Security analysis for Delay/Disruption Tolerant satellite and sensor Networks

N.Bhutta,G.Ansa, E. Johnson
Centre for Communication Systems Research
University of Surrey
Guildford, United Kingdom
m.bhutta, g.ansa, e.johnson - @surrey.ac.uk

N. Ahmad, M. Alsiyabi, H.Cruickshank
Centre for Communication Systems Research
University of Surrey
Guildford, United Kingdom
n.ahmad, m.alsiyabi, h.cruickhank - @surrey.ac.uk

***Abstract*— In the last few years, Delay/Disruption Tolerant Networking has grown to a healthy research topic because of its suitability for challenged environments characterized by heterogeneity, long delay paths and unpredictable link disruptions. This paper presents a DTN security architecture that focuses on the requirements for lightweight key management; lightweight AAA-like architecture for authentication/authorisation; resilience to Denial of Service attacks and user anonymity.**

Keywords—security, DT, Bundle, PKI and key management

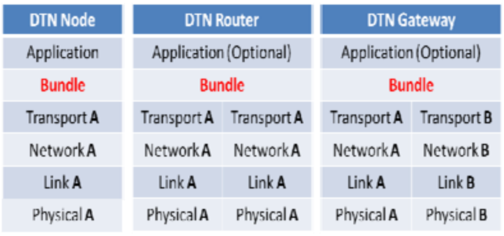
I. INTRODUCTION

Today's Internet protocols perform poorly when faced with heterogeneous environments characterized by very long delay paths and possible link disruptions such as satellite and sensor networks. These environments often referred to as “Challenged Networks”, become even worse when coupled with terminals characterized by severe power or memory constraints. In addition, communication outside of the Internet is usually accomplished on independent networks, each supporting specialized communication requirements.

Delay/Disruption Tolerant Networking (DTN) is promising network architecture for heterogeneous environments. It aims at solving both challenged networks problems and independent networks incompatibility [1],[2]. It works as overlay architecture on top of independent networks, including the Internet. DTN offers an application interface structured around an optionally-reliable store and forward packet exchange, with restricted or null expectations of end-to-end connectivity and possibly limited node resources.

The DTN architecture was designed to accommodate not only network connection disruptions, but also to provide a framework for dealing with lower layers heterogeneity by introducing a new layer called “Bundle” layer. It works on top of transport layer to better handle the long delays or disconnectivity and high loss rate due to disruption by using store-forward-mechanism. The data (called bundle) is stored in persistent storage on each DTN device and is forwarded to other node when the link is available.

There are three main components in DTN architecture: Node (or Bundle Node), Router and Gateway as shown in Figure 1. Every DTN node is aware of the bundle layer which helps to provide better performance in high delays/disruptions and data loss environment. DTN routers work in one network region (areas having similar networking technology) while DTN gateways work in different network regions to handle different transport, network, and link layers. More details on DTN architecture are available in [2].



DTN Node	DTN Router		DTN Gateway	
Application	Application (Optional)		Application (Optional)	
Bundle	Bundle		Bundle	
Transport A	Transport A	Transport A	Transport A	Transport B
Network A	Network A	Network A	Network A	Network B
Link A	Link A	Link A	Link A	Link B
Physical A	Physical A	Physical A	Physical A	Physical B

Figure 1. DTN Layers Stack

This paper focuses on security issues in the application of DTN architecture to satellite and sensor networks. This may include scenarios such as United Nation (UN) peacekeeping forces, environmental and disaster monitoring, Governmental or Non-Governmental Organizations (GOs and NGOs) aid in underdeveloped regions of the world.

We will elaborate the UN peacekeeping in war zones and conflict areas scenario and use it as the motivation and framework for the rest of the work in this paper. This will be the bases of threat analysis, security requirements and derive the security architecture that satisfies these requirements. The global scale of this scenario requires collaboration between various security domains such as satellite operators (e.g. Inmarsat), UN headquarters in New York and local governments in the conflict area. This scenario is suitable for use of satellites and also suitable for DTN because of the unreliable and unscheduled communications.

Figure 2 shows the UN peacekeeping scenario with 4 satellite terminals in independent regions. Each region has DTN Gateway (DTN-G). DTN-G1 and DTN-G2 represent the UN sensors and communications networks in two different areas of the conflict region (e.g. UK and US soldiers working under UN control). DTN-G3 represents the local government or an aid organisation region (e.g. Red

Cross) and DTN-G4 represents the UN headquarter. Both DTN-G3 and DTN-G4 are connected to the public internet to provide limited services to the local population in the conflict area.

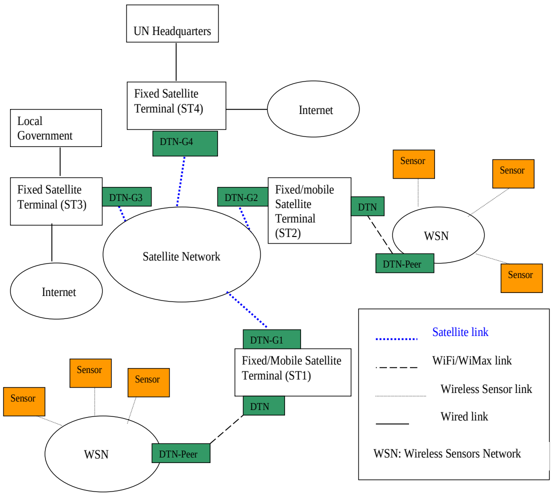


Figure 2. UN peacekeeping scenario with DTN concept

The types of services that are envisaged for this network are:

- Limited, but reliable data exchange, Internet Access, Chat and E-mail for the UN personnel, aid workers and local population.
- Vehicles and equipment tracking, positioning and emergency messages. These services require a combination of telecommunication and positioning systems.
- Sensor networks for data collection in relation to the UN monitoring and operations.

From security prospective, DTN-G1, DTN-G2, DTN-G3 and DTN-G4 represent four security gateways in independent regions but can collaborate with each other.

II. Threat Analysis

In general, security threats can be divided into passive and active threats. The initial threat analysis of the above scenario shows that passive threats are a major concern due to the broadcast nature of satellites. One example is an intruder monitoring the satellite broadcast and then extracting some sensitive data. This includes eavesdropping and traffic analysis with the goal to obtain private information and gain knowledge about the communicating parties.

Active threats (or attacks) are more difficult to implement successfully than passive threats and usually require more sophisticated resources and may also require access to the satellite terminal. Examples of active attacks are:

- Masquerading: An entity pretends to be a different entity such as UN personnel, aid worker or legitimate local person. The aim is gaining access to the network resources in an un-authorised way.
- Modification of transmitted messages. This includes intruders trying to disrupt the UN operations in the war or conflict regions.
- Replay attacks: Here an intruder sends some old (authentic) messages to the receiver. In the case of a broadcast link, access to previous broadcast data is easy.
- Denial-of-Service (DoS) attacks: The aim of the attacker is preventing authorized users from accessing a service. For example, an intruder (attacker) can send a large number of bogus messages to a DTN Gateway in order to keep it busy and degrade the services to other users.

Examining the above threats gives rise to DTN security requirements such as lightweight key management; lightweight AAA-like architecture for authentication/authorisation; resilience to Denial of Service (DoS) attacks and providing anonymity to end users. The following sections elaborate each of these requirements.

III. DTN Security Architecture

Current Security Protocols do not perform well in high delay/disruption conditions, because of underlying assumption on which they are built, such as end-to-end connectivity is always present; low link delays between communicating parties and low error rate on link channels. Thus, new security architecture is needed to meet DTN requirements [3], [4].

Figure 3 shows two DTN Bundle Nodes BN1 and BN2 from two different networks connected to each other through DTN gateways BN2 and BN3. Any DTN node originating or forwarding the data packet, stores it in its memory until it has been delivered to next node, showing "Store and Forward" style of communication.

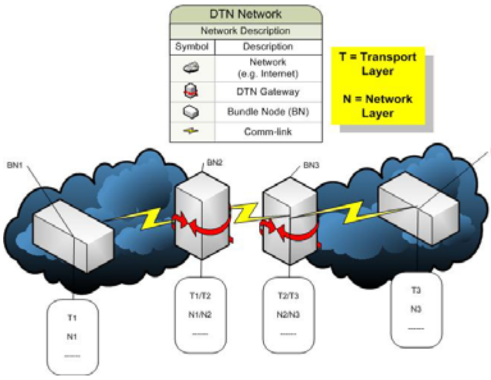


Figure 3. Internetworking of DTN Networks Using Bundle Gateways

The security architecture supports hop-by-hop and end-to-end authentication and integrity validation, to ensure data is correct before forwarding. Figure 4 shows the hop-by hop authentication/integrity check using Bundle Authentication Block (BAB). The BAB is used to assure the authenticity and integrity of the bundle along a single hop from forwarder to intermediate receiver. Thus, the communications path is divided into security zones in Figure 4. Similarly and for end-to-end security services, the Payload Integrity Block (PIB) and Payload Confidentiality Block (PCB) are used. Further details on security architecture in DTN can be found in [4].

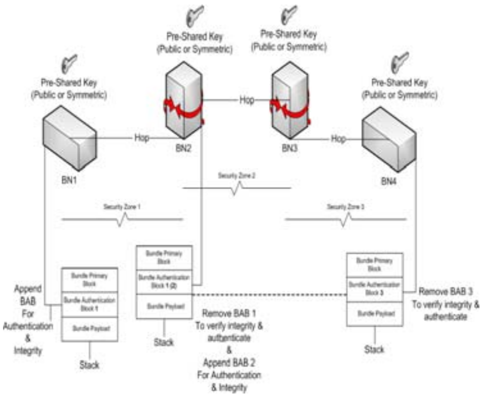

Pre-Shared Key (Public or Symmetric)
Pre-Shared Key (Public or Symmetric)
Pre-Shared Key (Public or Symmetric)
Pre-Shared Key (Public or Symmetric)
Hop
Hop
Hop
BN1
BN2
BN3
BN4
Security Zone 1
Security Zone 2
Security Zone 3
Bundle Primary Block
Bundle Authentication Block 1
Bundle Payload
Bundle Authentication Block 1 (2)
Bundle Authentication Block 3
Stack
Append BAB For Authentication & Integrity
Remove BAB 1 To verify integrity & authenticate & Append BAB 2 For Authentication & Integrity
Remove BAB 3 To verify integrity & authenticate

Figure 4. Hop-by-hop authentication and integrity check [4]

IV. KEY MANAGEMENT IN DTN

To enable peacekeeping forces and aid workers to communicate securely, all security services like confidentiality, integrity, non-repudiation etc, are required to be provided end-to-end and hop-by-hop within the DTN infrastructure. Key Management is one of the most difficult problems in DTN security. DTN security requires that before forwarding the bundle it must be authenticated and integrity checked. In DTN, link availability is an important resource and special techniques need to be applied to maximise the utilization of such link. The key management requirements can be summarised as follows:

- A single key management scheme might not be sufficient for DTN networks due to heterogeneity of networks, like satellite networks, sensors networks etc. So, a whole framework is required to provide the services of key management.
- Different kind of key transport and key agreement options should be provided to handle heterogeneity and also key management framework should provide schemes based on pre-shared secrets or manual keys.
- As DTN architecture supports heterogeneity, so different nodes capabilities should be taken into consideration. It should be assured that proposed schemes are also suitable for very low powered devices as well.
- The key management scheme should be adaptive and less chatty. The key management messages should be exchanged within minimum number of passes.

Examining the requirements above, reveal that existing key management schemes are not suitable for DTN environment.

Public Key Infrastructure (PKI) is widely used today and provides secure key transport, but incurs high computational cost. The large number of certificate verifications and certificates revocation lists check requires link and bandwidth availability. Thus, traditional PKI alone cannot provide good performance in DTN networks.

DTN needs to support symmetric as well asymmetric cryptography in order to obtain robust security architecture. There are several symmetric key management protocols in existence. Although computationally less expensive than public key cryptography, symmetric cryptography use for key management requires larger number of message exchanges. This can be problematic in DTN environment.

In DTN, security-source and security-destination can be different from data original-source and final-destination. Therefore delegation mechanism is required. Proxy certificates based schemes seem to be promising techniques [5].

Our current research focus is to formalize different key management parameters based on proxy certificates and PKIs, Kerberos based public key authentication mechanisms like PKINIT and M-PKINIT. A combination of these protocols (public and symmetric cryptography based mechanisms) can be manipulated to achieve a more efficient key management solution which will be more suitable for DTN networks. An example of PKI and Kerberos based security architecture is “Computationally Efficient PKI based Single Sign On protocol (PKASSO)” described in [6].

V. AUTHENTICATION AND AUTHORISATION IN DTN

Authentication and Authorization are two processes that can be used to provide access control. This can be part of the key management procedures or performed separately. It protects the network from unauthenticated entities and usage of network resources from unauthorized entities. Centralized and decentralized architectures are known architectures for access control implementation [7]. The decentralized architecture is either distributed where access control decision is fully decentralized or hierarchical where access control decision is partially decentralized. The centralized architecture has a single entity responsible for making access control decisions and might use a single set of operational policies. The distributed architecture is ideal for multi-regional networks with region-specific policies. In the hierarchical architecture [8], the regional access control decisions are delegated to the regional management centres or gateways. The AAA (Authentication, Authorization and Accounting) architecture is an example of the centralized architecture. However, this architecture is known to have single point of failure and operational complexity.

A workable access control framework in DTN that suits the UN Peace Keeping scenario (Figure 2) has the following requirements:

- Separate authentication from authorization;
- Prevent masquerading and modification attacks;
- Support offline processing and internal decision making;
- Reduce load on authentication/authorisation servers.

With these in mind, the classical AAA architecture and the distributed trust models are considered not suitable for direct implementation in DTN. We therefore propose a lightweight hierarchical architecture based on the AAA architecture concept that uses a common parameter for data communication. The hierarchical architecture is a good choice because of the need for a centralized entity (third party) to coordinate and monitor the activities of the various regions (distributed) networks. We also opted for the AAA architecture concept because: of the implementation flexibility offered by the AAA standard and the three party authentication model facilitating secured communication in heterogeneous environment.

As shown in Figure 5, the DTN-G4 of the UN Headquarter is the centralized entity that administers the DTN network and authenticates the participating organizations in this network. As examples, the Red Cross Society together with the British and American Armed Forces are participating organizations with distinct roles, and information destined for them must conform to their assigned roles. Each of the individual networks has a security gateway (access server). DTN-G4 authenticates the other security gateways during registration/service initialization phase and assigns them a network identity, role and common communication parameter for the data communication phase. The architecture is designed to allow the security gateways access to a section of messages routed through them to authenticate the source and determine the destination without having access to part of the message that is destined for the end user. Our future work will give a detailed description of the architecture and its components.

In addition, implementing access control and AAA mechanisms will have impact on the network Quality of Service QoS which is still a new research field in DTN. For example, implementing AAA will produce more overheads and may degrade the performance from QoS prospective as more processing will be required. However, both (security and QoS) are important network services in today's internetworked world and are not independent of each other because selecting one mechanism will impact the effectiveness of the other. Also, the access control process will have impact on the flow process (routing) of DTN bundles but yet, there is not identified mechanism for flow characteristic enhancement in DTN. Therefore it is still an active research field [9].

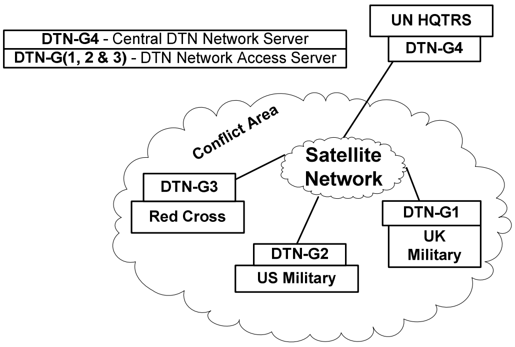


Figure 5. Authentication / authorization Scenario for DTN

VI. RESILIANCE TO DENIAL OF SERVICE (DOS) ATTACKS

Denial of Service (DoS) attacks aim at preventing legitimate users from accessing their entitled services. According to CERT's classification, there are mainly three kinds of DoS attacks [10]: the consumption of scarce, limited, or non-renewable resources, destruction or alteration of configurable information and the physical destruction or alteration of network components. We focus on resource consumption attacks, where the DTN architecture forbids the carriage of illegitimate traffic due to resource scarcity. In order to prevent an unauthorised entity from masquerading as UN personnel, aid worker or a legitimate local person, it is mandatory to authenticate traffic at all nodes which implement the bundle layer security [3].

The security gateways (DTN-G1, 2, 3 and 4) are critical components since they provide access to and from the different regions. Our focus will be on the protection of these security gateways against DoS attacks. Normally, these gateways (acting as authentication and access control points) use public key cryptography to authenticate clients. However, protocols that use strong authentication from the beginning can be used as a hook by an attacker to cause availability problems in the network. The reason is that public key algorithms use computationally expensive methods such as exponentiation and factorization to provide security. Therefore weak authentication mechanisms are required for DTN environment such as cookies [11] and the client puzzles techniques [12]. However, they are not suitable for deployment in DTN because both require several messages exchanges.

We define a number of security and networking requirements to guide our design towards protecting the security gateways from DoS attacks. The security requirements include:

- All traffic must be authenticated to verify the validity of the source through the hop-by-hop and end-to-end security features of the DTN architecture.
- Ensure availability by using lightweight authentication.
- Ensure data freshness by preventing the replay of old messages through the use of timestamps, sequence numbers and nonces.
- Ensure the integrity of messages to provide the assurance that bundle content has not been modified.

In terms of the networking requirements, the design should have:

- Resilience to delays and disruptions which may be in the order of minutes, hours or days.
- Ability to operate even when no end-to-end path exists from source to destination.
- Ability to withstand changes in scheduling and/or in contact of nodes.

In our initial design, we will assume that the attacker has unbounded resources. The security gateways have bounded resources that can be exhausted by a clever attacker. We assume that the attacker has the ability to replay, modify, transmit, receive, and execute the protocol. In order to achieve our objective, we add a light-weight authenticator (cookie) to every bundle which is evaluated by the gateway first (the weak authentication phase). Any traffic that fails the weak authentication is discarded immediately. The cookie verification will only require small amount of computational processing. As such, only a small amount of gateway resources are used in this phase. Otherwise, the client is allowed to proceed to the strong authentication phase (i.e. digital signature verification).

VII. Anonymity and Pseudonym in DTN

Traditional encryption hides transmitted data from intruders. However, the sender and receiver address, packet length and packet timings can provide useful information to adversaries (intruders) to achieve traffic analysis attacks. So this gives rise to the idea of identity protection and anonymity. Anonymity is the non identifiable state within a set of subjects. To achieve anonymity researchers define anonymous protocols in which we dealt with initiator/sender, receiver/recipient anonymity and their unlinkability (who is with whom). Anonymous protocol should prevent message coding attack, timing analysis, message volume analysis and flooding attacks [13]. Generally Anonymous Protocols are based on idea of Mix Network by David Chaum's and onion routing.

However, the above traditional solution for anonymity doesn't work in DTN because of the disconnect nature and routing strategy of DTN. With opportunistic and variable delays, source routing is not always possible. In DTN, there is no complete routing topology so Onion Routing (e.g. TOR) doesn't work because in TOR needs to know the route in advance and encrypt the message accordingly for each router. Mix networks can be applied to DTN as they hold the message for random amount of time and flushes when all packets arrived. To overcome these limitations, we provide DTN anonymity architecture with pseudonym based approach.

With reference to the UN peacekeeping force (Figure 2), DTN-G1 and DTN-G2 can send their secret information to the headquarter (DTN-G4) by encrypting it. The additional requirement here is to keep the identity of the end users (sender and receiver ID and IP address) secret. Examples in the UN peacekeeping scenario will be hiding the identity of high profile users such as high ranking UN and local officials. One possible technique can be the use of Pseudonyms. Pseudonym means falsely named (name other then the real name). In our scenario, we assume that each pseudonym is reference to one holder and can't be transferred to other subjects.

Assuming that DTN gateways (DTN-G1, 2, 3 and 4) are fully trusted and well known. Even with the possibility of an intermediate DTN router being compromised, the intruder will not be able to link the pseudonyms to the real user identity.

VIII. Conclusion

DTN concept is suitable for space as well as terrestrial wireless networks. An overview of DTN architecture and security threats was introduced together with an example scenario of the UN peacekeeping force using DTN concept. Paper shows that traditional key management, authentication/authorisation and DoS resilience methods are not suitable for DTN networks due to the long delays, disruptions and bandwidth limitations. The paper defines the specific requirements that are needed and some possible initial solutions. The paper also presents some initial work on user anonymity in DTN using pseudonym.

Acknowledgments

This work was supported by the EU Information Society Technologies SatNEx II Network of Excellence [14].

References

[1] V. Cerf et al, "Delay-Tolerant Networking Architecture", IETF RFC 4838, Apr. 2007.

[2] K. Fall and S. Farrell, "DTN: An Architectural Retrospective", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 26, NO. 5, JUNE 2008

[3] S.F. Symington, et al, "Bundle Security Protocol Specification", draft-irtf-dtnrg-bundle-security-08, IETF draft. March 2008

[4] S. Farrell, et al, Delay-Tolerant Networking Security Overview, draft-irtf-dtnrg-sec-overview-06, IETF draft. March 2009.

[5] A. Charbonneau, V. Terskikh, "SpectroGrid: Providing Simple Secure Remote Access to Scientific Instruments", HPCS 2008, Quebec June 2008, pp 76 – 82

[6] Ki-Woong et al "Computationally Efficient PKI-Based Single Sign-On Protocol PKASSO for Mobile Devices" in IEEE TRANSACTIONS ON COMPUTERS, VOL. 57, NO. 6, JUNE,2008

[7] M. Nakhjiri and M. Nakhjiri, AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility, John Wiley, c2005, ISBN 0470011947.

[8] A. R. Khakpour, et al, "WATCHMAN: An Overlay Distributed AAA Architecture for Mobile Ad Hoc Networks," in Proc. ARES'08, March 2008, paper 10.1109/ARES.2008.19, pp. 144-152.

[9] L. Wood, etal, "A Bundle of Problems". IEEEAC paper #1023, December 23, 2008

[10] M. Onen, R. Molva. "Denial of Service Prevention in Satellite Networks". IEEE Int'l Conference on Communications, Vol. 7, pp. 4387-4391, June, 2004.

[11] C-Kan Fung et al. "A Denial of Service Resistant Public-key Authentication and Key Establishment Protocol". The 21st IEEE International Performance, Computing, and Communications Conference, pp. 171-178, 2002.

[12] A. Juels at el. "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks". In Proc. Network and Distributed Systems Security Symposium, pp. 151-165, Feb. 1999.

[13] A. Kate, et al, "Anonymity and Security in Delay Tolerant Networks", University of Waterloo, Nov 2007.

[14] Satnex project home page: http://www.satnex.de