ID Based Cryptography and Anonymity in Delay/Disruption Tolerant Networks

Naveed Ahmad, Haitham Cruickshank, and Zhili Sun

Center for Communication Systems Research, University of Surrey
Guildford, Surrey, UK
{n.ahmad,h.cruickshank,z.sun}@surrey.ac.uk

Abstract. Due to the rapid development in technology, every network, application needs full time connectivity without disruption and delays. The Delay/Disruption Tolerant Networking (DTN) concept is suitable for applications such as rural and disaster areas networks, animal and environmental monitoring plus others. However, due to the shared and unsecured nature of such challenged networks a good cryptographic framework needed in DTN. Identity Based Cryptography (IBC) compares favorably with traditional public key cryptography while generating public key on a fly as required. In this paper, we will provide anonymity solution in DTN using IBC. This has the advantage over public key cryptography with respect to end-to-end confidentiality. Also we use pseudonyms to provide anonymity and hide the identity of the end user.

Keywords: Delay Tolerant Network Security, Identity Based Cryptography, Anonymity, Pseudonyms, Public Key Cryptography.

1 Introduction

The Internet TCP/IP protocol stack networks works normally when end-to-end connectivity is available and the round trip time is relatively small. To explain the problem with TCP in certain applications we take the scenario of interplanetary communications. If a node on earth wants to send data to space (or another planet) then it must go through the process of three way handshake. In addition to that if there is no communication for few minutes between two nodes then the TCP will assume time out. If we consider the data transfer between the earth and nearest planet then it will take approximately 24 minutes to reach data and TCP will definitely fail.

A Delay/Disruption Tolerant Network (DTN) is an overlay on top of regional networks including the Internet. The DTN architecture consists of a network of independent networks each characterised by Internet-like connectivity within, but having occasional communication opportunities among them. Connectivity can be scheduled and sometimes random. These independent networks form the DTN regions and are connected through a system of DTN gateways. Each DTN region relies on its own protocol stack that best suits its communication means, infrastructure and technologies. At the DTN nodes, a new layer, called the bundle layer, is added on top of the traditional transport layers to provide end-to-end data transfers among the DTN regions. The DTN overlay architecture operates above the existing protocol stacks

K. Sithamparanathan et al. (Eds.): PSATS 2010, LNICST 43, pp. 265–275, 2010.

found in other network architectures [1], [2]. DTN [3] supports heterogeneous environment and is based on idea of store and forward method. Its architecture with the help of the bundle layer supports heterogeneity of networks. In DTN, data is sent in the form of bundle through store and forward relay. Bundle protocol [4] is working as communication medium which defines rules for bundle. Figure-1 shows the layer stack of DTN where Internet is used to facilitate communication between two DTN regions. However DTN can be used for other network apart from Internet. DTN gateways are intelligent to handle different transport, network and data link layers.

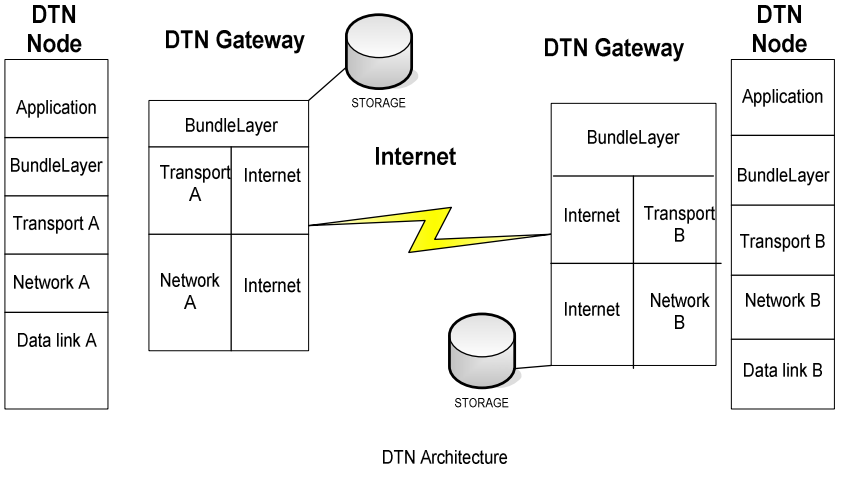

Fig. 1. DTN Layer Stack

In addition to space applications, DTN can be implemented in many applications [3] e.g. such as water pollution monitoring, disaster monitoring and telemedicine in rural areas. Apart from these, DTN can also support traditional applications such as Web cache, Emails and file transfer. Some applications need classification of their data as top secrete, secrete, confidential and unclassified in order to enforce security and hiding of data from intruders. However our scenario will focus on telemedicine application in rural areas. This is applicable to other rural area scenarios as well. Figure 2 depicts our scenario and will be used as a framework for our solution:

- A local doctor wants to send a patient (e.g. a village elder) medical data to a senior doctor in a main hospital in Europe for evaluation of the patient's condition. There is no communications connectivity in this rural village. So public buses can be used as part of the communications transport chain.
- The medical data is stored on the bus and then transferred to the rural area gateway (DTN gateway-1). The data will be stored until the availability of a transmission link (e.g. satellite or wireless) to the Internet.
- The bundle is passed through Internet routers to the Internet Service Provider (ISP) gateway and delivered to the hospital network gateway (DTN Gateway-2). The medical data is then transferred to the hospital local server, where the senior doctor can examine it.

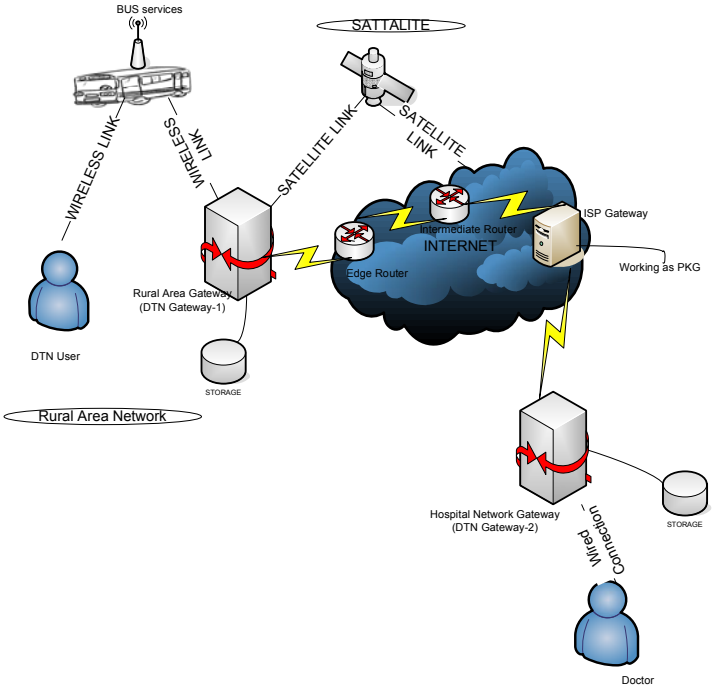

Fig. 2. Telemedicine scenario in rural area network

- We assumed that segmentation of the user (patient) data is performed according to the access technology (satellites, wireless and wired LAN) requirements in the DTN gateways.

This scenario shows a strong need for medical data security and patient identity privacy (anonymity). However achieving security and anonymity in such challenging network is a difficult task. Passive threats are major concern due to the broadcast nature of satellite, where an intruder can easily monitor the user sensitive data. Also there is possibility that intruder might gain access to the local buses stored information.

2 Security Requirements for DTN

Traditionally, security can be achieved through cryptographic functions by providing confidentiality, integrity and authentication. But due to disconnected nature of DTN, traditional cryptography is not an optimal solution. Researchers had tried to implement Identity Based Cryptography (IBC) as an alternative to traditional security techniques. Currently, the DTN related security work is focused within the DTN Research Group (DTNRG) and Internet Research Task Force (IRTF) [5], [6]. While designing security architecture, it is important to minimize the message exchanges between DTN nodes.

Another important consideration is the minimum contact with Trusted Authorities: DTN is opportunistic network, so there is no permanent connectivity among the nodes so one should take in to account that minimum interaction should be done with trusted authority, which, in case of public key cryptography is the Certification Authority (CA) which issues certificates and its equivalent the Public Key Generator (PKG) in IBC.

Current security protocols do not perform well in high delay/disruption conditions, because of underlying assumption 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 [7], [8], [9]. The current security architecture supports hop-by-hop and end-to-end authentication and integrity validation, to ensure data is corrected before forwarding. The hop-by hop authentication/integrity is achieved 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. Similarly 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 [8].

However, the current work in DTNRG does not address user anonymity and identity hiding. Therefore, in this paper we focus on user anonymity and provide IDC based mechanisms to hide the identity of the sender and receiver.

3 Public and Identity Based Cryptography

Cryptography can be divided into symmetric key cryptography (same key used for encryption and decryption) and asymmetric key cryptography (different keys are used for encryption and decryption) [11]. Public key cryptography is mostly attributed to Diffie, Hellman, Rivest, Shamir and Adleman [11]. To use traditional cryptography Public Key Infrastructure (PKI) provides a framework which provides foundation for other security services. It is used in many applications such as; e-voting, e-banking and e-commerce. PKI supports security building blocks such as confidentiality, authentication, integrity and non-repudiation. The primary goal of PKI is to allow the distribution of public keys and certificates and also binding them in a secure manner [11]. In case of challenged networks (such as DTN), PKI works well in authentication and integrity aspects, but to achieve confidentiality sender requires the receiver public key to encrypt data and also checking of Certificate Revocation List (CRL) for compromised keys [12]. As such, these functions require connection availability to the CA, which is not always possible as shown in our scenario (Figure 2).

To overcome the shortcomings of public key cryptography Shamir proposed the topic of Identity Based Cryptography (IBC) in 1984 [13]. In this new cryptographic approach, user identifier information such as email address, phone number, IP address are used instead of certificates as a public key for encryption and verification of digital signature [14], [15]. In PKI, the authority which manages certificates was CA and in IBC, the Public Key Generator (PKG) is the central authority which generates private key for participants. IBC can work with exiting public key cryptographic systems e.g. RSA, DSS. The PKG is shown in Figure 2 and it is assumed to be co-located with the ISP gateway.

IBC work in the following steps:

- **System setup: -** PKG generates its own private key S_{pkg} from security parameters pp (where PP is system wide parameters.).
- **Encryption: -** sender encrypts the message with the receiver public key $P_{receiver,}$ generated from ID of receiver.
- **Key extraction: -** PKG generates private key $S_{receiver}$ for receiver from his ID, security parameter pp and its own S_{pkg} as input.
- **Decryption: -** receiver applies its private key and can decrypt message.

Shamir only implemented digital signature in his early work and later on Boneh and Franklin [16] implemented encryption as well.

The disconnected nature of DTN can cause a problem in the PKI framework, where the sender needs the receiver certificate and public key when it wants to send data. IBC can solve some of the DTN security issues. IBC has no significant advantage in authentication and integrity but it works well in confidentiality [17]. To achieve integrity and authentication in IBC Seth et al [17] suggested the avoiding of Certificate Revocation List (CRL) and proposed periodic refreshing of underlying identifier information e.g. *alice@hotmail.com 12-10-2009* is refer to Alice key whose validity is till 12th October and the receiver can verify to look into the date. However this was challenged by S.Farrell [18] and argued that verifying Certificate from CA is similar to checking public parameter in IBC in DTN. But actually that parameter is long lived and no need to checked frequently.

4 Pseudonyms and Anonymity

One way of providing anonymity (identity hiding) is by using Pseudonyms. Pseudonym means falsely named (name other then the real name) and can used as an identifier of entity/node. It is created by the entity/node itself. There are four kind of pseudonym unlinkability [19]:

- **Public pseudonyms:** Linking between the subject and pseudonym are known publicly from beginning. e.g. name with phone number kept in public directory.
- **Initially non public pseudonyms:** This type limits its identity to certain parties. e.g. name with account number known by bank only.
- **Initially unlinked pseudonyms:** This provides high level of privacy and the pseudonym is known to the entity itself only.
- **Pseudonyms as public Key:** A digital pseudonym is a public key used to verify signature made by the anonymous subject of the corresponding private key [20]. This approach is also used in mobile ad hoc network (MANETS).

Encryption hides the data transmission from attackers. However sender and receiver identity, network address, packet length and packet timing (RTT) can provide useful information to adversaries to achieve traffic analysis attacks. So this gives rise to the idea of identity hiding and anonymity. The research on anonymity is dated back to the

paper [20] by D Chaum's. The term anonymity according to [21] "Is state of being not identifiable within a set of subjects". Types of anonymity can be defined as:
Sender anonymity: - To hide the originator of the message.
Receiver Anonymity: - That the adversary can't determine the intended receiver if the message.
Unlinkability: - To hide the association of sender and receiver.

Anonymity is required in many applications e.g. e-voting, digital cash, electronic email, news reporting, telemedicine and many more. To achieve anonymity researchers define anonymous protocols that focus on initiator/sender and receiver/recipient anonymity plus their unlinkability (who is with whom). Anonymous protocol should prevent message coding attack, timing attack, message volume attack, flooding attack, intersection attack and collusion attack [20]. To achieve anonymity there should some rule what we called Anonymous Communication Protocol (ACP). Generally most of the ACP are based on idea of Mixes Network by David Chaum's and onion routing [21],[22]. Table 1 shows different ACPs in term of some performance metrics.

Table 1. A survey of Anonymous Communication Protocol (ACP)

Protocol	Sender Anonymity	Receiver Anonymity	Unlink-ability	Discipline	Latency
TOR	Yes	Yes	Yes	Internet	Low
Tarzan	Yes	No	No	Peer-to-Peer	Low
Crowds	Yes	No	Yes	Web surfing	Large
Cypherpunk (Remailer-1)	No	Yes	Yes	Email	Large
Mixmaster (Remailer-2)	Yes	No	Yes	Email	Large
Mixminion (Remailer-3)	Yes	Yes	Yes	Email	Low

Above all discussed protocols either use the idea of onion routing or mix networks, and provides anonymity at some level. 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 [23]. In DTN, there is no complete routing topology so Onion Routing (OR) doesn't work because OR needs to know the route in advance and encrypt the message accordingly for each router. Mix networks can be applied on DTN as they hold

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.

5 DTN Anonymity Protocol Design

Our proposed protocol is based on IBC and Pseudonyms, where encryption, decryption, digital signature and keys are generated using IBC. The identities of users were hided through the use of pseudonyms. Each entity uses its email address as ID (for example) and generates a public key. The PKG generates private keys for each participating entity using its own secret key and security parameters pp. Considering our scenario (Figure-2), the DTN user (local doctor/patient) from rural area network wants to send medical data to a senior doctor in a major city hospital. However, we want to keep the sender and receiver identity hidden from intruders.

5.1 Assumptions

1. Sender and receiver know each other identities but unknown to other entities.
2. The PKG requires only once the identity of user to generate the private key. After that it stored the identity in the database and update with the date and time.
3. Once the entity received the key pairs, there is no need to interact with PKG anymore. and can send data to other entity.
4. The keys are distributed securely through traditional mechanisms such as Secure Socket Layer (SSL) to each entity. This key distribution is out of scope for this paper.
5. The DTN gateways are trusted. In our proposed solution, anonymity is achieved through the use of pseudonyms which allow DTN routers/gateways to know that the Pseudonym is belonging to the valid authenticated user without unveil his identity.
6. There is security association between each entity and their corresponding gateway. The pseudonym generated by each entity is securely send to gateway, where it stored in the persistence storage.
7. There is secure channel between both gateways where they exchange both the pseudonyms handed by the end entities, so that gateway-1 send the pseudonyms of the receiver node to the sender node and gateway-2 send the pseudonym of the sender node to the receiving node. In this way now both the end entities have each other pseudonym and they can generate the symmetric key and can send data securely.

We will show the message exchanges between DTN node (local doctor) and DTN gateway-1, DTN gateway-1 and DTN gateway-2, and finally will show the operation of intended receiver which senior doctor in our case.

1. DTN node (local doctor/patient) and Gateway-1
The sender (DTN node) will send its data to DTN gateway-1 (via the public bus). The DTN node generates random number and then will generate its public key (e.g. its email ID). Also generates pseudonyms by hashing the ID concatenated with random number. We are assuming that the sender knows the email ID of receiver. DTN node also generates one time symmetric key by concatenating a random number with the

pseudonym of receiver. In case of simple encryption and without contacting the PKG, the bundle sender can generate the key and send bundle to receiver, which is the main advantage of IBC over PKI. The sender sends the bundle to gateway-1 as next hope address. Figure-3 shows operation of DTN node and the exchange of messages between DTN node and Gateway-1.

Fig. 3. Messages exchange between DTN node and gateway-1

Where the functions calculated by DTN node as:

Generation of random number r
Public key= IDdtn
Pseudonym of dtn node=Pus=H(r.IDdtn)
Symmetric key between sender node and receiver node= Ks=(r.Pus)

Here the sender node put his pseudonym as Pus, and the receiver as Pur. As he received the pseudonym of receiver from the gateway-1 via secure channel. "M" is the message (e.g. patient medical data) which we want to send securely and anonymously.

2. DTN gateway-1 to DTN gateway-2

Whenever DTN gateway-1 receives the bundle it will keep record of pseudonyms with their corresponding IDs. It will forward the message to DTN gateway-2. The structure of the message is shown in figure-4.

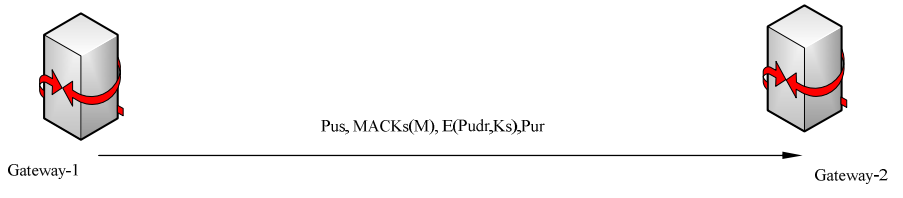

Fig. 4. Messages exchange between gateway-1 and gateway-2

3. Operation of receiving node

When bundle reach the intended receiver (hospital doctor) so it will do the same operation as of sender e.g. generating random number, public key and pseudonym. But here it will need private key to decrypt the message which was encrypted by its public key. As this network is directly connected to Internet so receiver will request for his private key to PKG the trusted authority residing at ISP server which generates private key for receiver using it security parameters pp and ID of receiver. It will securely send the

generated private key through SSL. So that the receiver will first decrypt the message by its own private key and will obtain the symmetric key and will verify MAC through symmetric key. The operation which will perform by receiving node and PKG is how in figure-5 Where the functions are calculated as:

Receiver side:-

Generation of random no r
Public key= IDdr
Pseudonym of receiving node=PurH(r.IDdr)
Ks←Decrypt(Sdr,Ks)
Decrypt message with Ks for authentication.

PKG:-

pp.Spkg.IDdr= Sdr (private key)

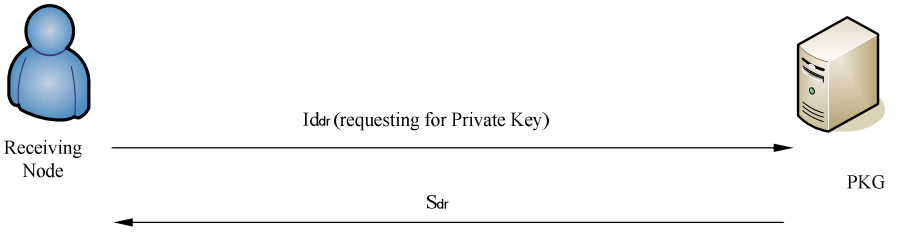

Fig. 5. Operations of the intended receiver

The receiving node already calculated the symmetric key, pseudonym prior to the receiving of bundle, upon the receiving it just send the request for private key to the PKG, which generate key for receiving node and send via secure channel.

In this pseudonym and identity based anonymous system we clearly show the anonymity of sender and receiver. Here the adversary can correlate two pseudonyms with each other but can not identify the real identities of those pseudonyms. A user can change its pseudonym frequently. As a bundle stored at gateway-1 for the connection to be up so that adversary unable to calculate the RTT and hence can not launch traffic analysis attacks. Adversary knows only the messages exchange between gateways which will not be useful with identifying the real sender/receiver. We used traditional public cryptography for authentication and integrity and for end to end confidentiality we successful used IBC. We used date concept described earlier with private key for validity reasons. As there is only one PKG so if the key of PKG compromise then adversary can easily generates keys for participants and can encrypt or decrypt data.

6 Conclusions and Future Work

The DTN concept is suitable for challenged networks such as deep space mission, disaster monitoring and rural area networks. In this paper, we focused on a telemedicine application in rural areas with the objective of exchanging confidential medical data securely with a hospital in a remote city. We provide patient anonymity and

identity hiding. An overview of DTN, Identity Based Cryptography and pseudonyms is presented. Also an analysis of anonymous routing protocols has shown that they are not suitable for DTN environment.

The paper presented our DTN anonymity protocol design and the message exchanges between the users and DTN gateways. The analysis showed that using pseudonym provides a convenient mechanism for user anonymity and medical data encryption. This work is at an early stage. However and in our future work, we will implement this system using Pairing Based Cryptography (PBC), where some earlier work was published by Stanford University [24]. We will implement our design in a testbed using DTN-2 reference model [25]. We also note that PKG is single point of contact in our design so our future will be extended to use hierarchical PKG and Hierarchical Identity Based Cryptography. We will also try to combine both encryption and digital signature i.e. signcryption using IBC, in order to reduce the cost of communication.

Acknowledgement

We would like to thank the EU Information Society Technologies SATNex II Network of Excellence for supporting this research work.

References

1. Cerf, V., et al.: Delay Tolerant Networking Architecture. IETF, Network Working Group, RFC 4838 (2007)
2. Fall, K.: A Delay Tolerant Network for Challenging Internet. In: SIGCOMM 2003 Conference on Application, Technologies, Architecture and Protocol for Computer communication, pp. 27–34 (2003)
3. Warthman, F.: A Tutorial Delay Tolerant Networks (DTNs). V 1.1, DTNRG (2003)
4. Scott, K., Burleigh, S.: Bundle Protocol Specification. IETF, Network Working Group, RFC 5050 (2007)
5. Farrell, S., Cahill, V.: Security consideration in space and delay tolerant networks. In: Second IEEE international conference, Space mission challenges for information technology, SMC-IT (2006)
6. Fall, K., Chakrabarthi, A.: Identity Based Cryptography for Delay Tolerant Networking (2003), `http://edify.cse.lehigh.edu/EdifyTeam/edifyTeamDocs/dtn_sec.pdf`
7. Symington, S.F., et al.: Bundle Security Protocol Specification. draft-irtf-dtnrg-bundle-security-08, IETF draft (2008)
8. Farrell, S., et al.: Delay-Tolerant Networking Security Overview. draft-irtf-dtnrg-sec-overview-06, IETF draft (2009)
9. Bhutta, M., Johnson, E., Ansa, G., Ahmed, N., Alsiyabi, M., Cruickshank, H.: Security Analysis for Delay/Disruption Tolerant Satellite and Sensor Networks. In: IWSSC 2009, Siena, Italy (September 2009)
10. Farrell, S., Cahill, V.: Delay and Disruption Tolerant Network (2006), ISBN. 1-59693-063-2
11. Weise, J.: Public Key Infrastructure Overview. Sun Blue Prints (2001)

12. Asokan, N., et al.: Applicability of Identity Based Cryptography in Disruption Tolerant Network. In: 1st international MobiSys workshop on mobile oppurtunistics networking, MobiOpp 2007, pp. 52–56 (2007)
13. Shamir, A.: Identity based cryptosystem and signature scheme. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
14. Gagne, M.: Identity based encryption: A survey. RSA Labortries, Cryptobytes 6 (2003)
15. Baek, J., et al.: A survey of Identity based cryptography. In: Proc. of Australian Unix Users Group Annual Conference (2004)
16. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 213–229. Springer, Heidelberg (2007)
17. Seth, A., Keshav, S.: Particle security for disconnected nodes. In: First workshop on Secure Network Protocols (NPSec), pp. 31–36 (2005)
18. Farrell, S., Symington, S., Weiss, H.: Delay Tolerant Network Security overview. Draft-irtf-dtnrg-sec-overview-08, IRTF (2008)
19. Pfitzmann, A., Hansen, M.: Anonymity, unlinkability, undetectability, unobservability, pseudonymity and identity management- A consolidated proposal for terminology (2008), http://dud.inf.tudresden.de/AnonTerminology.shtml
20. Chaum, D.: Untraceable electronic email, return address and digital pseudonym. Communication of the ACM (1981)
21. Reed, M.G., et al.: Anonymous connection and onion routing. IEEE journal on selected areas in communication, 482–494 (1998)
22. Danezis, G., Diaz, C.: A survey of anonymous communication channels. Journal of Privacy technology (2008)
23. Kate, A., et al.: Anonymity and security in delay tolerant networks. In: third international conference on security and privacy, SecureComm 2007 (2007)
24. Lynn, B.: Paring Based Cryptography (PBC) library, http://crypto.stanford.edu/pbc/
25. DTN Research group, http://www.dtnrg.org/wiki/Code