ISSN:0975-9646

Secure Key Establishment for Bundle Security Protocol of Space DTNs in Noninteractive manner

Chaitali S.Jadhav
P.G Student M.E Computer science & Engineering,
Shriram Institute of Eng. & Technology,
Paniv, Maharashtra, India

Prof.Prakash B. Dhainje
Vice-Principal Computer science & Engineering
Shriram Institute of Eng. & Technology
Paniv, Maharashtra, India

Dr.Deshmukh Pradeep K.
Principal Computer science & Engineering
Shriram Institute of Eng. & Technology
Paniv, Maharashtra, India

Abstract— **DTN's i.e Delay Tolerant Networks are emerging networks that are widely used in the communication field for implementing a more efficient protocol to use the available bandwidth in the network. DTNs are time independent message delivery systems. It is a kind of store and forward. However the security aspects of these networks are of more concerning subject. So to ensure and increase the authenticity, integrity, and confidentiality, the Committee for Space Data Systems bundle security protocol (BSP) specification have suggested four IPsec style security headers to provide four aspects of security services of bundles. But this specification does not involve the issue of key management. Traditionally, protocols tend to provide security services that are used either (or both) on a hop-by-hop or end-to-end basis. For DTN security though, we require that these services be usable also between nodes that are not a source or destination, but which can be in the middle of a route. So this paper aims the key establishment for Bundle protocol. In this paper, the aim is to utilize a time-evolving topology model and two channel cryptography to design an efficient and non-interactive key exchange protocol. A time-evolving model used to model predetermined behaviour of space DTN. So based on that the scheduling is done for public key exchange. And the two-channel cryptography enables DTN nodes to exchange their public keys and status information, with the assurity of authentication and in a non-interactive fashion. The proposed system helps to establish a secure support for BSP, and tolerating high delays, unexpected loss of connectivity of space DTNs.**

Keywords- Key establishment,SpaceDTN'S,Bundle Security Protocol(BSP).

I. INTRODUCTION

Unlike the Internet which is very broadly used, And many security mechanisms and applications on Internet rely on immediate end-to-end reachability.There are other applications where there is no internet, like in space applications, where it is necessary to communicate from outer space to earth or in the rural areas where internet is not very prevalent because the space internet, it is recognized as a type of Delay or disruption Tolerant Networks (DTNs) which is subject to a high delay and unexpected loss of connectivity.

To overcome these situations where network connection is not readily available, we have introduced Delay Tolerant Network (DTN). This is a store and forward network. As there are variable end-to-end connection between the source and destination the conventional Public Key Infrastructure (PKI) and online negotiation-based key distributing protocols are not applicable in this scenario. In this paper, the aim is to design non-interactive key exchange protocols based on which other security mechanisms are built, and two-channel cryptography is combined with the predictable contacts of space DTNs.

If we have a look over the security for DTN, we must have to take into account the architecture of DTN. DTN is an overlay network architecture which is more often used for communication across heterogeneous communication protocols. This makes communication among different networks easy and secure. It also increases the connectivity in mostly disconnected networks. The networks in this type of scenarios are majorly disconnected so the messages are get stored and then forwarded when the link is get available. This is called store-and-forward network. The research group has developed an RFC for the architecture of DTN. It formulated a new architecture. The new architecture has a Bundle Protocol Layer and Convergence layer in between the Application and Transport layers of the IP stack. Figure1 represents the modified architecture for DTNs.

II. RELATED WORK

A. Basics in Space DTN: In the literature survey we will discuss security issues in space DTN [4] and space DTN and what is the non-interactive message authentication .We will discuss that below.

Space DTNs- The DTN architecture [9] is described as defined in in RFC-4838 as a generalized store-and-forward network overlay, which is applicable to inter-planetary communication environment's. This architecture originates from NASA JPL's experiences in developing store and-forward communication networks for deep space. These kind of networks suffers from high delays and frequent disconnectivity. The Bundle Protocol (BP) defined in DTNRG RFC 5050 supports interoperability across different networks, by creating an overlay network where two or more endpoints can simply exchange information overcoming different transport and network layers. The bundle protocol provides the ability to encrypt protocol elements so that messages in transit cannot practically be read. The bundle security protocol allows for fairly. Flexible combinations of application of the confidentiality and integrity services. However, it disallows some insecure combinations, e.g. a plaintext signature that is out of scope of a confidentiality service would allow plaintext guesses to be verified. So we don't want to offer that option, other things being equal. Protocol Data Unit of DTNs also named as bundles, can be sent over an link which is available and buffered at the next hop until it gets next link in the path. Currently, the architecture for a DTN is defined based on the store, carry and forward manner.

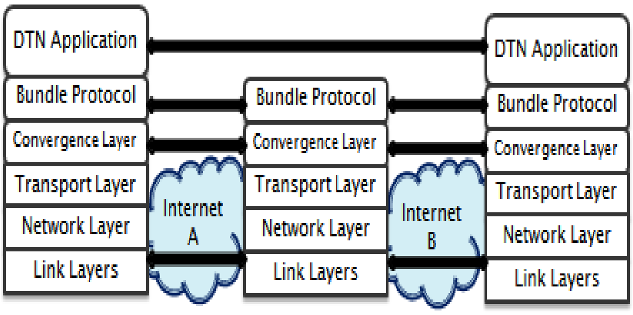

Fig: 1 Network architecture for DTN

The Bundle Protocol provides the following services:

– Completeness: The Bundle Protocol provides an atomic, message-oriented delivery service with no notion of sequenced delivery. Individual messages are delivered or not in their entirety. A Bundle is not delivered with gaps.

– Error-free data delivery: The Bundle Protocol as currently defined may deliver data with errors if the end-to-end data integrity mechanisms specified in the Bundle security protocol are not invoked. If end-to-end integrity is not used, the Bundle Protocol relies on the hop-by-hop reliability mechanisms of the individual underlying transport mechanisms. If end-to-end integrity is used, Bundles are guaranteed to be delivered error-free.

– Delay/disruption tolerant data delivery- If DTN PDUs reach a point in the network path where no forward progress can be made (because, e.g., the next-hop data link is not available), DTN may store the PDUs while waiting for the next-hop link to become available.

– Flexible naming/addressing scheme- DTN uses Uniform Resource Identifiers (URIs) [6] to identify the endpoints of communication. In addition to traditional '(host, port)'-type addressing, these URIs allow data to be addressed to users that meet some criteria, such as all sensors that have registered an event within the past hour.

– Time-to-live- Each Bundle is assigned (by the source application) a 'time-to-live' that is meant to reflect the useful lifetime of the data. The time-to-live represents actual time duration, not a network hop count, and is used to remove Bundles from the system if they cannot be delivered in a timely manner.

B. Security issues in Space DTNs:

Security is the most important issue in the space DTNs [3]. As the BP gets operated over various different networks and underlying technologies so it is very important to save it from various attacks and unauthorized operations. And application of security mechanisms to BP is very challenging in a constrained scenario. So to assure data integrity and confidentiality protecting services for space DTNs, the DTN Research Group (DTNRG) has published an Internet draft as a Bundle Security Protocol Specification (BSPS) [5]. There are security blocks designed which aims to provide four aspects of security services.

Bundle Authentication Block- The Bundle Authentication Block (BAB) provides authentication hop by hop by adding a Message Authentication Code or a signature to each bundle. It identifies the bundle as a DTN bundle and that it is valid.

Payload Integrity Block- This provides the integrity of the payload from the source to destination. Any node on the path between the source and the destination can verify the integrity or authenticity of a bundle via its Protocol integrity block (PIB).

Payload Confidentiality Block- The Payload Confidentiality Block (PCB) is used to encapsulate payload that is encrypted as whole or in part at the PCB source, in order to protect the bundle content. The encrypted payload can be decrypted by the PCB destination as needed.

Extension Security Block- The Extension security block (ESB) provides security for non-payload data like the metadata of the bundle related to the payload but not the actual payload details. It is typically used to apply confidentiality protection and placed in the bundle in the same position as the block being protected.

C. Key establishment and cryptography concepts:

As resources are already limited in DTN, we must reduce the usage of resources for efficient key management. Also, the connections are intermittent and hence, the exchange of keys must not be time consuming. Also, the key revocation is hard as the nodes are not always connected or online and hence, revocation is difficult and need to wait for all the nodes to come online and update their certificates. DTN must avoid unauthorized access to resources on network. It must also prevent unauthorized nodes from reading the data transmitted. This is based on the key management because the keys shared between the users provide the services for access control. And the conventional key management mechanisms used in Internet today is online key distributing protocols or PKI, which can't be applicable to space DTNs, because they rely on the immediate end-to-end reachability that never holds true in space DTNs. So this motivates the requirement for a non-interactive key management scheme as a substitute for the application of any traditional online key distributing protocol or PKI. The non-interactive message authentication [7] protocol needs a lower amount of information over the authenticated channel. But, it is built on the assumption that Hybrid-Collision Resistant (HCR) [8] hash functions. Basically, a non-interactive message authentication protocol uses two separate channels. One is a broadband insecure channel and the other is a narrow-band authenticated channel. Some practical narrow-band channels include Voice-over-Internet-Protocol (VoIP). The narrow-band channels are called as Out-Of-Band (OOB) channels what follows are the common assumptions on two channel cryptography. Two-channel cryptography techniques are often used to design non-interactive message authentication protocols, especially in constrained environments. The OOB channels are recognized as the optimal approach for strong authentication in highly constrained environments. The major advantage of OOB channels are message integrity and authentication, instead of confidentiality. An OOB channel assures each other's identity to two users interacting over it and ensures that the contents of their conversation are not modified.

III. Proposed Approach

A. Problem Definition-

Development of key establishment for Bundle protocol, and public key for tolerating high delays and loss of connectivity of space DTNs. For that purpose we have considered the periodic and predetermined pattern of space DTN links and time-evolving topology model associated with two-channel cryptography to design efficient and non-interactive key exchange protocols.

B. Proposed Approach

This paper proposes a public key establishment scheme which will provide a fundamental key management support for BSP of space DTNs. This involvs two stages one is a bootstrap stage and another is exchange stage. We prefer to use pre-authentication mechanisms to bootstrap the secure contexts for BSP secure communications. At bootstrapping stage, by using two-channel cryptography [1] techniques, the authentication information comes directly and demonstratively from their owners via authenticated OOB channels, and then the legality of this information can be checked easily. In addition to initiating and bootstrapping as above described, the DTN nodes need to exchange and update their public keys periodically in the future life of the network. In the proposed scheme, the network nodes implement this process according to schedule. The protocol will work in the following manner.

1) The sender, Xi, displays its identity as IDi and the current time t to its public key PKi ,and then sends the result PKi-Idi at time *t* to the receiver Yj over a broadband insecure channel.
2) The sender, Xi computes hash value as h = H(PKi-0IDi-t);
3) The sender, Xi, sends the authentication information for its public key, i.e., h, to the receiver Yj over the narrowband channel which is authenticated.
4) While receiving the public key PKi-Idi at time t and the authentication information h for this public key from Xi over the traditional channel and the OOB channel respectively, the receiver Yj accepts PKi as the public key of Xi if t is the correct timestamp and h_ = H(PKi-Idi-t_) otherwise, reject it.

Here, H is a collision resistant hash function.

In addition to this for identifying Geographic position Pi (t) the space-time graph is constructed. And for deciding the nodes at what time and to whom the public key is to be sent the time-evolving geography positions of nodes plays very important role. Fortunately, the geography position of a node Xi at time t, Pi (t), is predictable in space DTNs, because the positions of ground based network nodes are known and the celestial bodies have predictable motion as well.

IV. Conclusion And Future Work

In this paper, by using the two-channel cryptography And non-interactive public key exchange protocol is given, in order for establishing secure context to support for BSP of space DTNs and replacing the traditional application of PKI or other key exchange mechanisms. In the proposed protocol, the space-time graph is also utilized for modelling and predicting the property of space networks. So the key exchange becomes scheduled. As coming towards future work the designing usable and secure OOB channels for space DTNs is an interesting, challenging and valuable future work.

Acknowledgment

The proposed system is based on IEEE Transaction paper under the title “Non-Interactive Key Establishment for Bundle
Security Protocol of Space DTNs” published in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014.

References

[1] A. Mashatan and D. Stinson, “Practical unconditionally secure two channel message authentication,” *Designs, Codes Cryptogr.*, vol. 55, no. 2, pp. 169–188, 2010.

[2] Delay Tolerant Networking Research Group, http://www.dtnrg.org/

[3] S. Farrell, S. Symington, H. Weiss, “Delay-Tolerant Networking Security Overview” draft-irtf-dtnrg-secoverview- 01.txt, March 2006, work-in-progress.

[4] NASA. (2012). *Nasa Disruption Tolerant Networking (DTN) Project*, Washington, DC, USA [Online]. Available: http://www.spacecomm.nasa.gov/spacecomm/programs/technology/dtn/

[5] S. Symington, S. Farrell, H. Weiss, “Bundle Security Protocol Specification” draft-irtf-dtnrg-bundle-security- 01, March 2006, work-in-progress.

[6] T. Berners-Lee, R. Fielding, and R. Fielding. *Uniform Resource Identifier (URI): Generic Syntax*. STD 66. Reston, Virginia: ISOC, January 2005.

[7] W. Van Besien, “Dynamic, non-interactive key management for the bundle protocol,” in *Proc. 5th ACM Workshop Challenged Netw.*, 2010, pp. 75–78.

[8] A. Mashatan and D. Stinson, “Noninteractive two-channel message authentication based on hybrid-collision resistant hash functions,” *IET Inf. Sec.*, vol. 1, no. 3, pp. 111–118, 2007.

[9] Cerfv. Burleighs. HookeA etal, Delay-Tolerant Netowrk Architecutes. IETF RFC4838. Informational 2007.

[10] Kate, G. Zaverucha, and U. Hengartner.Anonymity and security in delay tolerant networks. *In SecureComm, 2007.*

[11] CCSDS, “Rationale, scenarios, and requirements for DTN in space,” CCSDS, Reston, VA, USA, Inf. Rep. CCSDS 734.0-G-1,Aug.2010.