RESEARCH ARTICLE OPEN ACCESS

Bundle Security Protocol of Space DTNs Using Cryptographic Algorithm

E.Mukundhan[1], MTech, Mr.R.Veeramani,M.E (Assistant Professor)[2]
Department of Computer Science and Engineering,
SRM University, Ramapuram Campus,
Chennai-600089

----------**********----------

ABSTRACT

The abstract of this paper is to asure the authenticity, integrity, and confidentiality, the in-transit Protocol Data Units of bundle protocol (BP) in space delay/disruption tolerant networks (DTNs), the Consultative Committee for Space Data Systems bundle security protocol (BSP) specification declares four IP sec style security headers to provide four aspects of security services. In any way, this specification leaves key management as an open problem. Aiming to apply the key establishment issue for Bundle Protocol, in this journal, we utilize a time-evolving topology model and two channel cryptography to design efficient and non interactive key exchange protocol . A time-evolving model is used in formal manner model the periodic and set in advance behavior patterns of space DTNs, and therefore, a system can schedule when and to whom it should send its public key. Meantime, the application of two-channel cryptography enables DTN nodes to replace their public keys or revocation status information, with authentication assurance and in a non interactive manner. The proposed scheme helps to establish a secure environment to defend for BSP, tolerating high delays, and unexpected loss of connectivity of space DTNs.

Keywords: - **Bundle Security, Delay Tolerant Network, Key Management, Time Evolving Network**.

----------**********----------

1. INTRODUCTION

On Internet today we depend on many security mechanisms and applications for immediate end-to-end reach ability. But, in the space-net this theory never holds true, because the space internet, which is realized as a type of Delay/disruption Tolerant Networks (DTNs), is content to a high delay and unexpected loss of connectivity. Accordingly, the existing conventional Public Key Infrastructure (PKI) and online negotiation-based key distributing protocols are not applicable. In this paper, we target to design non-interactive key exchange protocols on which other security mechanisms are built, by utilizing two-channel cryptography joined with the predictable contacts of space DTNs.

SPACE DTNs

DTN architecture as a generalized store-and-forward network overlay, which is applicable to inter-planetary communicating environments. This architecture initiates from NASA JPL's experiences in developing store-and-forward communication networks for deep space. This type of networks receives by high delays and frequent disconnectivity. The work for DTNs is still in build. Currently, the architecture for a DTN is defined basis on the store, carry and forward technology.

SECURITY FOR SPACE DTNs

Security is an important view for space DTNs. The particular environment of the underlying networks over which the BP operates, makes it essential for a DTN to be defended from attacks or unauthorized operations. This constrained environment makes unique challenges to the secure mechanisms applying to BP. Additionally, space DTNs may be deployed in environments where some hops or links might become compromised.

The specification presents four IPsec style security headers that can be appended to bundles, directing to provide four facts of security services. The Bundle Authentication Block (BAB) provides authentication for single hop by adding a Message Authentication Code (MAC) to each bundle. The Payload Integrity Block (PIB) is used to allow for authentication for the payload from the source, which produces the PIB, to the destination, which verifies the PIB authenticator. Any node on the path between the source and the destination can verify the authenticity of a bundle via its PIB, if this node has verify this bundle which access to the public key and revocation status information.

2. RELATED WORKS

KEY MANAGEMENT

Herewith, high delays and unexpected loss of connectivity, an interactive protocol does not work well in space DTNs. This motivates a pattern of non-interactive key exchange protocols in an authenticated manner. The two-channel cryptography and OOB channels have an advantage to designing a non-interactive message authentication protocol, which we use to enable two DTN nodes to securely exchange their public keys (or revocation status information).

The main concept is to exchange a public key, that may be long term, on the normal channel, and independently calculate a cryptographic hash value from public key. Hash value is then transmitted from one device to the other over the OOB channel, in order to verify that the public key exchanged on the normal channel has not been altered. Because of only processing at security-aware nodes, i.e., a "single hop" from a security-aware forwarder to the next security-aware intermediate receiver, an authenticated OOB is easily achieved. In Accordance with, by utilizing two-channel cryptography, public keys can be authenticated between a forwarder and the next intermediate receiver, if it is needed.

EQUATIONS

Here we consider a space node Si that possesses the public key PKi and performs the public key exchange protocol. This protocol enables Si to securely send its public key PKi to another node Sj which is reachable in one hop for Si. In more detail, the protocol is performed as follows:

1) The sender, Si , appends its identity I Di as well as the current time t to its public key PKi , and thereafter sends the result PKi ‖I Di ‖t to the receiver Sj over a broadband insecure channel (a traditional channel);

2) The sender, Si , computes h = H(PKi ‖I Di ‖t);

3) The sender, Si , sends the authentication information for its public key, i.e., h, to the receiver Sj over the narrowband authenticated channel (often OOB channels);

4) When receiving the public key PK`i ‖ I D`i ‖t` and the authentication information h` for this public key from Si over the traditional channel and the OOB channel respectively, the receiver Sj accepts PKi as the public key of Si if t` is the correct timestamp and h` = H(PK`i ‖ I D`i ‖t`); otherwise, reject it.

3. EXISTING WORK

Here, the existing issues, how a public key is made generally-available, how its revocation status information is well known timely, and how the public key is updated if this is needed are not handled properly.

The existing negotiation-based security protocols, do not work well, because these protocols need to exchange certificates in multiple rounds on line and agree on certain cryptographic algorithms as well as security parameters. However, this is not always achievable, since the end-to-end path connection in DTNs is subject to a high delay and unexpected, frequent disconnectivity. The few works presenting solutions to DTN key establishment have largely focused on targeted networking environments.

We consider the problem of routing in emerging wireless networks where nodes move around explicitly carrying messages to facilitate communication in an otherwise partitioned network. The absence of a path at any of the instant of time between a source and destination makes the traditional mobile ad hoc routing protocols unsuitable for these networks. Anyhow,the explicit node movements create paths over time.

4. PROPOSED SCHEME

The current BSP is built on the assumption that the DTN nodes already have access to authenticated copies of each other's public keys. That is, the DTN nodes know who they are connected. This assumption can be achieved by combining pre-authentication with periodic key exchange via channels. We propose our public key establishment scheme which will provide a fundamental key management support for bundle security protocol. Thus by using the RSA techniques we encrypt and decrypt the files by which we upload the files to the local servers and store the encrypted files. Then we compress the files and make them as a single file. Then we share the file to the network systems which are present in the network .Thus the files are easily transferred and the respected key are easily transferred.

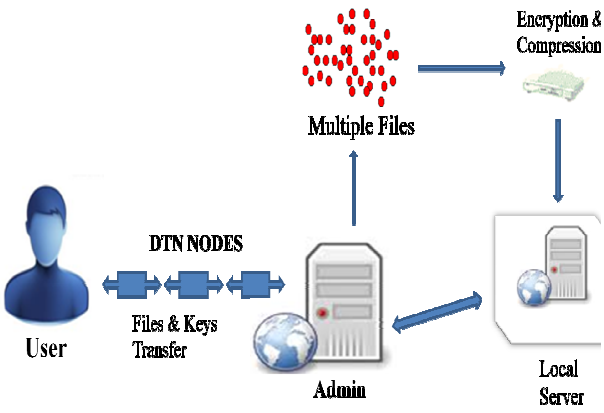

Fig.1. System Architecuture

BUNDLE SECURITY PROTOCOL

The Bundle Protocol (BP) is used in DTNs which overlay multiple networks. The objective of BP is to support interoperability across such restricted networks. It enables an application in one network to communicate with an application in anyother network, both of which are overlayed by DTNs. The in-transit PDUs (Protocol Data Unit) of DTNs, also named bundles, can be sent over an exist link and buffered at the next node until the next link in the path appears.

The Extension Security Block (ESB) provides protection for non-payload-related portions of a bundle, such as the bundle metadata that might specify the kind of data in the payload but not the actual payload detail. It is typically used to apply confidentiality protection and placed in the bundle in the same position as the block being protected. While reference implementations of the BP security have become available, key management (including public key management) in particular remains an open issue.

ENCRYPTION

The admin convert the plain text into cyper text using RSA Algorithm. The public key can be shared with everyone, whereas private key must be kept secret. In RSA algorithm, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA Cryprography has become the most widely used asymmetric algorithm: It provides a method of assuring the integrity, confidentiality, authenticity and non-reputability of electronic communications and data storage.

TIME EVOLVING NETWORK

We use time-evolving topology model and two-channel cryptography to design efficient and non-interactive key exchange protocols. A time-evolving model is utilized to formally model the periodic and predetermined links of space DTNs, such that a node is able to schedule when and to whom it should send its public key. Furthermore, the application of two-channel cryptography allows DTN nodes to exchange their public keys or revocation status information with authentication assurance and in a noninteractive manner. In this way, security mechanisms of BSP can achieve the support of generally-available public keys.

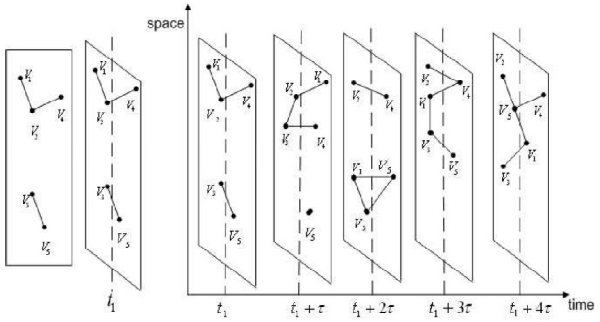

Fig.2. Time Evloving Graph

In a time-evolving network model, a sequence of static graphs is needed to model this type of networks. As shown in Figure, each static graph is a snapshot representing nodes and the contacts between them at a certain moment. In this diagram there is no end-to-end path between some node pairs at one time-step, and the network is not connected at some time-steps as well. Then, the dynamic network with a sequence of snapshots is able to describe the evolution of the topology and the node mobility over a period of time.

5. RSA KEY PAIR ALGORITHM

There are two main properties are essential. First, the authenticity of a signature generated from a fixed file and fixed private key can be verified by using the corresponding public key. Second, that should be computationally infeasible to generate a valid signature for a user without knowing that user's private key. A digital signature is an authentication that enables the creator of message to attach a code that act as a signature. It is produced by taking the hash code of message and encrypting the message with creator's private key.

A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A pairing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

6.CONCLUSION AND FUTURE WORK

In this paper, by exploiting the two-channel cryptography we have given a public key exchange protocol, in order for establishing secure environment to support for BSP of space DTNs and replacing the application of PKI as well as other negotiation-based key exchange mechanisms in this type of networks.The space-time graph is utilized to model the predictable property of space networks. This makes the key establishment process scheduled and not opportunistic. Designing usable and secure Out Of Band channels for space DTNs is an interesting and valuable.

7.REFERENCES

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

[02] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, “Delay-tolerant networking architecture,” in Proc. RFC, Apr. 2007, pp. 1–4.

[03] S. Symington., S. Farrell, H. Weiss, and P. Lovell, Bundle Security Protocol Specification. Washington, DC, USA: IRTF, May 2011.

[04] S. Farrell and V. Cahill, “Security considerations in space and delay tolerant networks,” in Proc. 2nd IEEE Int. Conf. SMCIT, Mar. 2006, pp. 1–8.s

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

[06] Z. Jia, X. Lin, S. Tan, L. Li, and Y. Yang, “Public key distribution scheme for delay tolerant networks based on two-channel cryptography,” J. Netw. Comput. Appl., vol. 35, no. 3, pp. 905–913, May 2012.

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

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