Wireless Sensor Network, **2010, 2, 645-648**
doi:10.4236/wsn.2010.28076 Published Online August 2010 (http://www.SciRP.org/journal/wsn)

Considerations and Open Issues in Delay Tolerant Network'S (DTNs) Security

Harminder Singh Bindra, Amrit Lal Sangal
Department of Computer Science and Engineering, *NIT Jalandhar*, *Punjab*, *India*
E-mail: *bindra.harminder@gmail.com*
Received April 10, 2010; *revised May* 21, 2010; *accepted June* 2, 2010

Abstract

Delay Tolerant Network (DTN) addresses challenges of providing end-to-end service where end-to-end data forwarding paths may not exist. Security and privacy are crucial to the wide deployments of DTN. Without security and privacy guarantees, people are reluctant to accept such a new network paradigm. To address the security and privacy issues in DTNs, we in this paper have discussed the various open issues and challenges which need to be addressed to evolve the secure DTNs.

Keywords: Delay Tolerant Network, Routing, Security, Cryptography

1. Introduction

A delay tolerant network is a newly emerging network [1], which usually deals with communications in extreme challenging environments, such as space communications and networking in sparsely populated areas [2], vehicular ad hoc networks [3,4] and underwater sensor networking [5]. In these environments, the continuous end-to-end paths between the source and the destination are usually unguar anteed.

The work of DTN is still in progress [6]. Currently, the architecture for a delay tolerant network is defined based on the store, carry and forward paradigm [1]. The key part in this paradigm is the bundle protocol, which is described by DTN architectures [7] and bundle protocol specifications [8].

2. Architecture of DTN

RFC 4838 points out some fundamental assumptions built into the Internet architecture that are problematic in DTNs [7]:

1) An end-to-end path between the source and destination exists for the duration of a communication session.

2) Retransmission based on timely and stable feedback from data receivers is an effective means for repairing errors (for reliable communication).

3) End-to-end loss is relatively small.

4) All routers and end stations support the TCP/IP protocol suite.

5) Applications need not worry about communication performance.

6) End-point-based security mechanisms are sufficient for meeting most security concerns.

7) Packet switching is the most appropriate abstraction for interoperability and performance.

8) Selecting a single route between sender and receiver is sufficient for achieving acceptable communication performance.

The DTN architecture relaxes most of these assumptions—it uses variable-length messages as the communication abstraction and a naming syntax that supports a wide range of naming and addressing conventions to enhance flexibility. It's designed to use storage within the network to support store-and-forward operation over multiple paths and potentially long timescales, and not to require but to support end-to-end reliability. The DTN architecture envisages security mechanisms that protect the infrastructure from unauthorized use by allowing for policy-based discarding of traffic as quickly as possible. The DTN architecture also assumes roughly synchronized clocks [9]. The DTN overlay network specifies a bundle protocol which is layered on top of a "convergence layer", which is itself on top of other lower layers. The DTN Bundle Protocol [DTNBP] describes the format of the messages (called bundles) passed between DTN bundle agents that participate in bundle communications to form the DTN store-and-forward overlay network [10].

3. Security in DTN

The possibility of severe resource scarcity in some DTN dictates that some form of authentication and access control to the network itself is required in many circumstances. It is not acceptable for an unauthorized user to flood the network with traffic easily, possibly denying service to authorized users. In many cases it is also not acceptable for unauthorized traffic to be forwarded over certain network links at all.

Several goals are established for the security component of the DTN architecture:

1) Promptly prevent unauthorized applications from having their data carried through the DTN

2) Prevent unauthorized applications from asserting control over the DTN infrastructure

3) Prevent otherwise authorized applications from sending bundles at a rate or class of service for which they lack permission

4) Promptly discard bundles that are damaged or improperly modified in transit

5) Promptly detect and de-authorize compromised entities

Most network security methods attempt to mutually authenticate user identities and the integrity of messages, but do not attempt to authenticate routers that forward information. In DTNs, forwarding nodes (routers and gateways) are also authenticated, and sender information is authenticated by forwarding nodes, so that network resources can be conserved by preventing the carriage of prohibited traffic at the earliest opportunity.

In the public key cryptography, for example, each user has a private key and public key pair. A certificate is a file, digitally signed by a certificate Authority (CA), confirming the user's identity and containing a conformed copy of the user's public key. In DTN, both user and forwarding nodes have key-pair and certificates and the certificates of the users also indicate their class of service (CoS) rights. Sender can sign their bundle with their private key, producing the bundle specific digital signature. This signature allows receiver—using the sender public key—to confirm the authenticity of the sender, the integrity of the message, and the sender's CoS rights.

Using public key cryptography as an example, the security steps are [9]:

1) The source sends its bundle, together with its bundle specific signature, to an adjacent forwarding node. If that node does not already have a copy of the sender's certificate, it obtains one from the sender or a CA.

2) The forwarding node that first receives the sender's bundle (shown below as Adjacent Router or Gateway) verifies the senders identity and CoS rights, using its stored copies of adjacent-user certificate and CA public keys (shown below as User Lists). Then the forwarding node replaces the sender's signature with its own signature (shown below as Router's Signature) and forwards the information.

3) Each subsequent forwarding node verifies only the identity of the previous forwarding node, using its stored copies of adjacent-router certificate and CA public keys (shown below as Router List). Then it replaces prior node's signature with its own signature and forwards the information.

4. Open Issues in Delay Tolerant Networks

This section discusses some of the issues which are still very open, either due to a lack of consensus in the DTNRG, or due to there being areas (like DTN key management) where much basic research remains to be done.

4.1. Key Management

The major open issue in DTN security is the lack of a delay-tolerant method for key management. We are at the stage where we only really know how to use existing schemes, which ultimately require an on-line status checking service or key distribution service which is not practical in a high delay or highly disrupted environment.

The only generally applicable schemes we currently have are basically equivalent to shared secrets or else irrevocable public key (or certificate based) schemes. Clearly, this is an area where more research work could produce interesting results.

4.2. Handling Replays

In most networking scenarios, we either wish to eliminate or else dramatically reduce the probability of messages being replayed. In some DTN contexts this will also be the case—particularly as replaying a (e.g., authenticated, authorized) message can be a fairly straight forward way to consume scarce network resources.

The element of delay in DTNs also complicates handling replays. Replay detection schemes generally depend on noting some unique aspect of messages (via digesting of some message fields) and then keeping a list of (the digests of) recently seen messages. The problem in the DTN context is the "recently seen" part of such replay detection algorithms, since maintaining a list for say 30 days would be fairly resource intensive, but might be required if latencies are of that size. So the most obvious ways to protect against replays are problematic.

The result is that the extent to which we can, or should, define a generic DTN replay detection scheme is hard to determine and at this point remains an open DTN security issue.

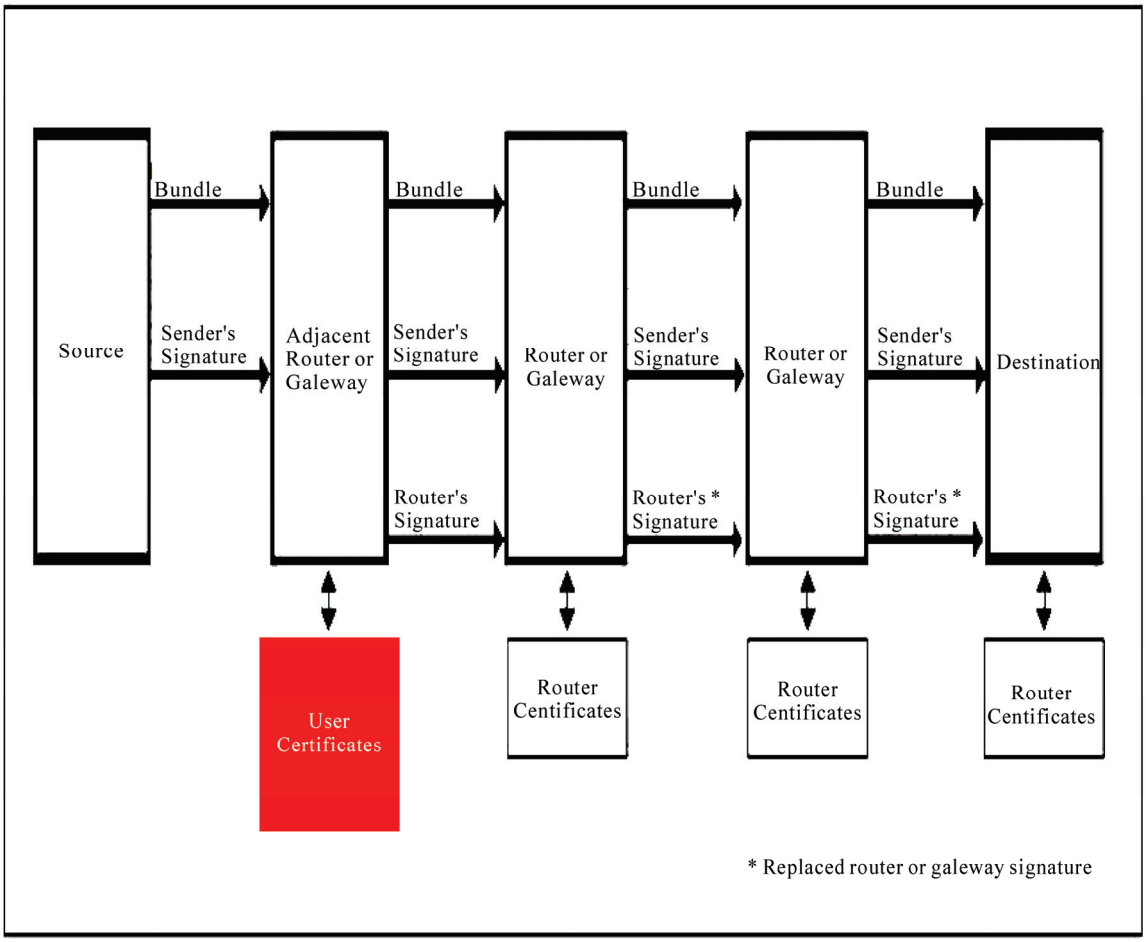

Figure 1. Security steps using public key cryptography [9].

4.3. Traffic Analysis

A general traffic analysis protection scheme is probably not, in any case, a realistic goal for DTNs, given their tendency to be resource-scarce and there have been no calls for a generic approach to this problem. However, for some disruption tolerant networks, hiding traffic (e.g., the existence of a signal from a sensor net) may be a very important security requirement. So, the first open issue here is the extent to which there is a real need for a generic scheme for protection against traffic analysis. If there were, then the second open issue is how to define such a scheme to be delay and disruption tolerant and which also doesn't consume too many resources. Finally, traffic analysis protection may be left as a local matter for the underlying network layers.

4.4. Routing Protocol Security

DTN routing protocol security must clearly be in our list of open issues. However, if a putative DTN routing protocol was to use either the Bundle protocol or LTP, it could clearly make use of their existing security features.

The security mechanism proposed for metadata blocks has been generalized for other non-payload blocks and may provide a solution to some of these issues.

4.5. Multicast Security

Within DTN, there is currently no mechanism defined for restricting which nodes may register in a "multicast" or "anycast" endpoint. The security architecture currently does not address the security aspects of enabling a node to register with a particular multicast or anycast EID. Without a capability to restrict the registration of nodes in multicast or anycast endpoints, any node may register in such an endpoint and thereby receive traffic sent to that endpoint. In addition, even though an endpoint may be a singleton endpoint, meaning that it is not permitted to contain more than one node, it may be possible for a second (or more) node to register in a singleton endpoint and receive bundles that are sent to that endpoint if the bundles are routed in such a way that they are forwarded to that node (e.g., using flood routing).

Modifications to the mandatory end-to-end(ish) ciphersuites or additional ciphersuites would need to be defined to provide the possibility that a bundle could be encrypted or authenticated differently for different nodes in its multicast or anycast endpoint.

In a DTN, registering in a multicast endpoint may be more akin to signing up to a mailing list, so that bundles that originated before the registration occurred may be received afterwards. In principle, such a late registering node might get sent the entire mailing list archive either by design or in error. Even if some sort of mechanism to authenticate registering nodes were to be defined, there are still issues that arise out of the fact that the endpoint registration process may itself be lengthy.

4.6. Performance Issues

Provision of security within a DTN imposes both bandwidth utilization costs on the DTN links and computational costs on the DTN nodes.

The provision of DTN security will consume additional bandwidth. The amount consumed depends on the way optional parameters are encoded, or not, and on the cryptographic algorithms used. In addition, if more than one security service is used for the same bundle (e.g., a MAC to be removed by the next hop and a signature for the final destination) more of the possibly limited amount of bandwidth available for security purposes will be used.

The use of DTN security also imposes computational costs on DTN nodes. There may be limits regarding how much CPU can be devoted to security and the amount of computation will depend on the algorithms used and their parameters.

5. Conclusions

In this paper we have introduced DTN and some of the open issues in the Delay Tolerant Network's Security. This paper can serve a guiding path to the researcher to find the open issues and the areas which needs to be researched in the security of DTN.

6. References

[1] K. Fall, "A Delay Tolerant Networking Architecture for Challenged Internet," In: *Proceedings of the* 2003 *conference on applications, technologies, architectures, and protocols for computer communications*, *SIGCOMM*' 03, Karlsruhe, 2003, pp. 27-34.

[2] A. Kate, G. Zaverucha and U. Hengartner, "Anonymity and Security in Delay Tolerant Networks," *The* 3*rd International Conference on Security and Privacy in Communications Networks and the Workshops*, Secure Communication, September 2007, pp. 504-513.

[3] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen, "Security in Vehicular Ad Hoc Networks," *IEEE Communications Magazine*, 2008, Vol. 46, No. 4, pp. 88-95.

[4] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," *The* 27*th IEEE International Conference on Computer Communications*, INFOCOM 2008, Phoenix, 15-17 April 2008.

[5] J. Cui, J. Kong, M. Gerla and S. Zhou, "The Challenges of Building Mobile Underwater Wireless Networks for Aquatic Applications," *IEEE Network*, Vol. 20, No. 3, 2006, pp. 12-18.

[6] Delay Tolerant Networking Research group, November 2008. http://www.dtnrg.org

[7] V. Cerf, *et al.*, "Delay-Tolerant Network Architecture, IETF RFC 4838, Informational," April 2007. http://www.ietf.org/rfc/rfc4838.txt

[8] K. Scott and S. Burleigh, "Bundle Protocol Specification, IETF RFC 5050, Experimental," November 2007. http://www.ietf.org/rfc/rfc5050.txt

[9] A. McMahon and S. Farrell, "Delay- and Disruption-Tolerant Networking," *IEEE Internet Computing*, Vol. 13, No. 6, 2009, pp. 82-87.

[10] F. Warthman, "Delay-Tolerant Networks (DTNs) A Tutorial." http://www.dtnrg.org/March 2003

