future internet

MDPI

Article

Cryptographic Key Management in Delay Tolerant Networks: A Survey

Sofia Anna Menesidou [1,*,†], Vasilios Katos [2,†] and Georgios Kambourakis [3,4,†]

1 Department of Electrical and Computer Engineering, Democritus University of Thrace, University Campus, Xanthi 67100, Greece
2 Department of Computing and Informatics, Bournemouth University, Poole House, Fern Barrow BH12 5BB, UK; vkatos@bournemouth.ac.uk
3 Department of Information and Communication Systems Engineering, University of the Aegean, Samos GR-83200, Greece; gkamb@aegean.gr
4 Computer Science Department, George Mason University, Fairfax, VA 22030, USA
* Correspondence: smenesid@ee.duth.gr
† These authors contributed equally to this work.

Academic Editor: Dino Giuli
Received: 23 May 2017; Accepted: 24 June 2017; Published: 27 June 2017

Abstract: Since their appearance at the dawn of the second millennium, Delay or Disruption Tolerant Networks (DTNs) have gradually evolved, spurring the development of a variety of methods and protocols for making them more secure and resilient. In this context, perhaps, the most challenging problem to deal with is that of cryptographic key management. To the best of our knowledge, the work at hand is the first to survey the relevant literature and classify the various so far proposed key management approaches in such a restricted and harsh environment. Towards this goal, we have grouped the surveyed key management methods into three major categories depending on whether the particular method copes with (a) security initialization, (b) key establishment, and (c) key revocation. We have attempted to provide a concise but fairly complete evaluation of the proposed up-to-date methods in a generalized way with the aim of offering a central reference point for future research.

Keywords: cryptographic key management; delay tolerant networks; DTN

1. Introduction

It is without a doubt that cryptography is an important and powerful tool for achieving secure communications. Key management, including key distribution and revocation, is a central part of any cryptographically protected secure communication and is one of the weakest links of system security in general and protocol design in particular [1]. In most communication scenarios, cryptographic keys need to be established between the communicating network nodes prior to any service can be delivered. Cryptographic key management is considered to be a challenging and open issue in DTNs [2]. Such environments are typically encountered in extreme terrestrial environments, deep space or interplanetary communications, and are characterized by long latency and high degree of disruption mainly due to physical phenomena (noise, limitations of wireless radio, etc.). Specifically, the difficulties and challenges are due to the constraints of the restricted networking conditions DTNs typically operate in, rather than the actual features of the underlying key management cryptographic protocols and solutions. Typically, the constraints of DTN environment make a number of mature and robust key management protocols described in the literature totally or partially unsuitable.

Over the past few years, significant research has been performed in the field of communication in DTNs. DTN architecture [3] introduces an overlay protocol, namely the Bundle Protocol (BP) [4], that interfaces with either the transport or lower layers and exists anywhere between the transport

and the application layers. In addition, DTN architecture is based on the well-known store and forward model, an old mechanism used in postal systems since ancient times [5]. The main dissimilarities between the assumptions of traditional Internet-like networks and DTNs are the intermittent connectivity, implying the lack of a continuous end-to-end path between the source and destination and the long propagation delays. Conventional mechanisms for routing and key management do not work in a DTN mainly because of these assumptions. In fact, the literature has a relatively long domain of routing in DTNs, but very few consider the security parameter.

The unique DTN characteristics, including long round-trip delay, frequent dis-connectivity, fragmentation, etc. [3], make the existing security protocols designed for the conventional networks unfit for DTN ecosystems. Cryptographic key management and secure routing are important issues in DTNs, but the solutions proposed until now tend to consider them separately. Several approaches have been adopted to achieve cryptographic key management in such challenged networks. The main bulk of research has been focused on two main approaches: the traditional Public Key Infrastructure (PKI) [6] and Identity Based Cryptography (IBC) [7]. Each of them has its own benefits and drawbacks and is suitable in certain domains of DTN [3] .

To our knowledge, so far no work in the literature has attempted to provide a comprehensive survey of the various works addressing cryptographic key management specifically for the DTN domain. Motivated by this fact, the survey at hand offers an extensive study of the relevant literature in the last 13 years, spanning a period from 2005 to 2017. The surveyed protocols are categorized based on four distinct factors, namely the communication type, method used, type of the challenged network, and evaluation method.

The rest of the paper is organized as follows: The next section briefly reviews the background of research on preliminaries regarding key management and DTN characteristics. Section 3 reviews and classifies all major contributions in the field of key management in DTNs. A discussion on the surveyed schemes is provided in Section 4. Section 5 presents alternative key management taxonomies for DTNs, while Section 6 lists the main security callenges in this type of networks. The last section summarizes and concludes the survey by posing open questions and future directions of applying key management to secure DTNs.

2. Background

This section concentrates on cryptographic key management for DTNs by examining its unique characteristics, and the associated challenges. To familiarise the reader with this topic, the section starts with a brief introduction containing the basic methods for key management and the corresponding terminology.

2.1. Preliminaries

Cryptographic key management is the process by which cryptographic keys are generated, stored, protected, transferred, loaded, used, and destroyed [8] and is one of the most difficult problems in DTN security [9]. The reason is that cryptographic key management generally requires multiple round trips in order to securely exchange or establish keys. This is problematic because of the long delays and possible connectivity disruptions in such restricted networks. As further discussed in Section 4, there are currently no key management schemes that appear to suit DTNs. Naturally, poor or weak cryptographic key management will have an adverse effect on the cryptographic techniques, which risk of being rendered insecure or inefficient [10].

Security initialization or bootstrapping, as the name suggests, is how to initially establish security associations between the communicating nodes. Key establishment is one of the basic concepts in this context, which is defined as a method that two or more parties adopt with the aim of sharing a secret value for secure communication. Key establishment is divided into (a) key transport or key distribution and (b) key agreement. In key transport, one party creates or receives a secret value and securely transfers it to the other party. In key agreement, a shared secret value is derived jointly by

two (or more) parties. As already mentioned, the bulk of the research so far has been focusing on two main approaches. More specifically, the two main up-to-date proposed ideas are IBC and PKI. Both approaches are based on asymmetric or public-key cryptography (PKC).

- *Identity Based Cryptography (IBC)*—Shamir first introduced IBC in 1985 [7]. In this cryptographic approach, user identifier information such as email address, IP address, and so forth are used as a public key for encryption and verification of digital signatures instead of certificates. In addition, in IBC, the Private Key Generator (PKG) is the central authority (similar to a Certificate Authority, CA in PKIs) which generates the private keys for participants.
- *Public Key Infrastructure (PKI)*—Traditional asymmetric or public key cryptography widely and effectively used in the Internet and a plethora of business realms relies on a PKI. The latter depends on the availability and security of a CA, a central control point that everyone trusts.

2.2. DTN Characteristics and Key Management

Network environments characterized by intermittent connectivity, network heterogeneity, and large delays are called "challenged networks". DTN is a computer networking architecture that aims to address the technical issues present in challenged networking environment, as well as specify the necessary components for interconnecting heterogeneous networks. The term DTN stems from Fall's paper [11], which introduced an architecture generalized from design work for the InterPlanetary Networking (IPN), which in turn addressed networking challenges in deep-space communications.

The two main challenges addressed by DTNs are related to (a) long propagation delays and (b) intermittent connectivity, implying the lack of a continuous end-to-end path. Under such restricted and harsh networking conditions, traditional internetworking protocols (e.g., TCP/IP) are neither applicable nor suitable [12]. Networks where DTN architectures may apply include:

- *Deep space networks [13]*—They are characterized by extremely long delays that typically cause memory and/or storage exhaustion.
- *Sensor-based networks [13]*—Their idiosyncrasies include extremely low end-node power, memory, and CPU capability.
- *Terrestrial wireless networks [14]*—This ilk of networks is characterized by high mobility and changes in signal strength.
- *Vehicular AdHoc networks [15]—They exhibit mobility, self-organization, distributed communication*, and road-pattern restrictions.
- *Satellite networks [16]*—They are characterized by long delays and high rate of packet loss.
- *Underwater acoustic networks (undersea networks) [3,17]*—They demonstrate spatial coverage and high density of nodes.
- *Rural area DTN [18]*—They are distinguished by opportunistic behaviour, sporadic and isolated message transmission.

The constraints under which such challenged networks function has also severe effects on the security protocols, and therefore traditional solutions cannot be directly applied. The need for secure communications in open networks like DTNs is higher than ever . However, until recently, security was not considered to be an issue for DTNs in space missions. Moreover, the authors in [2] propose a practical mechanism to evaluate security protocols, including key exchange ones in DTNs. This is done by considering node credentials and network topology. Such a method could help in identifying the most efficient key management scheme in terms of delay for experimentally tested scenarios.

2.3. Security in Real DTN Implementations

Several existing DTN implementations have been released with varying compliance regarding the proposed standards [19]. More specifically, the main implementations considering security are listed below.

- *DTN2* [20]—This is the most well known implementation of the BP, which implements partially the Bundle Security Protocol (BSP) specification. It uses OpenSSL library to perform the cryptographic operations, although most functionality for cryptographic operations is not yet implemented [19].
- *ION* [21]—JPL's implementation of the BP. It implements the BSP Bundle Authentication Block (BAB), Bundle Confidentiality Block (PCB) and Bundle Integrity Block (PIB) security blocks in versions greater than 3.0.0.
- *IBR-DTN* [22]—BP implementation for embedded systems, which relies on the BSP specification.
- *ByteWalla* [23]—BP implementation for Android devices. It implements the BSP PCB security block with AES in Galois Counter Mode (GCM).

3. Key Management Taxonomy in DTNs

As already pointed out, cryptographic key management is the foundation of network security, so it is an indispensable part of the DTN security. Key management schemes in DTNs can be classified into three major categories depending on whether they deal with one or more of the following issues (a) security initialization, (b) key establishment, and (c) key revocation. Key establishment can further be classified into two-party and group communications based on the number of communication parties. To exemplify, Figure 1 depicts a classification of the surveyed key management schemes in such networks based on category, type of communication, and the cryptographic methods used. Note that the majority of works related to security and key management in DTN for the aforementioned three main categories are listed in Tables 1–5 in chronological order. It is to be noted that due to the difficulty of performing tests to a real DTN environment, all the works so far evaluate their scheme either theoretically or via some kind of simulation. Therefore, the performance results are not directly comparable to each other. In fact, only a small fraction of the papers have implemented their scheme. Moreover, the existing results are not comparable to each other because the authors address different kind of DTN and/or the simulation parameters are dissimilar. For this reason, and to avoid any bias, we opt to exclude performance results from the tables. Finally, in the last subsection all the so far standardisation efforts in terms of RFCs and Internet drafts are summarised.

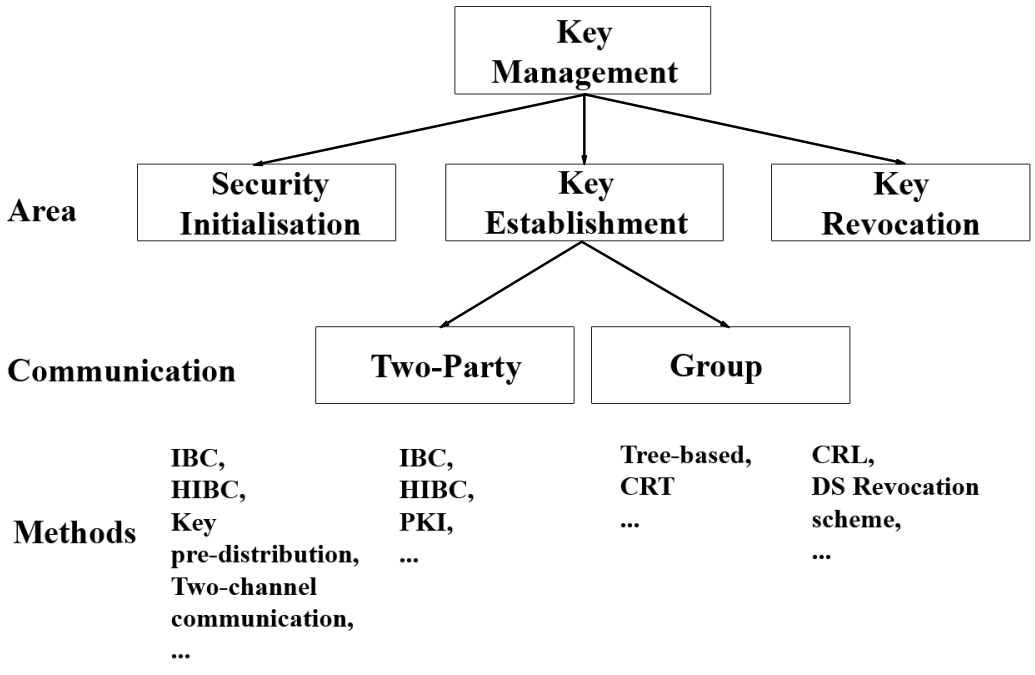

Figure 1. Key management Taxonomy.

Table 1. Comparison of Security Initialisation Methods.

Scheme	Crypto-Graphy	Methods/Protocols/Schemes	DTN Network	Evaluation Method	Architecture	Year
Seth, A., and Keshav, S. [24]	PKC/SKC	HIBC, Gentry-Silverberg HIBC (HIBE and HIBS), authorized distribution	Rural Area DTN	N/A	Centralised	2005
Asokan, N., Kostiainen, K., Ginzboorg, P., Ott, J. and Luo, C. [25]	PKC/SKC	IBC, cellular authentication infrastructure	Rural Area DTN	Theoretical	Centralised	2007
Patra, R., Surana, S., and Nedevschi, S. [26]	PKC	HIBC	Network-agnostic	N/A	Centralised	2008
El Defrawy, K., Solis, J., and Tsudik, G. [29]	PKC	social contact information	Rural Area DTN	Simulation	Decentralised/Distributed	2009
Du, J. and Kranakis, E., and Nayak, A. [31]	PKC/SKC	key pre-distribution, neighbor distributed key establishment (DKE)	Sensor and Actor Network DTN (DTLBS-WSAN)	Theoretical, Simulation	Decentralised/Distributed	2011
Shikfa, A., Önen, M., and Molva, R. [30]	PKC	self-organised, pseudonym certificates, encapsulated signatures	Opportunistic Networks	Theoretical	Decentralised/Distributed	2012
Jia, Z., Lin, X., Tan, S., Li, L., and Yang, Y. [34]	PKC	two-channel cryptography, dynamic virtual digraph (DVD)	pocket DTN	Simulation	Decentralised/Distributed	2012
Xie, Y., and Wang, G. [32]	SKC	distributed secret key generation system, self-certified identity	Network-agnostic	Simulation	Decentralised/Distributed	2013
Djamaludin, C.I., Foo, E., and Corke, P. [33]	PKC	PGP, Leverage of Common Friends (LCF) method	Network-agnostic	Simulation	Decentralised/Distributed	2013
Lv, X. and Mu, Y. and Li, H. [35]	PKC	two-channel cryptography, time evolving model	Space DTN	Simulation	Decentralised/Distributed	2014
Jadhav, C., Dhainje, P., and Pradeep, D. [36]	PKC	two-channel cryptography, time evolving model	Space DTN	N/A	Decentralised/Distributed	2015
Mukundhan E. and Veeramani, M.E. [37]	PKC	two-channel cryptography, time evolving mode	Space DTN	N/A	Decentralised/Distributed	2015

Table 2. Comparison of two-party IBC-based key establishment methods.

Scheme	Crypto-Graphy	Key Manage-Ment Area	Methods/Protocols/Schemes	DTN Network	Evaluation Method	Architecture	Year
Kate, A., Zaverucha, G., and Hengartner, U. [12]	PKC/SKC	key agreement	IBC, Sakai-Ohgishi-Kasahara (SOK) key agreement scheme and HIBC (HIBE and HIBS)	Rural Area DTN	Simulation	Centralised	2007
Van Besien, W.L. [41]	PKC/SKC	key pre-distribution, key distribution	IBC bilinear maps over elliptic curves	Network-agnostic	N/A	Centralised	2010
Ahmad, N., Cruickshank, H., and Sun, Z. [40]	PKC/SKC	key agreement	IBC	Rural Area DTN	N/A	Centralised	2010
Ding, Y., Zhou, X., Cheng, Z., and Zeng, W. [42]	PKC/SKC	key agreement	CPK (Combined Public Key), AKP protocol, ECC	Network-agnostic	Theoretical	Centralised	2013

Table 3. Comparison of two-party PKI and PGP-based key establishment methods.

Scheme	Crypto-Graphy	Key Manage-Ment Area	Methods/ Protocols/Schemes	DTN Network	Evaluation Method	Architecture	Year
Bhutta, M., Ansa, G. and Johnson, E., Ahmad, N., Alsiyabi, M. and Cruickshank, H. [45]	PKC/SKC	key predistribution, manual keys, key establishment	PKI, proxy certificates	Satellite and Sensor DTN	N/A	Centralised	2009
Menesidou, S.A., and Katos, V. [46]	PKC/SKC	key agreement	PKI, HMP protocol	Space DTN	N/A	Centralised	2012
Johnson, E., Cruickshank, H., and Sun, Z. [47]	PKC	key pre-distribution	PKI	Satellite DTN	Simulation	Centralised	2013
Bhutta, M., Cruickshank HS., and Sun Z. [48]	PKC/SKC	key distribution	PKI, proxy signatures, Symmetric Key Transport, Efficient, Scalable Key Transport Scheme (ESKTS)	Network-agnostic	Simulation	Centralised	2014
Rajan, G., and Cho, G. [49]	PKC/SKC	key distribution	PKI	Network-agnostic	N/A	Centralised	2015
Andrade, D., and Albini, C. [50]	PKC	key establishment	PGP, DSC-KM	Network-agnostic	Simulation	Decentralised/Distributed	2016

Table 4. Comparison of Group Key Management Proposed Methods.

Scheme	Crypto- Graphy	Security Properties	Methods/Protocols/Schemes	DTN Network	Evaluation Method	User Join Message Cost	User Leave Message Cost	Architecture	Year
Edelman, P., Donahoo, M., and Sturgill, D. [52]	PKC	FS, BS, KI, CF	Group Membership Tree (GMT), Logical Key Hierarchy (LKH), key graphs	Network-agnostic	Simulation	O (log n)	O (log n)	Centralised	2010
Xu, Gl, Chen, X., and Du, X. [53]	SKC	FS (one-to-many scenario),BS, CF	XOR, Chinese Remainder Theorem, Chinese Remainder DTN Group Key (CRDGK) scheme, time-based group key management scheme	Network-agnostic	Simulation	O (1)	O (1)	Centralised	2012
Zhou, J., Song, M.m Song. J., Zhou, X., and Sun, L. [54]	PKC	FS, BS, KI, CF	autonomic group key management (AGKM) scheme, Logical Key Hierarchy (LKH), one-encryption-key multi-decryption-key key protocol	Space DTN	Theoretical Proof, Simulation	O (log n)	O (1)	Centralised	2014
Gupta [51]	PKC	FS, BS, CF	Modified version of Chinese Remainder Theorem	Network-agnostic	Theoretical Proof, Simulation	O (1)	O (1)	Centralised	2016

Table 5. Comparison of key revocation methods.

Scheme	Crypto-Graphy	Methods/Protocols/Schemes	DTN Network	Evaluation Method	Architecture	Year
Djamaludin, C.I., Foo, E., Camtepe, S. and Corke, P. [57]	PKC	DS revocation scheme, PGP,△CRL	Large scale DTNs (e.g., MANET, VANET)	Simulation	Decentralised/Distributed	2016
Bhutta, M. and Sun, Z. [56]	PKC	PKI, Hash Table, CRL	Network-agnostic	Simulation	Centralised	2017

3.1. Security Initialization

The first attempt of researchers to solve the problem of security initialization and key management in DTN was based on IBC rather PKI. This was mainly due to the frequently disconnected nodes and hostile nature of such networks. Works [24–26] are characteristic examles of this situation. More specifically, the authors in [24] proposed the first work based on IBC for key management in DTN. They state that the traditional PKI-based approach is unsuitable for DTNs due to their disconnected nature. Their work examines the practical aspects related to deployment of DTN in remote rural and/or disconnected areas. This includes practices for both initial key establishment and roaming among different service providers. They propose a forward-secure Hierarchical Identity Based Cryptography (HIBC) scheme that according to them can can be proved efficient and practical toward secure channel establishment, mutual authentication of parties, and revocation in DTNs. On the downside, as the authors admit, it is well-known that HIBC suffers from the problem of PKG compromisation, where all the generated private keys for lower level PKGs and users can be yield. To bypass this problem their work is founded on the assumption that PKG is trusted and uncompromisable. Moreover, their work is based on time-based keys (keys that rely on the high synchronized clocks between all entities), which can be a problem of practicality with respect to actual deployment [27]. Another work that evaluates IBC cryptography in the context of DTN and discusses the trade-offs between PKI and IBC is that in [25]. Specifically, the authors investigate how security in DTNs can be bootstrapped from existing cellular large-scale security infrastructure. They describe how a PKG can verify whether a new principal have the right to public identifier or not as compared to [24]. Moreover, in their work, they analised the applicability of IBC in DTNs and they found that there is no significant advantage over traditional cryptography in terms of authentication. In [26] the authors propose an architecture based on HIBC that according to them provides end-to-end security services as well as the ability to have fine-grained revocation and access control. In addition, their scheme is alleged to offer efficient key distribution across DTN regions. One drawback of IBC-based works is that there is a need to check IBC public parameter [28]. This is the same problem researchers tried to overcome in PKI with CA certificate verification. However, in [25] the authors argue that such a comparison is unfair. Another drawback of IBC is the difficulty of key revocation.

The work in [29] focuses on the problem of initial secure context establishment in DTNs and proposes a method that allows users to leverage social contacts to exchange confidential and authentic messages. More specifically, if a node does not posses its peer's public key, then it can encrypt the message with the public keys of several nodes near the destination, in terms of either physical proximity or contact frequency. However, this algorithm has the problem of having to constantly maintain contact information for several nodes in the network, and therefore it does not scale well or it may lead to deadlock if the destination has currently no neighboring nodes. The authors in [30] propose a local and self-organised key management scheme in opportunistic networks (OppNets). They use pseudonym certificates and encapsulated signatures to enable the bootstrapping of local, topology-dependent security associations between a node and its neighbours along with the discovery of the neighbourhood topology. The authors identify that for content-based communication IBC-based solutions are inapt and self-organised solutions suit better. Their scheme consists of two phases the setup/initialization phase and the key agreement one.

In [31] the authors describe a Distributed Key Establishment (DKE) protocol in location-based social wireless sensor and actor DTNs. Their mechanism uses a combination of key pre-distribution and neighbour key establishment to set up key pairs at nodes. To improve security and counter network disruptions, they also propose a distributed way to store public key certificates and certificate revocation list (CRL). The authors in [32] recognise that both traditional PKI system and IBC schemes are not suitable for DTNs because they rely on centralised infrastructures and require multiple round-trip interactions. They propose a distributed secret key generation system with self-certified identity that does not require any PKG and threshold cryptosystem. This sceme is based on secret key crypography (SKC). In [33] the authors build and compare different decentralised trust systems for

implementation in autonomous DTN systems. They employ a key distribution model that is based on the Web of Trust (WoT) principle and compare it with two other decentralised methods. However, in such a model, if a highly trusted node is compromised, the entire model collapses.

Various works also proposed two-channel cryptography [34–37] as a candidate solution for DTN. Two-channel cryptography techniques first introduced in [38] and have several applications in constrained and infrastructure-less environments. The authors in [34] introduced a model for public key distribution, named Dynamic Virtual Digraph (DVD). This model extends conventional graph theory. Also, they present a public key distribution for pocket DTN based on two-channel cryptography. In [35] the authors propose a non-interactive key establishment scheme for the BSP focusing on space DTNs [39]. They use a time-evolving model based on the periodic and prearranged behaviour patterns of space DTNs. Based on this model, they were able to schedule when and where to send the corresponding public key. Another work based on [35] is that in [36]. Precisely, the authors propose a scheduled key exchange mechanism for BSP of space DTNs too. For their mechanism, they also use two-channel cryptography and non-interactive public key exchange protocol to replace the traditional PKI. A more recent work that utilises a time evolving topology model and two-channel cryptography to design a non-interactive key exchange protocol is that in [37]. In any case, all the aforementioned two-channel cryptography works rely on the security of the authenticated channel, and on the strong assumption that the adversary has limitted control over that channel.

Table 1 summarises all the aforementioned schemes for security initialization in DTN based on four (mostly) common in all the surveyed works criteria, namely cryptosystem, cryptographic protocol or method, area of application, and evaluation method.

3.2. Key Establishment

3.2.1. Two-Party Communication

Identity-Based Cryptography (IBC)

As already mentioned, IBC has been examined as a possible solution for key management in DTN. In this context, we can stand out the works in [12,40–42]. In [12], the authors introduce an anonymous authentication scheme. They also propose a secure communication solution based on the non-interactive Sakai-Ohgishi-Kasahara (SOK) key agreement scheme. This scheme is based on Boneh-Franklin HIBC, for greater scalability and signature verification. Also, according to the authors, it is more efficient compared to [24], as it incurs no additional overhead for routing and can optionally be made non-interactive. Nevertheless, this scheme is very tightly tied to the DakNet model [43], and it assumes a strongly trusted central authority [44]. Instead, for DTN a more general approach is required, where a trusted central authority cannot be assumed. The work in [40] is based on IBC too. The authors present a method using IBC and pseudonyms to transfer securely medical data from rural areas to a hospital in a remote city. They also state that there is no need to check frequently the public parameter as suggested in [24].

More recently, the author in [41] presents a key distribution protocol for infrastructure-less networks, which is based on the BP [4] and more specifically on the BSP [39] . The BP is used to send application data across a DTN network, while BSP provides data integrity and confidentiality services for the BP [39]. It can be argued that with this non-interactive scheme, cryptographic keys can be established for all the BSP mechanisms. The derived keys will be used for the BSP supported algorithms. For instance, HMAC-SHA1 for authentication, RSA for signatures, and AES for encryption. However, this sceme assumes a pre-distributed key. The authors in [42] present an anonymous combined public key (CPK) based protocol. CPK techniques integrate public key cryptography with IBC. Their CPK cryptosystem is based on elliptic curves cryptography (ECC) and eliminates the need of PKC on-line retrieval compared to IBC. Instead, an offline repository is needed. In fact, this work is also based on IBC, which has proved impractical for DTNs.

In addition, IBC solutions are undesirable due to intractability of some problems such as the PKG parameter distribution, private key revocation, identity name space management, key escrow, and so forth [35]. The PKG parameter distribution is the main problem in IBC. More specifically, a single PKG has to generate private keys for all the users and also establish secure channels to transmit them, which is a burdensome job in large networks. The use of hierarchy in HIBC alleviates the aforementioned problem making the process faster and more secure in case of key compromisation. Table 2 presents a comparison of IBC-based key establishment schemes proposed for DTNs using the same criteria as in Table 1.

Public Key Infrastructure (PKI) & Pretty Good Privacy (PGP)

An analysis related to the applicability of IBC in DTN systems by [25] resulted that for authentication IBC had no significant advantage over traditional cryptography. Works such as [45–49] are based on the classic PKI because it is well-examined and recognised. However, PKI schemes are associated with limitations such as server unavailability and cryptographic operations overhead. The authors in [45] proposed a DTN security architecture, which focuses on different key management parameters based on proxy certificates and PKI. Their method supports both hop-by-hop and end-to-end authentication with the aim of ensuring data correctness before forwarding using BAB. In their work, they identify that a single key management scheme does not suffice for DTNs because of the overlaid heterogeneous networks.

The authors in [46] propose a one-pass key establishment protocol for space DTNs. Their protocol is based on an adoption of the Horsters-Michels-Petersen (HMP) protocol. More specifically, they use asymmetric authenticated encryption with message recovery to encrypt the parameters of the new key. In their method, they inject protocol messages in the bundle payload as part of the message. In addition, an encryption decision-making workflow diagram of a DTN custodian node is presented. The authors in [47] propose a traditional cryptography based authentication scheme specially designed for Satellite DTN. According to the authors, the proposed scheme does not depend on network administrator's availability during post network authentication communication and facilitates bundle processing by the recipient in the absence of connectivity.

More recently, the work in [48] presents an Efficient and Scalable Key Transport Scheme (ESKTS) based on public key cryptography and proxy signatures. This scheme ensures that integrity and authentication is achieved at hop-by-hop as well as end-to-end level. It also achieves end-to-end confidentiality and freshness for end communicating parties. In addition, the authors in [49] propose a secure way of cryptographic key distribution to the DTN nodes. The proposed DTN security architecture offers a way of key distribution and prevention of nodes during possible threats and attacks, while at the same time affords all the security features of BSP.

Last but not least, the authors in [50] propose a decentralised distributed scheme that is based on Digital Signature Chains Key Management Scheme (DSC-KM) and Pretty Good Privacy (PGP). According to the authors, the strong point of their scheme is it does not have a single point of failure. This is in contrast to other proposals that follow the centralised model.

As with the previous subsections, Table 3 presents a comparison of PKI and PGP-based schemes proposed for DTNs.

3.2.2. Group Communication

Security in-group communications is a highly desirable feature in military and law enforcement DTN scenarios and the need of confidentiality in group communication grows at a day-by-day basis [51]. As presented in Table 4, nearly a handful of works [51–54] cope with group key management and specifically with rekeying in DTNs. Before delving into the details of the aforementioned works, it is to be noted that group key management protocols should take into account various security requirements such as forward and backward secrecy. More specifically, the most important security requirements for a group key management protocol are [55]:

- *Forward secrecy (FS)*—requires that users who left the group and know a contiguous subset of old group keys cannot discover subsequent group keys. This ensures that a member cannot decrypt data sent immediately after it leaves the group.
- *Backward secrecy (BS)*—mandates that a new user that joins the group and knows a contiguous subset of group keys cannot discover preceding group keys. This ensures that a member cannot decrypt data sent before it joins the group.
- *Collusion freedom (CF)*—requires that any set of fraudulent users who have much information about past keys should be incapable of deducing the current used group key.
- *Key independence (KI)*—requires that a passive adversary who knows any proper subset of group keys cannot compromise other past or future group keys. That is, the combination of backward and forward secrecy yields key independence.

The first attempt for group key management in DTNs is presented in [52]. Specifically, the authors proposed a group-oriented security solution for DTNs that provides access control and secure group communications. They suggest a centralised group key management mechanism based on the Logical Key Hierarchy (LKH). Group key management in DTN has been studied in [53] as well. The proposed protocol capitalizes on the Chinese Remainder Theorem (CRT). The concept of key lifetime is also introduced to alleviate the forward security problem in many-to-many DTN communication scenarios. In addition, the authors suggest that group key management for DTNs should use stateless and not stateful schemes such as LKH because there is no need for users to possess any previous keys. On the downside, the drawback in LKH scheme is that whenever a user joins or leaves, the group structure of tree has to be rearranged and logical key at each ancestor node has to be recomputed. Specifically, the computation cost is analogous to the network scale [54]. Actually, this is the reason why LKH scheme is unsuitable for space DTN.

More recently, another research work on group key management is given in [54]. More precisely, the authors propose an autonomic group key management (AGKM) scheme based on one-encryption-key multi-decryption-key (OMPK) key protocol for deep space DTNs. In this work, the authors also prove the forward, backward, passive security, and key independence qualities of their proposed protocol. In terms of efficiency, their scheme seems to produce a smaller penalty than other proposed (e.g., LKH), making it more suitable for deep space DTNs. Due to the lack of central key management center support, rekeying can be attained by a local leaving or joining user.

Last but not least, the work in [51] proposed a scheme which is based on a modified version of Chinese remainder theorem. By shifting more computing load onto the key server, their scheme optimize the number of re-key broadcast message. For simulation results Opportunistic Networking Environment (ONE) Simulator is used and the results suggest that this scheme is better than LKH as well as Chinese remainder group key schemes. More precisely, this scheme does not broadcast any key update message in case of user join or leave, thus making it very efficient for secure communication in DTNs. Their work, reduced the complexity of user leave from $O(n)$ to constant $O(1)$.

3.3. Key Revocation

Unitil now, only a couple of works about key revocation in DTN have been proposed. In particularly, the authors in [56] propose a new validation and revocation mechanism as well as a new design for a lightweight CRL in compliance with PKI (X.509) for DTNs. The new designed CRL is of reduced size and arranges the revocation list in the form of a Hash Table (Map) data structure to increase the searching efficiency. Moreover, in [57] the authors present a secure and fully distributed key revocation and update scheme for DTNs called Distributed Signing (DS) revocations. This is based on a DTN without a centralised PKI that ensures entity authentication and utilises the LCF trust system presented in [33]. More specifically, neighbouring friendly nodes attest and vouch for a node's identity during the key revocation process. Table 5 summarizes and compares these two key revocation schemes using the same criteria as in the previous tables.

3.4. Standardisation Efforts

Until now, a handful of Internet drafts have been released regarding security and key management in DTN, but no full-fledged solution is yet proposed. In [28,58] the authors states a series of requirements for key management in DTNs without proposing a solution. In fact, in RFC6257 [39] and in Internet draft [59] key management is recognized as a cumbersome topic and the authors explicitly state that such exclusion is a result of an informed decision. The BSP specification [39] defines security features for the BP [4] and attempts to protect its operation by introducing security mechanisms that provide confidentiality, integrity, and bundle authentication. More specifically, it describes four security blocks to cater for different security services. These blocks, namely the BAB, the PIB, the PCB and the Extensions Security Block (ESB), are defined in the Abstract Security Block (ASB). The Consultative Committee for Space Data Systems (CCSDS) released a green book [60] about key management concept in space environments, where they described the basics for the CCSDS standardization activities related to security services and key management schemes for space missions. In addition, an internet draft about DTN security services is given in [59], where the Streamlined Bundle Security Protocol (SBSP) is introduced. Specifically, SBSP is an improvement and simplification on BSP and provides authentication, integrity, and confidentiality for the "bundles" along the transmission path. It combines BSB with Bundle-in-Bundle encapsulation (BIBE) and supports three security blocks, namely BAB, BIB and BCB. As expected, SBSP applies only to security-aware nodes. More recently, the DTN Networking Security Key Management [61] and DTN Security Key Management [62] have been released. The former states the key management problem in DTNs and emphasizes that traditional security key management mechanisms are not always feasible in environments where DTN typically operate in. The latter proposes requirements and presents a design for key management in DTNs. Specifically, the core requirements and design criteria for DTN security key management are described. The newly published Internet draft [63] defines the DTN key management problem and at the same time provides high-level solutions for public key distribution and public key revocation. Finally, the Bundle Protocol Security Specification (BPSec) [64] defines a security protocol for the services of end-to-end data integrity and confidentiality of the BP. Table 6 summarizes all the security-related Internet drafts and RFCs.

Table 6. Security-related internet drafts and RFCs.

Title	Naming Conventions	Released Date	Expiration Date
DTN Key Management Requirements [58]	draft-farrell-dtnrg-km-00	June 2007	December 2007
Delay-Tolerant Networking Security Overview [28]	draft-irtf-dtnrg-sec-overview-06	March 2009	September 2009
Bundle Security Protocol Specification [39]	RFC6257	May 2011	-
Space Mission Key Management Concept [60]	CCSDS 350.6-G-1	November 2011	-
Delay Tolerant Networking Security Key Management - Problem Statement [61]	draft-templin-dtnskmps-00	March 2014	September 2014
Streamlined Bundle Security Protocol Specification [59]	draft-irtf-dtnrg-sbsp-01	May 2014	November 2014
DTN Security Key Management - Requirements and Design [62]	draft-templin-dtnskmreq-00	February 2015	August 2015
Architecture for a Delay-and-Disruption Tolerant Public-Key Distribution Network (PKDN) [63]	draft-viswanathan-dtnwg-pkdn-00	August 2015	February 2016
Bundle Protocol Security Specification [64]	draft-ietf-dtn-bpsec-04	March 2017	September 2017

4. Discussion

In the previous section we have classified the proposed solutons of cryptographic key management in DTNs into three major categories. However, as shown in the corresponding subsections, the majority of the examined approaches are hybrid in nature and may fall into more than one category. Characteristic examples of this situation are the works in [12,24,25,31,35], where the authors propose schemes that can be used in security initialisation and key establishment. Contributions such as [34,65] have shown that establishing the initial source context at the deployment phase is still an open issue. From Table 1 we can observe that the majority (8 out of 12) of the security initialisation methods are based on PKC. A number of other methods for security initialisation have relied on IBC, such as HIBC and its variations.

Also, there is an almost unanimous agreement, that traditional PKI is not always suitable for DTN. Specifically, in disconnected DTNs, without online access to the necessary certificate or the certificate revocation list posted by CAs, sending an encrypted message and authenticate senders' identity is infeasible. For this reason, apart from PKI, IBC has been examined as a viable solution for security within the DTN context. From Tables 2 and 3 it can be observed that few works propose the usage of pre-shared keys or pre-established trust between the nodes [41,47]. However, it is obvious that for scalability reasons such schemes apply only in a small and fixed-size DTNs.

By observing Table 4 it is clear that group key management for DTN is still in its infancy, with only four proposed works based on LKH or Chinese Remainder Theorem. Moreover, as given in Table 5, even fewer works proposed ways of handling key revocation in DTNs. It is worth mentioning that researches tried to address the key revocation issue almost eleven years (2016) after the first work related to key management in DTNs has been published [24]. To further exemplify this, Figure 2 provides a timeline of all the different methods introduced for key management in DTNs. It can be noticed that all the different methods proposed between 2005 and 2013 and the rest of the papers are based on the already proposed methods. Moreover, the bottom part of the same figure, includes the different kind of DTN network that is addressed by each work. For instance, the first chronologically proposed works on DTN key management focused on rural area DTNs, while the last ones on large scale DTNs.

In addition, as it can be seen from Tables 1–5, when applicable all the solutions included in this survey have been either evaluated only through theoretical proofs and/or simulations. This means that hardware testbeds and real-life deployments in cryptographic key management are still largely missing from the DTN research area. On top of that, up to date, most of the works in the context of key management in DTNs concentrate on rural or space networks neglecting other DTN applications, including vehicular or undersea ones. Last but not least, the analysis of the various works showed that the most recent ones (after 2012) tend to focus on space DTNs and generally on large scale DTNs.

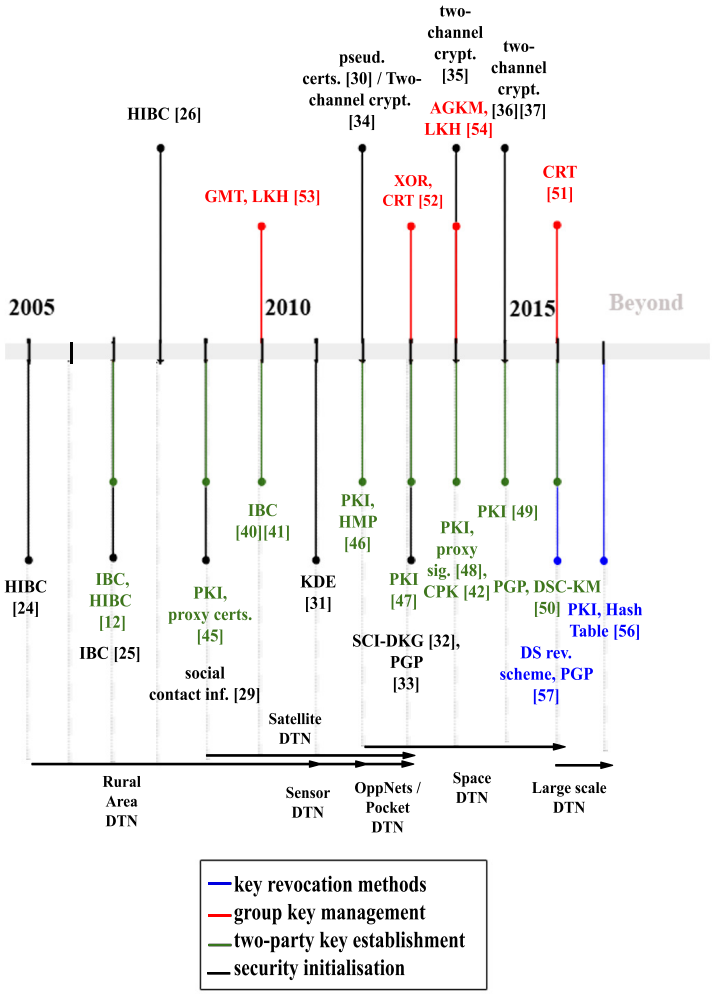

Figure 2. DTN key management timeline.

5. Alternative Key Management Taxonomies in DTNs

5.1. Require or Not Trusted Third Party (TTP)

Key management solutions can also be categorised based on whether they require a TTP or not. A TTP can be used for key management services such as key generation, key distribution or translation or keying material and certification [66]. Traditionally, in continuously connected networks the most proven practice for the key management is to contact an online TTP. Although the approach that imposes a TTP is secure and resilient, it is also not scalable for DTNs. In fact, DTNs require a different approach for handling key management. This is because every pair of nodes has to obtain keys from the online TTP, something that can not be guaranteed in DTNs with intermittent connectivity. Moreover, this approach has sizable communication overhead, which is unwelcome for DTNs. Also, the TTP constitutes a single point of failure. On the other hand, works that are self-organised may not have the aforementioned problems, but are applicable only to small size networks due to the computational overhead produced. Most of the works that do not require TTP tried to solve the security initialisation problem as an alternative solution, while most of the works that require TTP attempted to solve the key establishment, without considering the open issue of security initialisation. Contributions that require a TTP increase the communication overhead, while those which do not rely on a TTP produce additional computation overhead. As a result, both approaches can not always apply in such a hostile environment. Below, we categorize the majority of the works included in this survey based on the existence or not of TTP.

- *Require TTP*—Works such as [45–49] are based on PKI solutions mandate a TTP, and thus a CA. Works such as [12,24–26,40,41] that are founded on IBC solutions, require a TTP too, namely the PKG. In addition, schemes in group key management that rely on LKH such as [52,54], necessitate a TTP known as Key Distribution Center (KDC). Moreover, the work in [42], which is based on CPK, eliminates the need for online TTP and only needs an off-line PKG.
- *No TTP is required*—Works that rely on PGP [33,50] and two-channel cryptography [34] are self-organised [30,35] and do not require a TTP.

5.2. Centralised, Decentralised and Distributed

Key management solutions in DTN can be divided into three major categories, namely (a) centralised, (b) decentralised, and (c) distributed architecture. The schemes in the first category mandate the use of a TTP, and so far are the most commonly used and studied in the respective literature. Decentralised schemes on the other hand use more than one group to manage key distribution and are used with the purpose of sharing the overhead between the parties. The latter category of schemes pertains to group key management protocols, and therefore it imposes multiple cryptographic operations. This typically results to large communication and computational overheads [53]. Unfortunately, the various solutions proposed for the existing wired/wireless networks cannot apply to DTNs, because of the communication and computational overhead [53]. Also, in the DTN literature, the difference between decentralised and distributed models is unclear and sometimes is considered the same. Overall, due to its nature, the distributed model is more tolerant to infrastructure failures. This is in contrary to the centralised model which consists a single point of failure. Moreover, in the centralised model, join and leave operations for members are straightforward, but all communications require interaction with the TTP. The decentralised/distributed model not only makes privacy a hard issue to deal with, but also the more nodes in the network the more storage is needed, which is impractical in DTNs with low storage capabilities. Generally, works following the PGP philosophy are decentralised and distributed, while the rest of them which require a TTP, such as CA or PKG, are centralised. Lastly, it is to be noted that the three-fold taxonomy included in this subsection is most commonly used in group communications [67]. Tables 1–5 summarise the architecture used by each scheme.

6. Open Research Challenges

From the above discussion it becomes obvious that DTN architecture has a number of open issues that must be tackled. Many of them are directly related with the security factor in DTNs and are still open due to disagreements in the DTNRG and/or to the partial insufficiency of the research works in the field [28].

- *Key Management*—As already mentioned, cryptographic key management is the major open issue in DTNs and especially in deep space communications. Section 3 presents and categorises all the schemes proposed until now. Constraints in resources such as memory, power, storage, computation, and bandwidth in DTN nodes put additional challenges on the key management. Resource-conscious key management techniques become a necessity in DTNs. The key management issues that require further research are listed below:
  - *Security initialisation*—Security initialisation is an expensive procedure and considering the dynamic nature of DTNs is difficult to handle. As already discussed, the two main approaches are with either a TTP or self-organised. Both approaches have their advantages and disadvantages.
  - *Key update/key lifetime*—Key lifetime is difficult to choose and must vary based on the different constraints of DTN environments. For instance, if the key update period is too long, the corresponding key may be exposed. If it is is too short, frequent updates can add large overhead.

  - *Key storage*—Considering storage limitations in DTNs in general, and sensor or deep space DTNs in particular, each node must handle the number of possible keying material stored, based on a number of factors, including the number of neighbors, key validity, key expiration, key usage rate, length as well as other stored bundles. Apart from the volume, private keys must be stored securely to avoid compromisation.
  - *Key revocation*—Key revocation is impractical in DTNs due to the nature of DTNs. Different approaches must be used instead, depending on the specific network constraints.

- *Handling Replays*—In DTN networks, due to scarce network resources, the replayed volume of messages must be reduced to the minimum possible. However, this is not always the case due to various DTN scenarios (i.e., authentication scenarios) where at least some replay messages are desirable. Moreover, the huge delays in such networks, complicates handling replays, and therefore the formulation of a DTN replay protection scheme becomes very challenging.
- *Traffic Analysis*—There are not any security services for protecting/deterring against traffic analysis. However, for some disruption tolerant networks such as military ones, hiding traffic is rather a sine qua non.
- *Routing Protocol Security*—There are no well-documented DTN routing protocols, so DTN routing protocol security is an open issue. However, some of the existing security features of the underlying protocols can be used.
- *Multicast Security*—Currently, there is no mechanism to separate between a multicast and anycast endpoint. DTN security architecture does not address the security aspects of enabling a DTN node to register with a particular multicast or anycast endpoint identifier at all.
- *Performance Issues*—Security within a DTN imposes both bandwidth utilization costs on the communication links and computational costs at the nodes. In addition, there may be certain limitations regarding how much CPU, storage, energy, and so on can be devoted to security, and the amount of computation costs will undoubtedly depend on the underlying algorithms and their associated parameters.
- *Naming*—DTN naming is a hard open issue to cope with [9]. For instance, how names are to be used in routing, and the ways this will be mapped to the underlying routing of each convergence layer network, remains unclear. A properly constructed naming system can aid in simplifying both routing and security. That is, for security and resource allocation reasons, one would overwhelmingly prefer to be able to uniquely identify a source as well as to determine which group or groups this source may belong to.

7. Conclusions & Future Research

This survey is devoted to cryptographic key management mechanisms in DTNs. Though in its early stages, various methods have been proposed to address the challenging task of security and cryptographic key management in such restricted and challenging networks. From the analysis conducted, it emerges that the proposed methods are still far away from being real effective and further research attention is required [49]. Putting it another way, research on cryptographic key management, in such challenged networks is still in its infancy as the field is relatively new.

To spur and fuel further research efforts in this area, we have made an in-depth study of the solutions proposed so far in the literature and classified them into three major classes depending on which phase of key management each survey work addresses. As a future work, we intend to make an objective performance evaluation of the proposed methods considering characteristics and limitations of diverse DTN environments.

Author Contributions: All authors have written and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DTNs	Delay Toleran Networks
BP	Bundle Protocol
PKI	Public Key Infrastructure
IBC	Identity Based Cryptography
PKC	Public-Key Cryptography
PKG	Private Key Generator
CA	Certificate Authority
IPN	InterPlanetary Networking
BSP	Bundle Security Protocol
BAB	Bundle Authentication Block
PIB	Payload Integrity Block
PCB	Payload Confidentiality Block
GCM	Galois Counter Mode
HIBC	Hierarchical Identity Based Cryptography
OppNets	Opportunistic Networks
DKE	Distributed Key Establishment
CRL	Certificate Revocation List
SKC	Secret Key Crypography
WoT	Web of Trust
DVD	Dynamic Virtual Digraph
BSP	Bundle Security Protocol
BP	Bundle Protocol
SOK	Sakai-Ohgishi-Kasahara
LCF	Leverage of Common Friends
CPK	Combined Public Key
ECC	Elliptic Curves Cryptography
PGP	Pretty Good Privacy
HMP	Horsters-Michels-Petersen
ESKTS	Efficient and Scalable Key Transport Scheme
DSC-KM	Digital Signature Chains Key Management Scheme
FS	Forward secrecy
BS	Backward secrecy
CF	Collusion freedom
KI	Key independence
LKH	Logical Key Hierarchy
CRT	Chinese Remainder Theorem
AGKM	Autonomic Group Key Management
OMPK	One-encryption-Key Multi-decryption-Key
ONE	Opportunistic Networking Environment
DS	Distributed Signing
ESB	Extension Security Block
ASB	Abstract Security Block
CCSDS	Consultative Committee for Space Data Systems
SBSP	Streamlined Bundle Security Protocol
BIBE	Bundle-in-Bundle encapsulation
BPSec	Bundle Protocol Security Specification
TTP	Trusted Third Party
KDC	Key Distribution Center

References

1. Wu, B.; Wu, J.; Cardei, M. A Survey of Key Management in Mobile Ad Hoc Networks. In *Handbook of Research on Wireless Security*; IGI Global: Hershey, PA, USA, 2010.
2. Menesidou, S.; Vardalis, D.; Katos, V. Automated key exchange protocol evaluation in delay tolerant networks. *Comput. Secur.* **2016**, *59*, 1–8.
3. Cerf, V.; Burleigh, S.; Hooke, V.; Torgerson, L.; Durst, R.; Scott, K.; Fall, K.; Weiss, H. *Delay-Tolerant Networking Architecture*; Rfc4838; DTN Research Group: New York, NY, USA, 2007.
4. Scott, K.; Burleigh, S. *Bundle Protocol Specification*; Rfc5050; DTN Research Group: New York, NY, USA, 2007.
5. Warthman, F. *Delay-Tolerant Networks (DTNs): A Tutorial*; Technical Report; DTNs: Los Angeles, CA, USA, 2003.
6. Adams, C.; Lloyd, S. *Understanding PKI: Concepts, Standards, and Deployment Considerations*, 2nd ed.; Addison-Wesley Longman Publishing Co., Inc.: Boston, MA, USA, 2002.
7. Shamir, A. Identity-based Cryptosystems and Signature Schemes. In *Proceedings of CRYPTO 84 on Advances in Cryptology*; Springer: New York, NY, USA, 1985; pp. 47–53.
8. Law, Y.W.; Corin, R.; Etalle, S.; Hartel, P.H. A Formally Verified Decentralized Key Management Architecture for Wireless Sensor Networks. In Proceedings of the Personal Wireless Communications (PWC 2003), Venice, Italy, 23–25 September 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 27–39.
9. Ivancic, W. Security analysis of DTN architecture and Bundle Protocol Specification for space-based networks. In Proceedings of the Aerospace Conference, Big Sky, MT, USA, 6–13 March 2010; pp. 6–13.
10. Zamani, A.; Zubair, S. Secure and Efficient Key Management Scheme in MANETs. *OSR J. Comput. Eng.* **2014**, *16*, 146–158.
11. Fall, K. A delay-tolerant network architecture for challenged internets. In Proceedings of the ACM SIGCOMM 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Karlsruhe, Germany, 25–29 August 2003; pp. 27–34.
12. Kate, A.; Zaverucha, G.; Hengartner, U. Anonymity and security in delay tolerant networks. In Proceedings of the Securecomm 2007, Nice, France, 17–21 September 2007; pp. 504–513.
13. Ochiai, H.; Ishizuka, H.; Kawakami, Y.; Esaki, H. A DTN-Based Sensor Data Gathering for Agricultural Applications. *IEEE Sens. J.* **2011**, *11*, 2861–2868.
14. Mashhadi, A.; Ben Mokhtar, S.; Capra, L. Habit: Leveraging human mobility and social network for efficient content dissemination in Delay Tolerant Networks. In Proceedings of the 2009 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops, Kos, Greece, 15–19 June 2009; pp. 1–6.
15. Burgess, J.; Gallagher, B.; Jensen, D.; Levine, B. MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks. In Proceedings of the INFOCOM 2006—25th IEEE International Conference on Computer Communications, Barcelona, Spain, 23–29 April 2006; pp. 1–11.
16. Caini, C.; Cruickshank, H.; Farrell, S.; Marchese, M. Delay- and Disruption-Tolerant Networking (DTN): An Alternative Solution for Future Satellite Networking Applications. *Proc. IEEE* **2011**, *99*, 1980–1997.
17. Chitre, M.; Shahabudeen, S.; Freitag, L.; Stojanovic, M. Recent advances in underwater acoustic communications and networking. In Proceedings of the OCEANS 2008, Quebec City, QC, Canada, 15–18 September 2008; pp. 1–10.
18. Husni, E. Rural Internet service system based on Delay Tolerant Network (DTN) using train system. In Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, Bandung, Indonesia, 17–19 July 2011; pp. 1–5.
19. Voyiatzis, A. A Survey of Delay- and Disruption-Tolerant Networking Applications. *J. Internet Eng.* **2012**, *5*, 331–344.
20. Sourceforge: Delay Tolerant Networking. Available online: http://sourceforge.net/projects/dtn/files/DTN2/ (accessed on 7 June 2017).
21. Interplanetary Overlay Network DTN (ION-DTN). Available online: http://sourceforge.net/projects/ion-dtn/ (accessed on 7 June 2017).
22. IBR-DTN. Available online: https://www.ibr.cs.tu-bs.de/projects/ibr-dtn/ (accessed on 7 June 2017).
23. DTN-Bytewalla. Available online: https://sourceforge.net/projects/bytewalla/ (accessed on 7 June 2017).

24. Seth, A.; Keshav, S. Practical Security for Disconnected Nodes. In Proceedings of the First International Conference on Secure Network Protocols, Boston, MA, USA, 6 November 2005; IEEE Computer Society: Washington, DC, USA, 2005; pp. 31–36.
25. Asokan, N.; Kostiainen, K.; Ginzboorg, P.; Ott, J.; Luo, C. Applicability of Identity-based Cryptography for Disruption-tolerant Networking. In Proceedings of the 1st International MobiSys Workshop on Mobile Opportunistic Networking, San Juan, PR, USA, 11 June 2007; ACM: New York, NY, USA, 2007; pp. 52–56.
26. Patra, R.; Surana, S.; Nedevschi, S. Hierarchical identity based cryptography for end-to-end security in DTNs. In Proceedings of the 2008 4th International Conference on Intelligent Computer Communication and Processing, Cluj-Napoca, Romania, 28–30 August 2008; pp. 223–230.
27. Wood, L.; Eddy, W.; Holiday, P. A bundle of problems. In Proceedings of the Aerospace conference 2009, Big Sky, MT, USA, 7–14 March 2009; pp. 1–14.
28. Farrell, S.; Symington, S.; Weiss, H.; Lovell, P. *Delay-Tolerant Networking Security Overview*; Draft-Irtf-Dtnrg-Sec-Overview-06, Expires: September 2009; DTN Research Group: New York, NY, USA, 2009.
29. El Defrawy, K.; Solis, J.; Tsudik, G. Leveraging Social Contacts for Message Confidentiality in Delay Tolerant Networks. In Proceedings of the 2009 33rd Annual IEEE International Computer Software and Applications Conference, Seattle, WA, USA, 20–24 July 2009; Volume 1; pp. 271–279.
30. Shikfa, A.; Önen, M.; Molva, R. Local Key Management in Opportunistic Networks. *Int. J. Commun. Netw. Distrib. Syst.* **2012**, *9*, 97–116.
31. Du, J.; Kranakis, E.; Nayak, A. Distributed Key Establishment in Disruption Tolerant Location Based Social Wireless Sensor and Actor Network. In Proceedings of the 2011 Ninth Annual Communication Networks and Services Research Conference, Ottawa, ON, Canada, 2–5 May 2011; IEEE Computer Society: Washington, DC, USA, 2011; pp. 109–116.
32. Xie, Y.; Wang, G. Practical distributed secret key generation for delay tolerant networks. *Concurr. Comput. Pract. Exp.* **2013**, *25*, 2067–2079.
33. Djamaludin, C.; Foo, E.; Corke, P. Establishing initial trust in autonomous Delay Tolerant Networks without centralised PKI. *Comput. Secur.* **2013**, *39*, 299–314.
34. Jia, Z.; Lin, X.; Tan, S.H.; Li, L.; Yang, Y. Public Key Distribution Scheme for Delay Tolerant Networks Based on Two-channel Cryptography. *J. Netw. Comput. Appl.* **2012**, *35*, 905–913.
35. Lv, X.; Mu, Y.; Li, H. Non-Interactive Key Establishment for Bundle Security Protocol of Space DTNs. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 5–13.
36. Jadhav, C.; Dhainje, B.; Pradeep, K. Secure Key Establishment for Bundle Security Protocol of Space DTNs in Noninteractive manner. *Int. J. Comput. Sci. Inf. Technol.* **2015**, *6*, 944–946.
37. Mukundhan, E.; Veeramani, M. Bundle Security Protocol of Space DTNs Using Cryptographic Algorithm. *Int. J. Comput. Tech.* **2015**, *2*, 51–54.
38. Mashatan, A.; Stinson, D.R. Practical Unconditionally Secure Two-channel Message Authentication. *Des. Codes Cryptogr.* **2010**, *55*, 169–188.
39. Symington, S.; Farrell, S.; Weiss, H.; Lovell, P. *Bundle Security Protocol Specification*; Rfc6257; DTN Research Group: New York, NY, USA, 2011.
40. Ahmad, N.; Cruickshank, H.; Sun, Z. ID Based Cryptography and Anonymity in Delay/Disruption Tolerant Networks. *LNICST* **2010**, *43*, 265–275.
41. Van Besien, W. Dynamic, Non-interactive Key Management for the Bundle Protocol. In Proceedings of the 5th ACM Workshop on Challenged Networks, Chicago, IL, USA, 20–24 September 2010; ACM: New York, NY, USA, 2010; pp. 75–78.
42. Ding, Y.; Zhou, X.; Cheng, Z.; Zeng, W. Efficient Authentication and Key Agreement Protocol with Anonymity for Delay Tolerant Networks. *Wirel. Pers. Commun.* **2013**, *70*, 1473–1485.
43. Pentland, A.; Fletcher, R.; Hasson, A. DakNet: Rethinking connectivity in developing nations. *Computer* **2004**, *37*, 78–83.
44. Le, Z.; Vakde, G.; Wright, M. PEON: Privacy-enhanced opportunistic networks with applications in assistive environments. In Proceedings of the 2nd International Conference on PErvsive Technologies Related to Assistive Environments, Corfu, Greece, 09–13 June 2009; ACM Press: New York, NY, USA, 2009; pp. 1–8.

45. Bhutta, N.; Ansa, G.; Johnson, E.; Ahmad, N.; Alsiyabi, M.; Cruickshank, H. Security analysis for Delay/Disruption Tolerant satellite and sensor networks. In Proceedings of the 2009 International Workshop on Satellite and Space Communications (IWSSC), Siena, Italy, 9–11 September 2009; pp. 385–389.
46. Menesidou, S.A.; Katos, V. Authenticated Key Exchange (AKE) in Delay Tolerant Networks. In Proceedings of the 27th IFIP International Information Security and Privacy Conference, Crete, Greece, 4–6 June 2012; Gritzalis, D., Furnell, S., Theoharidou, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 376, pp. 49–60.
47. Johnson, E.; Cruickshank, H.; Sun, Z. Providing Authentication in Delay/Disruption Tolerant Networking (DTN) Environment. In *Personal Satellite Services*; Pillai, P., Shorey, R., Ferro, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; Volume 52; pp. 189–196.
48. Bhutta, N.; Cruickshank, H.; Sun, Z. An Efficient, Scalable Key Transport Scheme (ESKTS) for Delay/Disruption Tolerant Networks. *Wirel. Netw.* **2014**, *20*, 1597–1609.
49. Rajan, G.; Cho, G. Applying a Security Architecture with Key Management Framework to the Delay/Disruption Tolerant Networks. *Int. J. Secur. Its Appl.* **2015**, *9*, 327–336.
50. Andrade, D.D.; Albini, L.C.P. Fully Distributed Public Key Management through Digital Signature Chains for Delay and Disrupt Tolerant Networks. In Proceedings of the 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Brasilia, Brazil, 10–13 October 2016; pp. 316–324.
51. Gupta, M. Group Key Exchange Management in Delay Tolerant Network. *Int. J. Comput. Appl.* **2016**, *144*, 16–19.
52. Edelman, P.; Donahoo, M.; Sturgill, D. Secure group communications for Delay-Tolerant Networks. In Proceedings of the 2010 International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 8–11 Novemebr 2010; pp. 1–8.
53. Xu, G.; Chen, X.; Du, X. Chinese Remainder Theorem based DTN group key management. In Proceedings of the 2012 IEEE 14th International Conference on Communication Technology (ICCT), Chengdu, China, 9–11 November 2012; pp. 779–783.
54. Zhou, J.; Song, M.; Song, J.; Zhou, X.; Sun, L. Autonomic Group Key Management in Deep Space DTN. *Wirel. Pers. Commun.* **2014**, *77*, 269–287.
55. Barskar, R.; Chawla, M. A Survey on Efficient Group Key Management Schemes in Wireless Network. *Indian J. Sci. Technol.* **2016**, *9*, doi:0.17485/ijst/2016/v9i14/87972.
56. Bhutta, M.; Cruickshank, H.; Sun, Z. Public-key infrastructure validation and revocation mechanism suitable for delay/disruption tolerant networks. *IET Inf. Secur.* **2016**, *11*, 16–22.
57. Djamaludin, C.; Foo, E.; Camtepe, S.; Corke, P. Revocation and update of trust in autonomous delay tolerant networks. *Comput. Secur.* **2016**, *60*, 15–36.
58. Farrell, S. *DTN Key Management Requirements*; Draft-Farrell-Dtnrg-Km-00, Expires: December 2007; DTN Research Group: New York, NY, USA, 2007.
59. Birrane, S. *Streamlined Bundle Security Protocol Specification*; Draft-Irtf-Dtnrg-Sbsp-01, Expires: November 2014; DTN Research Group: New York, NY, USA, 2014.
60. CCSDS. *Space Mission Key Management Concept*; Report, CCSDS 350.6-G-1, Green Book, Issue 1; CCSDS: Darmstadt, Germany, 2011.
61. Templin, F. *Delay Tolerant Networking Security Key Management—Problem Statement*; Draft-Templin-Dtnskmps-00, Expires: September 2014; Network Working Group: Ottawa, ON, Canada, 2014.
62. Templin, F. *DTN Security Key Management—Requirements and Design*; Draft-Templin-Dtnskmreq-00, Expires: August 2015; Network Working Group: Ottawa, ON, Canada, 2015.
63. Viswanathan, K.; Templin, F. *Architecture for a Delay-and-Disruption Tolerant Public-Key Distribution Network (PKDN)*; Draft-Viswanathan-Dtnwg-Pkdn-00, Expires: February 2016; Network Working Group: Ottawa, ON, Canada, 2015.
64. Birrane, E.; McKeever, K. *Bundle Protocol Security Specification*; Draft-Ietf-Dtn-Bpsec-04, JHU/APL; Network Working Group: Ottawa, ON, Canada, 2017.
65. Farrell, S.; Cahill, V. Security considerations in space and delay tolerant networks. In Proceedings of the Second IEEE International Conference on Space Mission Challenges for Information Technology, Madrid, Spain, 27–29 September 2006; pp. 8–38.

66. Fumy, W. Key Management Techniques. *State of the Art in Applied Cryptography, Course on Computer Security and Industrial Cryptography—Revised Lectures*; Springer: London, UK, 1998; pp. 142–162.
67. Challal, Y.; Seba, H. Group Key Management Protocols: A Novel Taxonomy. *Int. J. Comput. Electr. Autom. Control Inf. Eng.* **2008**, *2*, 105–118.