ID Based Cryptography and Anonymity in Delay/Disruption Tolerant Networks

Naveed Ahmad, Haitham Cruickshank, Zhili Sun

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

Abstract. The Delay/Disruption Tolerant Networking concept enables new applications and services in challenged networks such as rural and disaster areas networks, animal and environmental monitoring plus others. However and due to the shared and unsecured nature of such challenged networks, a good cryptographic framework is needed. Identity Based Cryptography compares favorably against traditional public key cryptography, by generating encryption keys on a fly, based on the recipient identity. In this paper, we will provide security solution for the Delay/Disruption Tolerant Networking in rural areas using this technique. In addition, 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

Networks based on TCP/IP protocol stack works normally when end-to-end connectivity is available and the round trip time is small. To explain the problem with TCP in certain applications we take the scenario of interplanetary communications. If a node on earth wants to transmit 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 transmit 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 (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 found in other network architectures [1], [2]. DTN [3] supports heterogeneous environment and is based on idea of store and forward method. Bundle layer is an implementation of DTN which supports heterogeneity of networks and ties together different regional 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 layers with the help of convergence layer which is the part of bundle layer, however, network and data link layers are transparent to bundle layers.

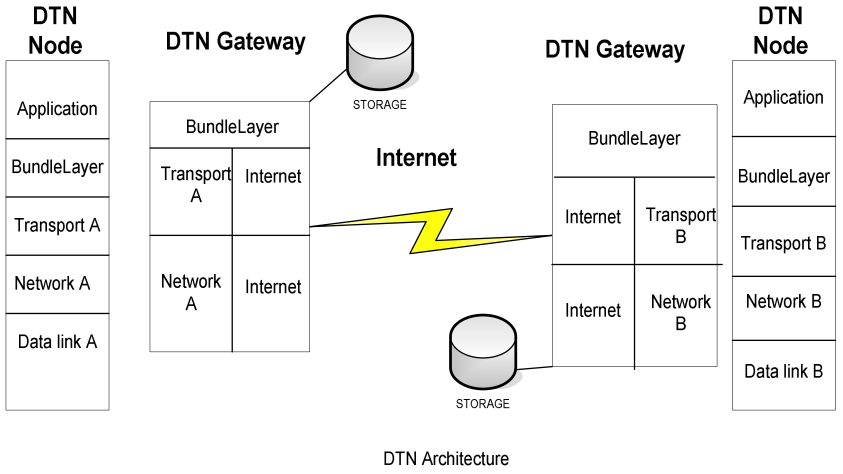

Figure 1 DTN Layer Stack

DTN can be implemented in many applications [9] e.g. Lake pollution monitoring, Deep space mission, Disaster monitoring and Rural area network. Apart from these it can also replace IP networks in applications like Web cache, Emails, Metallurgical data transfer and many more. All these 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 area networks. 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 transmit 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.
- We assumed that segmentation of patient data (sometime called bundle in DTN) is done according to the technology used e.g. satellite link or Internet is done by DTN gateway-1.

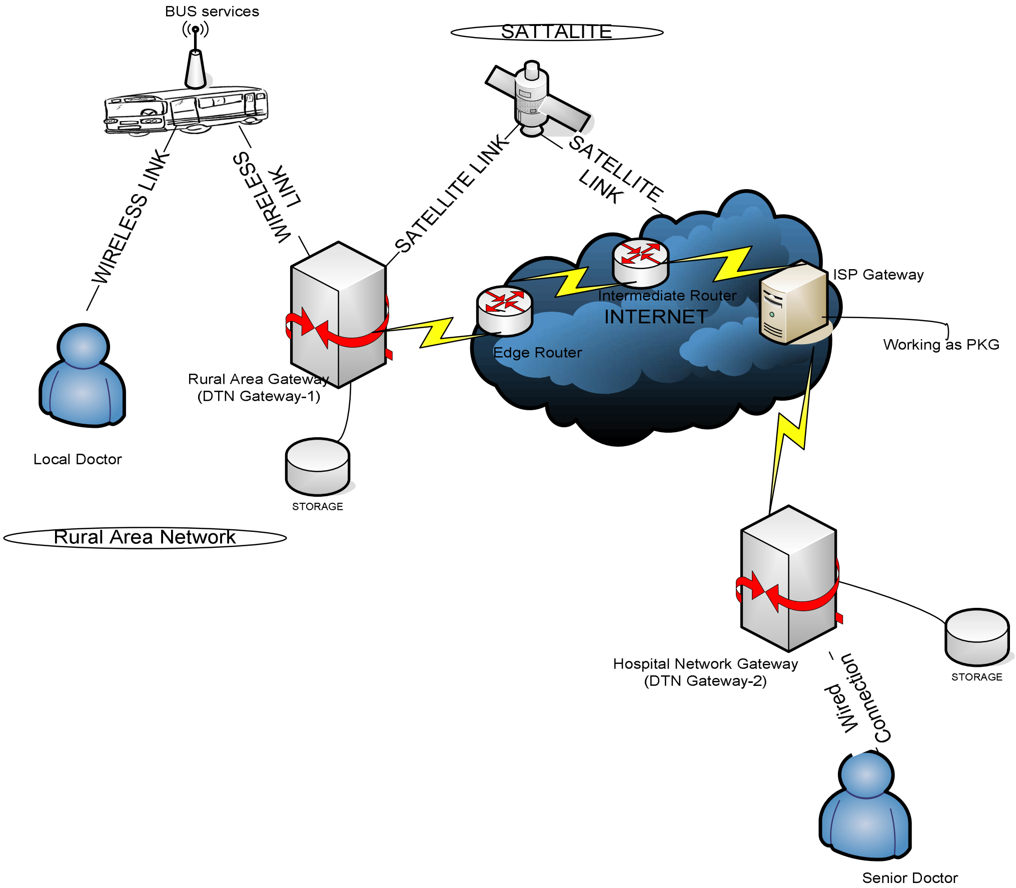

Figure 2 Telemedicine application in rural area network

The above 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.

2 Security requirements for DTN

In any network like DTN or Internet, 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]. While designing security architecture for DTN one must consider some properties, which are [6].

2.1 Reduce message exchanges

As DTN is suffered from long trip times, so while designing the architecture serious attention is required to minimize the message exchanges between two nodes.

2.2 Minimum contact with Trusted Authority

DTN is opportunistic network, so there is no permanent connectivity among the nodes so one should take into account that minimum interaction should be done with trusted authority, which, in case of public key cryptography is Central Authority (CA) which issues certificates and Public Key Generator (PKG) in IBC.

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 [7], [8]. 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 some mechanism of message exchange which hides 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). Public key cryptography is mostly attributed to Diffie, Hellman, Rivest, Shamir and Adleman [10]. To use traditional cryptography Public Key Infrastructure (PKI) provides a framework which provides foundation for other security services. It is used in many application e.g. e-voting, banking, e-commerce and many more. 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 [10]. 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 [11]. Such that, these functions require connection availability to the Certificate Authority (CA), which is not always possible as shown in our scenario (Figure 2).
To overcome the shortcomings of public key cryptography Adi Shamir proposed the topic of Identity Based Cryptography (IBC) in 1984 [12]. 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 [13], [14]. In PKI, the authority which manages certificates was CA. In IBC, 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 works on the following basic algorithms:

- **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.

Adi Shamir only implemented digital signature in his early work and later on Boneh and Franklin [15] implemented encryption as well.

There is no guarantee of permanent connectivity in DTN. This 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 [16]. To achieve integrity and authentication in IBC Seth et al [16] suggested the avoiding of Certificate Revocation List (CRL) and proposed periodic refreshing of underlying identifier information e.g. *alice@hotmail.com 12-10-2009 i*s 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 [17] 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

User anonymity (identity hiding) is an important concept in many applications and services such as our DTN scenario described in Figure 2. One way of providing anonymity 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 three kind of pseudonym with respect to unlinkability [18].

- **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 [19]. This approach was 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 work done by Chaum's [19]. The term anonymity according to [20] "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]. Anonymity is achieved though using some anonymous Communication Protocol (ACP). Generally most of the ACP are based on idea of Mix Networks by David Chaum's and onion routing [20], [21]. Table 1 shows different ACPs in term of some performance metrics.

Protocol	Sender Anonymity	Receiver Anonymity	Unlinkability	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

Table 1 A survey of Anonymous Communication Protocol (ACP)

All discussed protocols above either use the idea of onion routing or mix networks, and provides anonymity at some level. However, the above traditional solution for anonymity does not work in DTN because of the disconnected nature and routing strategy of DTN. With opportunistic and variable delays source routing is not always possible [22]. In DTN, there is no complete routing topology so Onion Routing (OR) does not work because OR needs to know the route in advance and encrypt the message accordingly for each router on the path. 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, this paper provides DTN anonymity architecture with pseudonym based approach.

5 DTN Anonymity Protocol Design

The 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 secrete 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 got the key pairs, they do not need to interact with PKG anymore and can send data to other entity.
4. There is shared secret key between PKG and the destination which in our case is senior doctor, through which it can encrypt the bundles exchanges between them.
5. The keys are distributed securely through mechanisms such as Secure Socket Layer (SSL) to each entity. This key distribution is out of scope for this paper.
6. Our DTN gateways are trusted. In our proposed solution, anonymity is achieved through use of pseudonyms which allow DTN routers/gateways to know that the Pseudonym is belonging to the valid authenticated user without unveil his identity
7. There is security association between each entity and their corresponding gateway, the pseudonym generated by each entity is securely sent to gateway, where it stored in the persistence memory.
8. Both gateways shared a secrete key which is used is to encrypt/decrypt bundles between them.
9. 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 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 local doctor will send the patient record to DTN gateway-1 (via the public bus). The local doctor 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. Local doctor 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 local doctor sends the bundle to gateway-1 as next hope address. Figure-3a shows operation of local doctor and the exchange of messages between local doctor and Gateway-1.

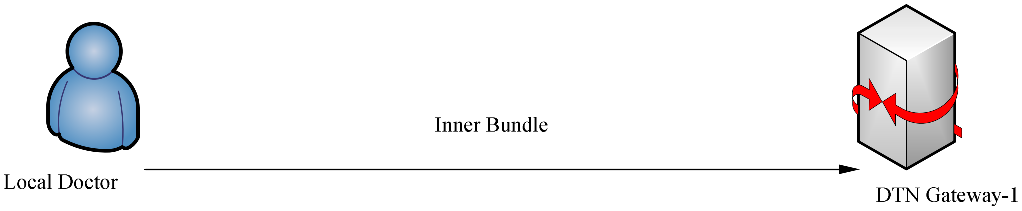

Figure- 3a messages exchange between DTN node and gateway-1

The formats of the source budle and the cryptographic suits applied by the local doctor are shown in Figure- 3b and Figure-3c respectively, where Pld is the pseudonym generated by the local doctor and Psd is the pseudonym generated by the senior doctor.

Security Source (Pld)
Security Destination (Psd)
Cryptographic functions
Data

Figure -3b inner bundle

Generation of random number r
Public key= IDld
Pseudonym of local doctor node=Pld=H(r.IDld)
Symmetric key between sender node and receiver node Ks=(r.Pld).

Figure- 3c Cryptographic functions

Here the local doctor node put his pseudonym as Pld, and the receiver as Psd. As he received the pseudonym of receiver from the gateway-1 via secure channel.

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-4a. The format of the gateway bundle is shown in figure-4b where the inner bundle comes as data part encrypted by shared symmetric key between both gateways (as presented in the assumption section 5.1). Gateway-2 will pass this bundle to senior doctor as it is by only changing the source and destination address to gateway-2 and senior doctor address respectively.

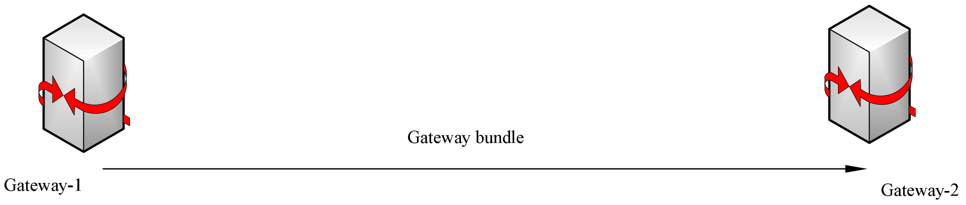

Figure- 4a messages exchange between gateway-1 and gateway-2

Gateway-1 address
Gateway-2 address
Data(inner bundle)

Figure-4b Gateway bundle

3. Operation of receiving node

When the gateway bundle reaches the intended receiver (senior doctor) so it will do the same operation as of sender e.g. generating random number, public key and pseudonym. The following figure-5a shows the bundle exchanges between senior doctor and PKG. Here senior doctor 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 by creating destination bundle shown in figure- 5b, putting its Identity as data and encrypted via the symmetric key between PKG and senior doctor (as presented in the assumption section 5.1). In our scenario 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 by creating PKG bundle shown in figure-5c encrypted via symmetric key. Now the senior doctor will first decrypt the PKG bundle and will get the private key and by using that private key senior doctor will first decrypt the message by its own private key and will obtain the symmetric key and will verify MAC through symmetric key.

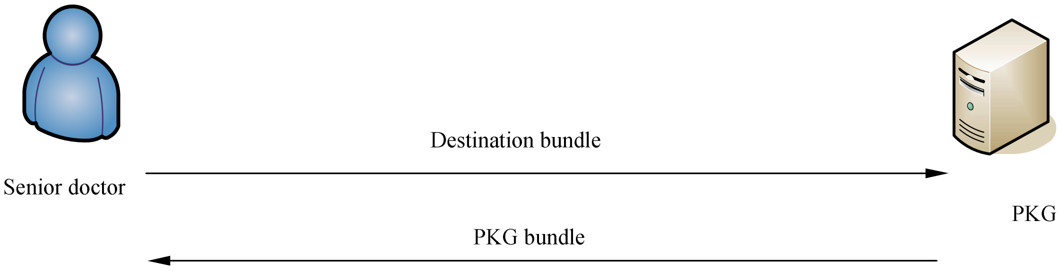

Figure -5a Operations of the intended receiver

Source address(senior doctor)
Destination address(PKG)
Data (email ID)

Figure-5b Destination bundle

Source address
Destination address
Private key

Figure- 5c PKG Bundle

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.

While on the way back when the senior doctor want to transmit the report to the local doctor, so it will fallow the same path i.e. senior doctor will generate a bundle as inner bundle same as described earlier and will send to the gateway-2. The gateway-2 will generate the gateway bundle and transmit it to gateway1 where the inner bundle will come as the data part encrypted using the shared secret key between pair of gateways. Then the gateway-1 will send the bundle to the local doctor and here we assumed that the local doctor has already got the its own private key and can performed all cryptographic functions.

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. In our future work, we will implement this system using Pairing Based Cryptography (PBC), where some earlier work was published by Stanford University [23]. We will implement our design in a testbed using DTN-2 reference model [24]. We also note that PKG is single point of contact in our design so our future work will be extended to use hierarchical PKG and IBC.

7 Acknowledgement

We would like to thank the EU Information Society Technologies SATNex II Network of Excellence VIII 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. SIGCOMM ’03 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. Space mission challenges for information technology, second IEEE international conference, SMC-IT, (2006).

6. Fall, K., Chakrabarthi, A.: Identity Based Cryptography for Delay Tolerant Networking. Available: http://edify.cse.lehigh.edu/EdifyTeam/edifyTeamDocs/dtn_sec.pdf, (2003)

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. Farrell, S., Cahill, V.: Delay and Disruption Tolerant Network. ISBN. 1-59693-063-2, (2006).

10. Weise, J.: Public Key Infrastructure Overview. Sun Blue Prints, (2001).

11. Asokan, N et al.: Applicability of Identity Based Cryptography in Disruption Tolerant Network, 1st international MobiSys workshop on mobile oppurtunistics networking, MobiOpp '07, Pages: 52 – 56, (2007).

12. Shamir, A.: Identity based cryptosystem and signature scheme. Proceedings of CRYPTO, pp.47-53, (1984).

13. Gagne, M.: Identity based encryption: A survey", RSA Labortries, Cryptobytes, Vol 6, (2003).

14. Baek, J et al.: A survey of Identity based cryptography. Proc. of Australian Unix Users Group Annual Conference, (2004).

15. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. Proceedings of CRYPTO, pp.213-229, (2007).

16. Seth, A., Keshav, S.: Particle security for disconnected nodes. First workshop on Secure Network Protocols (NPSec), pp. 31-36, (2005).

17. Farrell, S., Symington, S., Weiss, H.: Delay Tolerant Network Security overview. Draft-irtf-dtnrg-sec-overview-08, IRTF, (2008).

18. Pfitzmann, A., Hansen, M.: Anonymity, unlinkability, undetectability, unobservability, pseudonymity and identity management- A consolidated proposal for terminology. Available: http://dud.inf.tudresden.de/Anon Terminology.shtml, (2008).

19. Chaum, D.: Untraceable electronic email, return address and digital pseudonym. Communication of the ACM, (1981).

20. Reed, M.G et al.: Anonymous connection and onion routing. IEEE journal on selected areas in communication, pp. 482-494, (1998).

21. Danezis, G., Diaz, C.: A survey of anonymous communication channels. Journal of Privacy technology, (2008).

22. Kate, A et al.: Anonymity and security in delay tolerant networks. third international conference on security and privacy, SecureComm '07, (2007).

23. Lynn, B.: Pairing Based Cryptography (PBC) library. Available on http://crypto.stanford.edu/pbc/

24. DTN Research group, Available on. http://www.dtnrg.org/wiki/Code.