information identifying the user. The same URL is then set to the User so that they can directly request the data across the DTN. All communication sent across the Internet-based network is secured. This process does rely upon a number of assumptions (which hold true):

- A process exists for datasets to be distributed from Data Originators onto the DTN.
- A process exists for the Management Application to be knowledgeable of where the datasets are distributed throughout the DTN.
- The Management Application, Users and Trusted DTN nodes can communicate via a normal Internet-type connection

In reality, the communication path indicated by the label (4) could be any combination of un-trusted DTN nodes, security DTN nodes and Trusted DTN nodes. Indeed, on some data requests, the user might find themselves a single hop from a Trusted DTN node with the necessary datasets. On other occasions, the datasets might need to transverse large segments of the network.

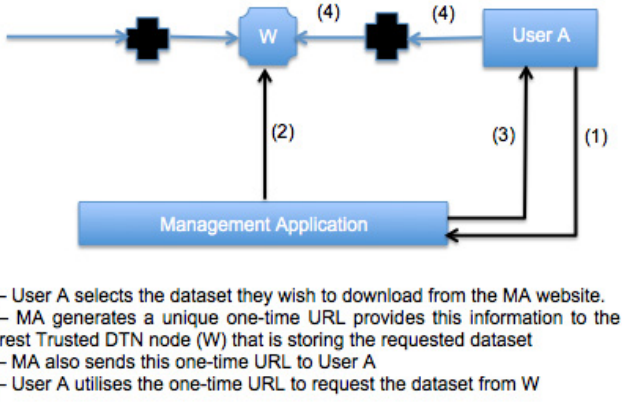

Fig. 2. Data Request Process

Based upon this architecture, there is a clear division between signals that communicate actual space-data and those that are concerned with management/control-based information:

- Space-Data transverses the DTN, is subject to delay and disruption but is capable of transferring large volumes of data reliably and securely.
- Management Data transverses the Internet, is not subject to delay and disruption and consists of relatively short volumes of data that enable efficient and secure operation of the Space-Data DTN.

The reasons for such a division reside with the capability of utilising existing security infrastructures within the Internet-based communications. Through being able to es-

tablish trust within key components of the network, the resulting threats are reduced and subsequent security mechanisms required can be taken from well-accepted standardised protocols (e.g. Transport Layer Security (TLS)).

4 DTN Data Security

The two main constraints influencing the design and deployment of the security mechanisms of a DTN infrastructure operating in a space environment are the limited bandwidth and the limited - yet in many cases predicted - connectivity between nodes. These constraints combined with the opportunistic data transfer approaches of DTN lead to the need for developing hybrid policies to effectively manage the trade off between security (i.e. the underlying computational and communication costs) and communication efficiency. As such, a data router must be equipped with the functionality to make routing decisions influenced by the security policy and needs.

In order to support efficient security mechanisms, key distribution consists of two key phases. The first phase involves computationally and communications intensive establishment of the long term key infrastructure. This can involve PKI components such as digital certificates. In addition, due to the limitations many devices may have in space (including power), low energy and memory consumption algorithms need to be considered, such as elliptic curve based PKIs.

The second phase refers to the secure session establishment. In this context, the term session depends on the security assertions and underlying scenario and is used to describe the situation where a node needs to create a confidential channel to some destination (not necessarily the final destination of the data, as end to end security cannot always be guaranteed or offered). Preference is given to one-pass security protocols.

The cryptographic keys and the cryptographic protocol metadata information will be transported using the Bundle Security Protocol specification. The BSP provides adequate flexibility to incorporate a wide range of key management protocols through the Extension Security Block (ESB) specified in BSP.

The BSP will also be used to support integrity services. Integrity in the space data layer is primarily offered by the Bundle Security Protocol when possible. In a DTN path that contains a mix of security aware and unaware nodes, integrity on the bundle layer will be verified whenever the custodian is a node capable of supporting BSP.

However there may be cases where the either the whole path is non BSP aware, or the integrity requirements are higher and the bundle layer integrity policies are not sufficient. Consider for example the case of remote firmware or operating system upgrades, where the upgrade instructions and firmware payload transferred to a deep space location will need to be both authenticated its integrity verified. In such a scenario, integrity will need to be offered by the application. Clearly in this case it is the MA which maintains the scope definitions of the data requiring integrity.

Finally, routing decisions are influenced by the security requirements of the underlying bundle and the data it holds. A router will need to implement a set of simple security and routing policies. A policy example is shown in Fig. 3.

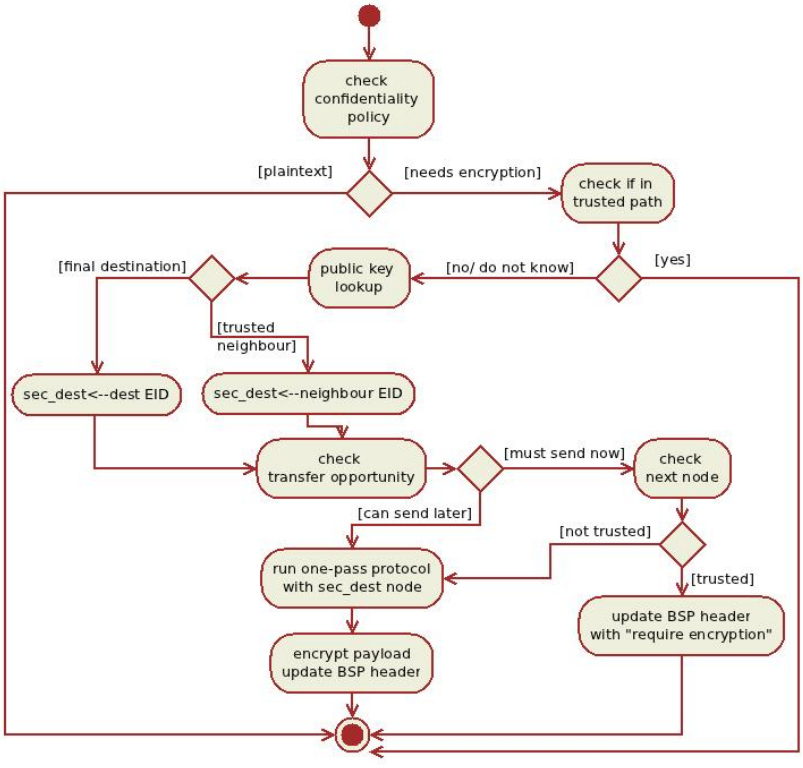

Fig. 3. Hybrid routing/security policy example (source: [12])

5 Conclusions and Future Work

The current state of the art clearly shows a significant lack in due consideration to both data-level security and to the operational security requirements. Given the set of security requirements, the security architecture has been proposed that has addressed the key requirements identified and protects against a wide range of DTN and non-DTN based threats that the system is vulnerable against. Key to this architecture is the use of both DTN and non-DTN networks that permit the use of a combination of both DTN specific security protocols and well-established (and thus accepted) security protocols typically found within secure internet-based services.

Future work will seek to validate the proposed architecture within an operational Space-Data DTN where it will be possible to evaluate the performance characteristics and usability of the proposed security mechanisms.

Acknowledgements. The research leading to these results has received funding fro the European Community's Seventh Framework Programme (FP7/2007-2013_FP7-SPACE-2010-1, SP1 Cooperation, Collaborative Project) under grant agreement no. 263330 (project title: SPACE-DATA ROUTERS for Exploiting Space DATA). This paper reflects only the authors views and the Union is not liable for any use that may be made of the information contained therein.

References

[1] Farrell, A., Symington, S.F., Weiss, H., Lovell, P.: Delay-Tolerant Networking Security Overview, internet-draft (2009), http://tools.ietf.org/html/draft-irtf-dtnrg-sec-overview-06

[2] Scott, K., Burleigh, S.: Bundle ProtcolSpecification, Request for Comments, RFC 5050

[3] Symington, S., Farrell, S., Weiss, H., Lovell, P.: Bundle Security Protocol Specification. Request for Comments, RFC 6257

[4] Cerf, V., Burleigh, S., Durst, R., Scott, K., Fall, K., Weiss, H.: Delay-Tolerant Networking Architecture, RFC 4838 (2007), http://www.ietf.org/rfc/rfc4838.txt

[5] Farrell, S.: DTN Key Management Requirements, work in progress as an inter-net-draft (2007), http://tools.ietf.org/html/draft-farrell-dtnrg-km-00

[6] Burgin, K., Hennessy, A.: Suite B Ciphersuites for the Bundle Security Proto-col, inter-net-draft (2012), http://www.ietf.org/id/draft-hennessy-bsp-suiteb-ciphersuites-00.txt

[7] Burgin, K., Hennessy, A.: Suite B Profile for the Bundle Security Protocol, internet-draft (2012), http://www.ietf.org/id/draft-hennessy-bsp-suiteb-profile-00.txt

[8] Ivancic, W.D.: Security Analysis of DTN Architecture and Bundle Protocol Specification for Space-Based Networks. In: Aerospace Conference, pp. 1–12 (2010)

[9] Asokan, N., Kostiainen, K., Ginzboorg, P., Ott, J., Luo, C.: Towards securing disruption-tolerant networking. Technical Report NRC-TR-2007-007 (2007)

[10] Kate, A., Zaverucha, G., Hengartner, U.: Anonymity and Security in Delay Tolerant Networks. In: 3rd International Conference on Security and Privacy in Communications Networks and the Workshops, Secure Communication, pp. 504–513 (2007)

[11] Wood, L., Eddy, W.M., Holiday, P.: A bundle of problems. In: Aerospace Conference, pp. 1–14 (2009)

[12] Menesidou, S.A., Katos, V.: Authenticated Key Exchange (AKE) in Delay Tolerant Networks. In: Gritzalis, D., Furnell, S., Theoharidou, M. (eds.) SEC 2012. IFIP AICT, vol. 376, pp. 49–60. Springer, Heidelberg (2012)