Authenticated Key Exchange (AKE) in Delay Tolerant Networks

Sofia Anna Menesidou and Vasilios Katos

Information Security and Incident Response Unit
Department of Electrical and Computer Engineering
Democritus University of Thrace
University Campus, Xanthi 67100, Greece
{smenesid,vkatos}@ee.duth.gr
http://isir.ee.duth.gr/

Abstract. Key exchange is considered to be a challenging problem in Delay Tolerant Networks (DTNs) operating in space environments. In this paper we investigate the options for integrating key exchange protocols with the Bundle Protocol. We demonstrate this by using a one-pass key establishment protocol. In doing so, we also highlight the peculiarities, issues and opportunities a DTN network maintains, which heavily influences the underlying security solution.

Keywords: Bundle Security Specification.

1 Introduction

Delay or Disruption Tolerant Networks (DTNs) are becoming popular both in terrestrial and deep space environments as they maintain certain advantages over traditional internetworking protocols such as TCP/IP. The benefits of adopting DTN technologies are clear in environments where connectivity in terms of end to end path availability cannot be guaranteed for the lifetime of a communications session.

Although DTNs by nature may support high availability (which in DTN terminology is referred to as reliability), they are not short of security issues. This is primarily due to the constraints of the unwelcoming and hostile in terms of communication environments the DTNs operate in. The three main limitations composing a typical space internetworking environment are the limited bandwidth, the relatively high bit error rates and the periods lacking connectivity where in some cases open loop communications is the only option.

The limited bandwidth dictates that the overheads should be kept to a minimum. As such, elaborate and message-rich cryptographic protocols are not suitable for deep space DTN applications. The integrity issues introduced by the high

D. Gritzalis, S. Furnell, and M. Theoharidou (Eds.): SEC 2012, IFIP AICT 376, pp. 49–60, 2012.

bit error rates are mainly accidental rather malicious by nature, and therefore cryptographic integrity checksums could be simplified. Lastly, the large delays in principle make interactive and many-pass protocols unsuitable. Interactive security protocols involve a series of computations to be performed by all participating entities in an asynchronous yet orderly manner. There is a wealth of efficient protocols in the literature which cannot always be adopted due to the limitations of the environment. However, it seems that making assumptions that allow a limited use of these protocols, one can establish a security context on an higher initial cost (in terms of bandwidth) and then leverage the arranged setup to perform non-interactive type of security protocols without any significant decrease of security. For example, public key cryptography and protocols based on Diffie Hellman type of exchanges are not suitable for an ongoing and regular use, but limiting their invocation at the beginning of an association between the parties would result to a system offering practical and acceptable level of security. This is possible as the network topology in a space internetwork is fairly fixed.

On the other hand, certain security assumptions do not necessarily hold in a space internetworked environment. A fixed topology mentioned above requires a significant physical effort to change and as a result opportunities for a Man-In-The-Middle attack between two trusted nodes are rather slim. Yet, in DTN environments and particularly in deep space communications where each and every opportunity for sending data should be exploited to the highest possible means for economic reasons (amongst others) there may be a situation where it would be feasible and preferable to send data through a DTN node which is not trusted. In such case the sender is knowingly sending her data through a man in the middle which may or may not behave maliciously. In terms of DTN and deep space communication, a malicious action by the adversary targets confidentiality and/or integrity of the data; availability is generally treated by the DTN itself.

All the above suggest that the security goals for a space internetworked environment should be carefully selected and prioritized in order to select the most suitable authenticated key establishment protocol. This paper studies the assumptions and requirements for selecting a suitable AKE protocol in space internetworking applications against the limitations, opportunities and particular issues that apply in such environments.

2 Related Work

The area of key management in delay tolerant networks is relatively new and many research challenges remain to date; the DTN Research Group acknowledges key management as an open issue [10]. Traditional key management and AAA-like architectures are not suitable for DTN networks due to the environment limitations and technical constrains [3]. The work done until now is based on the assumption of shared keying material [26]. However, no method for automatic key distribution or agreement is yet defined within the bundle architecture.

The author in [10] states some requirements for key management in delay tolerant networks but no solution is yet proposed. Until now, a few solutions have been proposed to address this problem.

The authors in [2] introduce a solution based on Identity-Based Cryptography (IBC). IBC is a cryptographic method that enables message encryption and signature verification using a public identifier. In [15] the authors use the non-interactive Sakai-Ohgishi-Kasahara (SOK) key agreement scheme which is based on Boneh-Franklin IBC scheme. However, such IBC solutions appeared to superficially solve the problem [11].

In [4] the authors present a number of security goals and attributes for a key agreement protocol. In the same work they compare the key agreement protocols based on the intractability of Diffie-Hellman problem such as the ephemeral and static Diffie-Hellman, the KEA, the Unified Model and the MQV protocols. They also compare the one-pass version of these protocols. One-pass AK protocols are more efficient because they use only one message transmission. However such protocols have some security drawbacks because they do not offer known-key security and forward secrecy [4]. Another survey of the existing key establishment protocols is the work in [23]. The authors describe and compare a number of protocols using both symmetric and asymmetric techniques.

The work in [5] proposed one-pass authenticated key establishment protocol based on the Bellare Rogaway model for one-way communications. Their scheme is a slight adaptation on the basic elliptic curve Diffie-Hellman (ECDH) protocol with an authentication mechanism based on bilinear pairings. Even though their scheme is the strongest against the general key-compromise impersonation (K-CI) attack compared to one-pass versions of MQV, HMQV and CMQV, the use of bilinear pairings, makes this scheme less efficient [6]. Work in [19] proposes a two-pass authenticated key agreement protocol with key confirmation (2P-AKACP) and the one-pass version of this protocol (1P-AKACP) for one-way communications. Both protocols are based on the discrete logarithm problem (DLP) and have three phases: the registration, the transfer and verification, and the key generation. In addition the security and the computational complexities of these schemes outperform the protocols that are based on [22],[8,9]. However their claim proved incorrect and a several types of attacks presented in both protocols [7].

More recently, the author in [25] presents a dynamic and non-interactive key management for opportunistic networks using the Bundle Security Protocol (BSP). This means that the key management scheme will be used to derive keys for HMAC-SHA1 authentication, RSA digital signature and AES encryption which are the cipher-suits of BSP. Their scheme is based on the bilinear mappings over elliptic curves. In [14] the authors propose a dynamic virtual digraph (DVD) model for DTN public key distribution. They heuristically define the DVD model by extending the traditional graph theory and they also propose a two-channel public key distribution scheme.

3 Authenticated Key Establishment

3.1 The Setting

A representative scenario is depicted in Fig.1. Assume that the rover A, satellite C and ground station belong to Organisation A, whereas satellite B belongs to Organisation B. All devices are DTN enabled and nodes B and C can serve as intermediary routers. In deep space DTN terms, loss of connection availability can be accurately predicted and routing decisions can be planned in advance. As such, the sending node will be able to make risk assessment decisions and adopt the appropriate security controls. In our example scenario there is no line of sight between the rover and the trusted satellite C - hence no available communications channel - and therefore the former needs to route through the untrusted satellite B. An example security policy would require that the contents of the payload must not be available to node B, so confidentiality must be supported.

Encryption can be triggered on an intermediary node, if such node schedules (routes) transmission of the data through an untrusted node. Unlike conventional TCP/IP, each DTN node implements the Bundle Protocol where a *custodian* of the data is defined and the data may reside on the DTN router for a large amount of time. Therefore, while the data is arranged to be transmitted some time in the not-so-close future (in TCP/IP timings), the router/custodian of the data may have the option to further process the payload *in situ*. In fact, an optimal solution could involve a source sending immediately the plaintext data to its neighboring trusted node if there is a transmission window of opportunity, and some custodian along the transmission path may decide to encrypt the data. Once the data is encrypted, the decryption should be expected to take place at the DTN endpoint. The decision to encrypt the data could be influenced by the routing as mentioned earlier, but also by the QoS conditions. For example, there may be a security policy to encrypt data by default when they follow a certain path, but this requirement could be overridden if there are data that need to be sent urgently (that is, a preference of QoS over confidentiality), since a missed opportunity to transmit the data may result to long, unacceptable delays. These peculiarities appear in a DTN environment and introduce interesting challenges and issues surrounding the selection and application of cryptographic protocols.

One of the main challenges yet to be addressed in such environments is key management. The recently published Bundle Security Protocol Specification [24] does not cover key management and the authors explicitly state that such exclusion is a result of an informed decision. The analysis and proposed solution that follows is an attempt to identify the constraints and requirements of the described scenario above and to suggest a suitable set of security protocols for the key transport problem and more specifically for authenticated key establishment.

3.2 Preliminaries, Goals and Requirements

As already mentioned in the scenario above, confidentiality is the security requirement that must be fulfilled. In order to succeed that we need an authenticated key agreement protocol between the rover A and the satellite B. However,

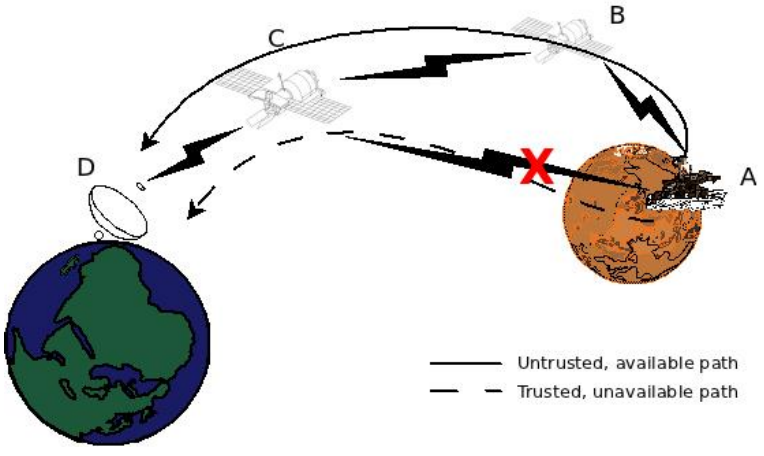

Fig. 1. A deep space communications example

we assume that both entities have pre-established long term keys. Based on this scenario the protocol we propose must satisfy a key agreement mechanism of the ISO/IEC 11770 [13]. The first time both entities will agree on a shared secret key, a three-pass protocol of the key agreement mechanism 10 of the ISO standard will be used. This mechanism uses elliptic curve cryptography to establish a shared secret with mutual implicit authentication. The next time both entities are going to establish a shared secret key based on mechanism 2 which is an one-pass key agreement protocol that establishes a shared secret to both entities with implicit key authentication but no entity authentication.

The key agreement protocols we selected for comparison are the Key Exchange Algorithm (KEA) [20], the one-pass version (KEA1) and the version with key confirmation (KEAA), the Unified Model (UM) [1], the one-pass version (UM1) and the version with key confirmation (UMA), the Menezes-Qu-Vanstone (MQV) [18], the one-pass version (MQV1) and the version with key confirmation (MQVA), the Revised Nyberg-Rueppel protocol (RNR) [21], the one-pass Authenticated Key Agreement with key confirmation protocol (1P-AKACP) and the two-pass version (2P-AKACP) [19], the Chalkias-Hristou-Stephanides-Alexiadis protocol (CHHSA) [5] and the Horster-Michels-Petersen protocol (HMP) [12]. From the above protocols the Nyberg-Rueppel (but not the revised version) and the Horster-Michels-Petersen protocol supports message recovery.

We adopt the definitions, attributes and requirements for Authenticated Key Establishment from [4]. In Tables 1 and 2 we present a summary of the candidate protocols against these definitions and attributes.

3.3 The Protocol

As already pointed out, the session key can be renewed with one-pass authenticated key exchange protocol. For instance, when a node A (security-source)

Table 1. One-pass Protocol comparison

	KEA1	UM1	MQV1	RNR	1P-AKACP	CHHSA	HMP
Fundamental security goals							
Implicit key authentication	Y	Y	Y	Y	Y	Y	Y
Explicit key authentication	N	N	N	Y^I	N	N	N
Desirable security attributes							
Known-key security	N	N	N	N	N	N	N
Forward secrecy	N	N	N	N	N	N	N
Key-compromise impersonation	N[5]	N[5]	N[5]	-	N[7]	Y	-
Unknown key-share	N^+[5]	Y	N^+[5]	-	Y	Y	-
Desirable performance attributes							
Minimal number of passes	1	1	1	1	1	1	1

Y^I: Yes only to Initiator

N^+ : assurance is not provided unless modifications are made

Table 2. Multiple-pass Protocol comparison

	KEA	UM	MQV	2P-AKACP	KEAA	UMA	MQVA
Fundamental security goals							
Implicit key authentication	Y	Y	Y	Y	Y	Y	Y
Explicit key authentication	N	N	N	Y	Y	Y	Y
Desirable security attributes							
Known-key security	Y	Y	Y	Y	Y	Y	Y
Forward secrecy	N	Y	Y	Y	N	Y	Y
Key-compromise impersonation	Y	N	Y	Y	Y	N	Y
Unknown key-share	N[17]	Y	N	Y	Y	Y	N[16]
Desirable performance attributes							
Minimal number of passes	2	2	2	2	3	3	3

wants to send some data to node D (security-destination) with a new session key, k, the most efficient way to do it is to transmit the data and the new k simultaneously in the same message. More specifically, the main idea is to use an asymmetric authenticated encryption with message recovery technique to encrypt the protocol's parameters of the new k and with this session key to encrypt the data, provided that the offset of the parameters displayed in the transmitted message. The security-destination will be able to recover the new k and to decrypt the transmitted data with the recovered k.

We propose an adoption of the Horster-Michels-Petersen [12] protocol. We selected this protocol over its main competitor Nyberg-Rueppel because it has a lower communication cost. This is mainly due to the fact that HMP does not offer non-repudiation which is not a requirement in our scenario. Based on HMP protocol security-source A creates a compressed message m, computes the parameters c and s and sends (c, s, $\{\text{data}\}_k$, $timestamp$, $EIDsource$, $EIDdestination$) to the security-destination D. The new session key calculated as $k = h(m, timestamp, EIDsource, EIDdestination)$, where timestamp is a field of the primary bundle block (bundle header) and $EIDsource$ and

Table 3. AKE protocol

1.	**A:** $m \in Z_p$
	generates n $\in Z_p$ secretly and randomly
	computes $c = h(g_D^n)^{-1} m \bmod p$
	computes $c' = c \bmod q$
	computes $s = n - x_A c' \bmod p$
	$k = h(m, timestamp, EIDsource, EIDdestination)$
2. A $\rightarrow$ **D:**	(c, s, {data}$_k$, $timestamp$, $EIDsource$, $EIDdestination$)
3.	**D:** computes $c' = c \bmod q$
	recovers $m = h(g_B^s g_A^{c' x_B}) c \bmod p$
	$k = h(m, timestamp, EIDsource, EIDdestination)$

EIDdestination are fields of the bundle payload block. The aforementioned parameters c and s can be incorporated at the bundle payload filed among the encrypted data created with the new session key. We can also use the Bundle Extension Block (ESB) to keep information such as the offsets of parameters c and s. Node D will be able to distinguish c and s because of the offsets and to recover the message. Consequently D can calculate the k and decrypt the data. Assume that the security aware communicating parties have agreed on the public parameters g, Z_p in the standard Diffie Hellman fashion and q is a divisor of $p - 1$. Entities A and D have ephemeral keys x_A and x_D respectively which correspond to their public keys $g_A = g^{x_A}$ and $g_D = g^{x_D}$. Table 3 summarises the AKE protocol.

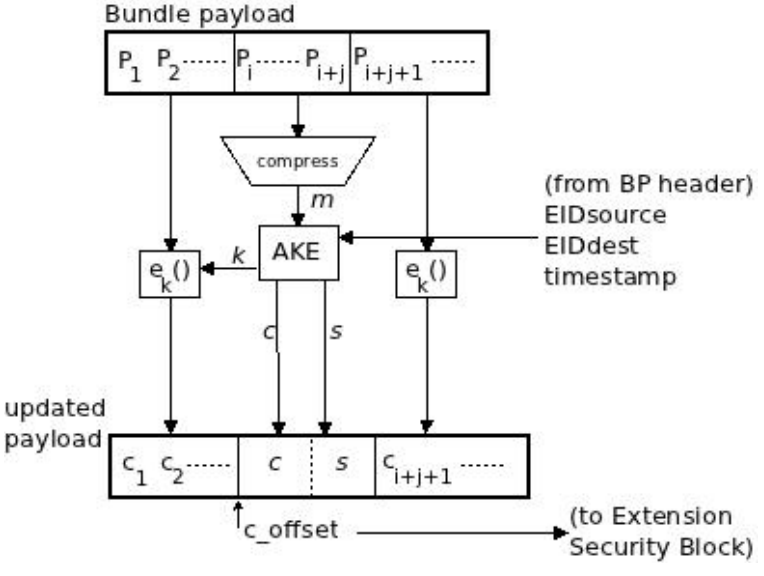

Fig. 2. AKE protocol within the bundle

The process for integrating the above protocol steps with the DTN architecture is presented in Fig. 2. Following the conventions shown in Fig. 1 earlier, assume that A (with public key g^A) needs to send data to D. Now since A knows that the data will need to be transferred to B who is untrusted in terms of confidentiality but, in DTN terms, will serve as the custodian, she would need to encrypt the data. In our example there are two alternatives:

1. A has exchanged public keys with the destination D, g^D.
2. A has only exchanged public keys with its immediate trusted neighbours in this case C, g^C.

From A's view the application of the security protocol and the resulting computational effort will be the same in both cases. The difference is that the protocol will be completed by a different party, D or C respectively. The Bundle Security Protocol (BSP) Specification has a data structure that allows seamless integration with either case. More specifically, the BSP contains the Abstract Security Block Structure (ASBS) where the security source and security destination endpoint identifiers are defined. In case (1) the security destination will contain the ID of D, whereas in case (2) the security destination will be refer to the ID of C. This distinction is crucial for two main reasons. First, the specification states that upon receiving a secure bundle, a security destination may need to take some actions. For example, if C is the security destination, but not the ultimate destination of the bundle, this may mean that C may need to decrypt the encrypted payload, re-encrypt it, or even disclose the session key to the destination. The precise action will depend on whether there are other untrusted nodes further down the transmission path, the capabilities of the final destination node or even if there are planned delays for forwarding the bundle. For example, a node in space may be aware that a window of opportunity for sending the bundle may be in say, after half a day, so it could perform decryptions while the data are under its custody. Alternatively, a node may prefer for similar reasons to expedite the transmission of the bundle, as it may know that not doing so may be a missed opportunity, asking for the next custodian to perform the encryption.

Second, the source or custodian of the bundle may not have had the opportunity to share long term keys with the destination, or in the case of PKIs, it may not have sufficient and timely access to the public keys. In a sense, a data source may delegate another trusted node to perform the encryption of the data. Therefore practical flexibility is vital in an environment with extremely large delays. An example activity diagram of the optimisation logic and encryption decision making is shown in Fig 3.

3.4 Evaluation

Although the HMP protocol has low communication overhead by design, in DTN space environments where bandwidth remains an issue, any savings on the bits transferred may have a significant impact on the overall communication quality. We have integrated the HMP protocol with the Bundle Protocol, but

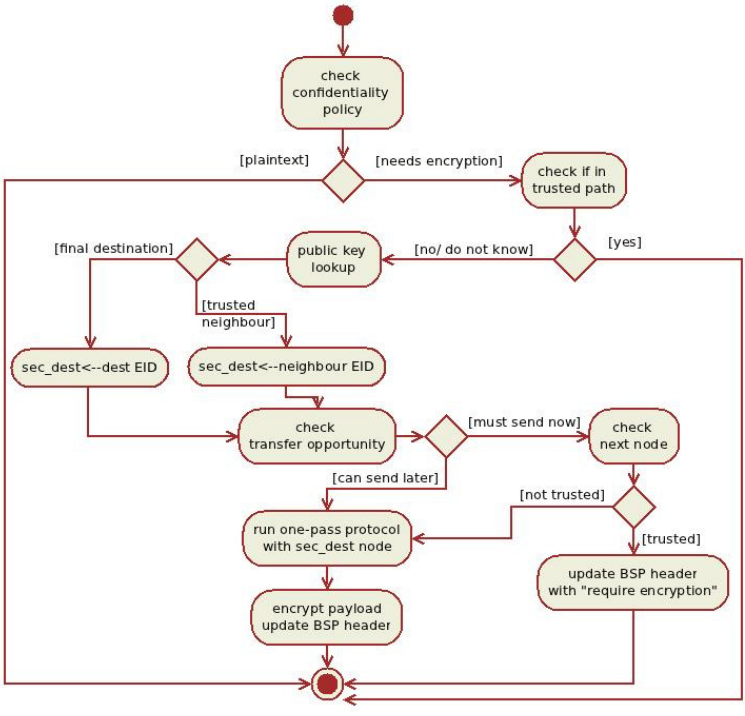

Fig. 3. Custodian's example encryption decision making activity diagram

this approach can be ported to a number of other published protocols. The design specification of the BP header as well as its extension blocks that use variable length attributes with self delimiting type of encoding, allows a variety of combination of protocols supporting a wide range of primitives. From a security perspective this is a very important feature as protocol updates in the DTN infrastructure will avoid security degradations. As such, our proposed scheme inherits the weaknesses of the underlying protocol.

The proposed approach includes the injection of the protocol messages in the payload and more specifically as part of the message. This is feasible for authenticated key exchange protocols with message recovery and the reason for doing so is purely for higher bandwidth utilization. As this message is also used for producing key material, the corresponding plaintext data need to be compressed to obtain high entropy and increase the corresponding effective key length. More precisely, the only inflation to the payload due to the cryptographic protocol is due to c. A side effect for this compression would be the lower communication costs, but this advantage can be easily lost if we introduce some further redundancy (say by means of a cryptographic checksum), according to the requirements of the specific, HMP protocol we have selected. It should be noted, however, that compression may also be a challenge for some nodes in deep space, as their hardware and energy resources may be limited. In this case having a

selection of different key exchange protocols available to allow application of different security policies, seems to be a necessary functional requirement.

4 Conclusion and Areas of Ongoing and Future Research

In this paper we have attempted to provide some directions and propose an approach for addressing the challenging problem of authenticated key exchange in space DTN environments. As the DTN is relatively new, the current state of the art is mainly limited to the "language" the security nodes should speak upon which the security services would be built. Limited work has been done in the area of key management and more specifically in key exchange.

We have demonstrated how to adopt a communication efficient authenticated key exchange protocol and make it suitable for a DTN environment. We have confirmed that the recently published Bundle Security Specification Protocol is appropriately designed to accommodate a plethora of key exchange protocols. We also realised that in an environment with relatively sparse resources the security decisions depend on the opportunities of the exploiting these resources and this needs to be reflected in the security policy. On this end, we proposed an encryption decision making workflow based on a popular communications scenario.

In terms of future research activities, the decision making policies need to be evaluated for correctness. This can be done by formal model checking methods, as these policies do not exhibit a large number of states and as such state space explosion will not be an issue.

Another area of ongoing research is the experimental integration of the proposed approach with an existing testbed in order to empirically evaluate this solution and explore other scenarios and protocols. We maintain a shared testbed with other research institutions and this activity is scheduled for the near future.

Acknowledgement. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013_FP7-SPACE-2010-1, SP1 Cooperation, Collaborative project) under grant agreement no. 263330 (project title: SPACE-DATA ROUTERS for Exploiting Space DATA). This paper reflects only the authors views and the Union is not liable for any use the may be made of the information contained therein.

References

1. Ankney, R., Johnson, D., Matyas, M.: The Unified Model, contribution to X9F1 2. ANSI X9.42, Agreement (1995)
2. Asokan, N., Kostiainen, K., Ginzboorg, P., Ott, J., Luo, C.: Towards securing disruption-tolerant networking, Technical Report NRC-TR-2007-007 (2007)
3. Bhutta, N., Ansa, G., Johnson, E., Ahmad, N., Alsiyabi, M., Cruickshank, H.: Security analysis for Delay/Disruption Tolerant satellite and sensor networks. In: International Workshop on Satellite and Space Communications (IWSSC), pp. 358–359 (2009)

4. Blake-Wilson, S., Menezes, A.: Authenticated Diffie-Hellman Key Agreement Protocols. In: Tavares, S., Meijer, H. (eds.) SAC 1998. LNCS, vol. 1556, pp. 339–361. Springer, Heidelberg (1999)
5. Chalkias, K., Halkidis, S.T., Hristu-Varsakelis, D., Stephanides, G., Alexiadis, A.: A Provably Secure One-Pass Two-Party Key Establishment Protocol. In: Pei, D., Yung, M., Lin, D., Wu, C. (eds.) Inscrypt 2007. LNCS, vol. 4990, pp. 108–122. Springer, Heidelberg (2008)
6. Chalkias, K., Baldimtsi, F., Hristu-Varsakelis, D., Stephanides, G.: Two Types of Key-Compromise Impersonation Attacks against One-Pass Key Establishment Protocols. In: E-Business and Telecommunication Networks (book chapter). Springer (2008)
7. Chalkias, K., Baldimtsi, F., Hristu-Barsakelis, D., Halkidis, S.T., Stephanides, G.: Attacks on the AKACP Protocol. IACR Cryptology Eprint Archive (2010)
8. Elkamchouchi, H., Eldefrawy, M.: A New Approach for Key Controlled Agreement. In: 24th National Radio Science Conference, NRSC 2007, pp. 1–7. Ain Shams University, Egypt (2007)
9. Elkamchouchi, H., Eldefrawy, M.: An Efficient and Confirmed Protocol for Authentication Key Agreement. In: 25th National Radio Science Conference, NRSC 2008, pp. 1–8. Tanta University, Egypt (2008)
10. Farrell, S.: DTN Key Management Requirements, work in progress as an internet-draft (2007), `http://tools.ietf.org/html/draft-farrell-dtnrg-km-00`
11. Farrell, A., Symington, S.F., Weiss, H., Lovell, P.: Delay-Tolerant Networking Security Overview, internet-draft (2009), `http://tools.ietf.org/html/draft-irtf-dtnrg-sec-overview-06`
12. Horster, P., Michels, M., Petersen, H.: Authenticated encryption schemes with low communication costs. IEEE Electronics Letters 30(15), 1212–1213 (1994)
13. Internationl standard: Information technology - Security techniques - Key management - Part3: Mechanisms using asymmetric techniques. 2 edn. (2008)
14. Jia, Z., Lin, X., Tan, S.-H., Li, L., Yang, Y.: Public key distribution scheme for delay tolerant networks on two-channel cryptography. Journal of Network and Computer Applications (2011)
15. Kate, A., Zaverucha, G., Hengartner, U.: Anonymity and Security in Delay Tolerant Networks. In: 3rd International Conference on Security and Privacy in Communications Networks and the Workshops, Secure Communication, pp. 504–513 (2007)
16. Krawczyk, H.: HMQV: A High-Performance Secure Diffie-Hellman Protocol. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 546–566. Springer, Heidelberg (2005)
17. Lauter, K., Mityagin, A.: Security Analysis of KEA Authenticated Key Exchange Protocol. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 378–394. Springer, Heidelberg (2006)
18. Law, L., Menezes, A., Qu, M., Solinas, J., Vanstone, S.: An efficient protocol for authenticated key agreement. Technical report CORR 98-05, University of Waterloo (1998)
19. Mohammad, Z., Chen, Y.-C., Hsu, C.-L., Lo, C.-C.: Cryptanalysis and Enhancement of Two-pass Authenticated Key Agreement with Key Confirmation Protocols. IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India) 27(3), 252–265 (2010)
20. National Security Agency: SKIPJACK and KEA algorithm speci cation, Version 2.0 (1998)

21. Nyberg, K.: On one-pass authenticated key establishment schemes. In: Workshop on Selected Areas in Cryptography (SAC 1995), pp. 2–8 (1995)
22. Pour, A.N.: Number Theory and Related Algorithms in Cryptography, Master's thesis, Japan Advanced Institute of Science and Technology, pp. 37–43 (2002)
23. Song, B., Kim, K.: Comparison of Existing Key Establishment Protocols. In: Information Security and Cryptography, pp. 1–13 (2000)
24. Symington, S., Farrell, S., Weiss, H., Lovell, P.: Bundle Security Protocol Specification. Request for Comments, RFC 6257, http://datatracker.ietf.org/doc/rfc6257
25. Van Besien, W.: Dynamic, Non-Interactive Key Management for Bundle Protocol. In: 5th ACM Workshop on Challenged Networks (CHANTS 2010), Illinois (2010)
26. Wood, L., Eddy, W.M., Holiday, P.: A bundle of problems. In: Aerospace Conference, pp. 1–14 (2009)