Trust-Aware Security for Disruption-Tolerant Networks

Vladimir Oleshchuk

Trust-Aware Security for Disruption-Tolerant Networks

Vladimir Oleshchuk

University of Agder, Department of ICT
Postboks 509, N-4898 Grimstad, Norway
vladimir.oleshchuk@uia.no

Abstract. The paper proposes an approach to security enforcement in disruption- and delay-tolerant networks (DTNs) suitable for emergency and crisis setting. Comparing with traditional networks, DTNs have many unconventional constraints such as long delays, high packet drop rates, unavailability of central trusted entity etc. Under such constraints existing security protocols do not work or not feasible. We propose an approach suitable for combining identity and attribute based encryptions (IBE and ABE) with subjective logic based trust model to provide adaptable trust-aware security solutions for wireless DTNs.

1 Introduction

We consider setting where traditional infrastructure-based wireless networks [14] are not available but mobile devices with wireless connectivity are widely distributed among population. Since fixed network infrastructure is not available, the connectivity between such Wi-Fi enabled devices will be disrupted. This is a typical setting for various disaster areas.

However, the devices may still be able to communicate on a peer-to-peer basis, form ad hoc P2P networks and convey messages between network participants. In this case, network nodes are responsible for supporting traditional network functionality such as message forwarding, topology maintenance, etc. However, such networks are formed by many unreliable, semi-trusted and untrusted nodes, which results in unreliable and insecure communication. As a consequence, transmitted messages may be illegitimately duplicated, modified, delayed, deleted etc. To be useful as tool for information gathering and sharing such networks must provide some level of reliability, security and possibly privacy protection to their users. High mobility, low device capacities make the maintenance of network functionality even more challenging. As result, many traditional network solutions are not feasible and new more suitable emerging network solutions that do not entirely rely on any fixed or wired infrastructure were proposed.

One of the most promising approaches proposed recently is disruption and delay-tolerant networks (DTNs) [4,5]. In disaster context, DTNs may provide low cost reliable connectivity and are suitable for rapid deployment to provide

first-responder and victim population with communication infrastructure [16]. However, the constraints of disaster settings make traditional security solutions often infeasible and even impossible. The main motivation and focus of this work is to propose a security enforcement approach to provide secure solutions suitable for DTNs networks in disaster context.

2 Security and privacy challenges

One of the distinguishing features of disaster setting is an existence of many untrusted and semi-trusted nodes and unavailability of central trusted authorities (TAs). It makes security and privacy enforcement challenging since it requires cooperation of nodes to secure essential network functionality. Providing security functionality such as secure routing, message confidentiality, integrity and authenticity, malicious node identification and isolation etc. will require establishment of trust associations, providing secure storage and key management. For example, one implication of long delays and high probability packet loss is that session key negotiation in SSL/TLS style is impractical and sometimes impossible. It also illustrate why we need new approaches to security (and privacy) of DTNs in disaster context [16]. Since we have to provide solutions based on cooperation of mobile (un)trusted and semi-trusted nodes without centralised TAs, we cannot expect to provide both perfect and usable security. Under such constraints, we will focus on how to provide context dependent adaptable security with mechanisms for their trustworthiness assessment seen as a measure of provided level of security. For example, security provided by a cryptographic solution (assuming it is not broken) depends on trustworthiness of identities and keys involved.

3 Security and trustworthiness

The de-centralised nature of DTNs may potentially provide more robust and resilient solutions comparing with centralised architecture where a centralised trusted authority can be a single point of failure. Traditional public-key infrastructure (PKI) is considered to be not well-suitable for DTNs, partly due to difficulties to access online servers and therefore inability to provide support for certificate revocation [20]. Therefore, the use of identity-based cryptography (IBC) has been proposed to provide security in DTNs [20]. However, analysis presented in [1], leads to conclusion that IBC has no significant advantages over traditional cryptographic approaches with respect to integrity and authenticity but it can provide better confidentiality protection. One of the weak points of using IBC with DTNs is verification by trusted third party called PKG (private key generator) of a new entity's right to an identifier that will be used as a public key in the subsequent communication in DTN.

In our approach, we propose to combine collaborative efforts several parties (some of them may have PKG functionality) to conform that a new entity does have right to claimed identity that will be later used as a public key. These

parties can jointly either conform that the entity do have right to an identifier while only one PKG is used as a public-key generator or several PKGs jointly generate the secret key) (by using, for example, a hierarchical IBC (HIBC)). The trustworthiness of this new identity will depend on trustworthiness of PKGs that have verified the identity of this new entity and have generated a secret key for it.

To work properly, such schemes need to maintain knowledge about trustworthiness of nodes and their public keys. As it was pointed out in [7,17], establishing an initial trust between nodes in the deployment phase is still an open problem.

However, in some scenarios (for example, in disaster management), it is reasonable to assume that deployment will involve human participants and some of these participants may already have credentials/certificates issued prior disaster. Typical examples of such participants could be police officers, medical doctors and nurses, firemen, local administration officials, school teachers, etc. such credentials may be used for initial trust establishment between nodes (participants).

Generally, in DTNs deployed in disaster areas we assume existence of three categories of nodes: nodes with security credentials issued trusted PKGs prior disaster (possibly currently unreachable), nodes without such credentials but with capabilities to act temporally as local PKGs for themselves and other nodes, and nodes without such capabilities. Nodes with credentials assigned by trusted PKGs form a subset of nodes with initially assigned level of trustworthiness. Trustworthiness of a participant without such credentials is initially unknown. However, trustworthy nodes can combine their efforts and generate locally (on site) credentials for those participants that do not have such capabilities. They can, in addition, base their decisions on social information assuming that socially-related people are collocated and often share the same security context [2,3].

4 Credential trustworthiness in emergency setting

We consider a set S of entities (nodes) where $S = \{s_1, s_2, ...\}$. Some members of S can function as temporal TAs, some have credentials issued by TAs, and some be without any credentials that are certified/issued by TAs. We assume that elements of S will be involved in activities requiring various degree of security enforcement such as message sending, accessing databases, etc. Members of S can be seen as entities (nodes) of DTN that are mobile and with varying levels of trustworthiness. Members of S in most cases can be seen as mobile devices accompanying human beings. They often have a social context which may help to infer trust associations between members, when, for example, they know each other or have professional or personal relations such as co-workers, family members, etc.

We write $[s_1 \rightarrow c]s_0$ to denote that credential c is bound to s_1 by s_0. It can be, for example, a digital certificate issued by s_0 to s_1. The notation is inspired by [6]. We assume that a trust association is already established between s_0 and s_1 either from social context or by other formal means like revealing verifiable credentials to each other for authentication (such as digital or physical passports,

driving license, ID cards, etc.). Then, trustworthiness of c when used by s_1 will depend on trustworthiness of s_0.

In the remaining part of this section we consider several cases to illustrate handling of different types of c such that identities, attributes, roles, etc.

Consider the case when c is an identity. Assume that c is an identity. Then, $[s_1 \rightarrow c]s_0$ states that s_0 conforms that c is an identity of s_1 by, for example, issuing corresponding digital credential (certificate). The trustworthiness of such binding is directly determined by trustworthiness of s_0. As it was already mentioned, trustworthiness that entities have rights to their identifiers is essential for successful use of IBC in DTNs since these identities serve as identities' public keys. Therefore, realistic trustworthiness estimation of such bindings is crucial when security is based on IBC.

Trustworthiness of $[s_1 \rightarrow c]s_0$ will influence trustworthiness of all subsequent credentials s_1 will issue (signed by s_1). To increase trustworthiness of such binding we can seek its endorsement by several entities. For example, if both s_0 and s_1 confirm binding c and s_2 by issuing credentials $[s_2 \rightarrow c]s_0$ and $[s_2 \rightarrow c]s_1$, then the trustworthiness of binding c and s_2 is defined by a combined trustworthiness of s_0 and s_1. Such credential will be denoted as $[s_2 \rightarrow c]s_0, s_1$.

Finally, any credential c owned by an entity can be either directly issued by another entity or delegated. In the first case issuing entity is assumed to have acceptable level of trustworthiness to be able issue trustworthy credentials (for example, be a security administrator for specific service). In the second case, an entity the delegated credential is supposed to be issued with permission for further delegation.

5 Subjective logic based trust management

In this section we describe how to apply subjective logic based trust model for trustworthiness estimation and management of credentials in DTNs used in settings discussed above.

Subjective logic is a type of probabilistic logic that explicitly takes uncertainties and believes into account [8]. It is suitable for modelling and analysing situations which involve uncertainty and incomplete knowledge. Subjective logic can be seen as an alternative to Dempster-Shafer theory, with main difference from the former that subjective logic defines belief mass as a function of not only belief and uncertainty, but also of an a priori probability in the absence of any evidence. It is also argued [12] that subjective logic is suitable to formulate more expressive beliefs than Dempster-Shafer theory. For example, the consensus operator provided by subjective logic can be applied to combine trustworthiness of PKGs that are involved in corresponding key generation.

The level of trustworthiness in subjective logic is represented as an opinion. An opinion is defined as a tuple $\omega = \{t, d, u, a\}$, where components t, d, u and a, represent levels of trust, distrust, uncertainty and base rate respectively, where $t, d, u, a \in [0, 1]$, $t+d+u = 1$ and a denotes the a priori probability in the absence

of evidence. Trustworthiness expressed by opinions provides more adequate trust model of real world since it includes uncertainties as a member of opinion tuple.

Subjective logic defines several operators for combining opinions. Some of them, relevant for our approach, will be explained in the following subsection. More details, related to subjective logic can be found in [8,12,11,13].

5.1 Conjunction of opinions

Let s_0 and s_1 be to entities (nodes) of a DTN. Assume that ω_0 denotes an opinion about trustworthiness of s_0 and trustworthiness of s_1 is unknown. Assume that $[s_1 \to c]s_0$ denoting that s_0 issues credential c to s_1. We assume that trustworthiness of c issued by s_0 will totally depend on trustworthiness of s_0 and therefore in our is estimated to be equal to ω_0. We also assume that trustworthiness of any entity may be estimated as a combined trustworthiness of its credentials. When several credentials are issued to an entity, its trustworthiness will be estimated by combining opinions expressing trustworthiness of all its credentials (more specifically, as a conjunction of these opinions).

Formally, let us consider two entities s_1 and s_2 with trustworthiness given by ω_1 and ω_2, respectively. Assume that s_1 issues credential c_1 to s and s_2 issues credential c_2 to s, that is, $[s \to c_1]s_1$ and $[s \to c_2]s_2$. Issuing credentials from different subjects is a conjunction of two propositions from two distinct of judgements and the opinion about trustworthiness of s is a new opinion reflecting the truth of both judgments simultaneously. Then trustworthiness of s will be expressed by opinion $\omega = \omega_1 \wedge \omega_2$ defined as in [12]:

$$\omega = \omega_1 \wedge \omega_2 = \{t, d, u, a\}$$

where

$$t = (t_1 t_2 + (1 - a_1)a_2 t_1 u_2 + a_1(1 - a_2)u_1 t_2)/(1 - a_1 a_2)$$
$$d = d_1 + d_2 - d_1 d_2$$
$$u = u_1 u_2 + ((1 - a_2)t_1 u_2 + (1 - a1)u_1 t_2)/(1 - a_1 a_2)$$
$$a = a_1 a_2$$

For example, if $\omega_1 = \{0.8, 0.1, 0.1, 0.5\}$ and $\omega_2 = \{0.7, 0.1, 0.2, 0.5\}$ (both express high levels of trustworthiness with low uncertainty), then $\omega = \omega_1 \wedge \omega_2 = \{0.64, 0.19, 0.18, 0.25\}$.

If the first entity has high level of trust with low uncertainty, for example, $\omega_1 = \{0.8, 0.1, 0.1, 0.5\}$, but the second entity has low trust level with high uncertainty, for example, $\omega_2 = \{0.2, 0.1, 0.7, 0.5\}$, the trustworthiness of s is estimated as $\omega = \omega_1 \wedge \omega_2 = \{0.35, 0.19, 0.46, 0.25\}$. We can see that resulting opinion expressing trustworthiness s combines trust with respect to uncertainty levels.

In the case when the first entity has high level of trust with high uncertainty, for example, $\omega_1 = \{0.5, 0.0, 0.5, 0.5\}$ but the second entity has low trust level with low uncertainty, for example, $\omega_2 = \{0.2, 0.74, 0.06, 0.5\}$. Then trustworthiness of s will be estimated as $\omega = \omega_1 \wedge \omega_2 = \{0.14, 074, 0.12, 0.25\}$ where high trust with high uncertainty does not increase resulting combined trust level.

5.2 Consensus of opinions

Let us consider two entities s_1 and s_2 that have two (possibly different) opinions ω_1 and ω_2 about trustworthiness of the same credential c. The consensus opinion of two possibly conflicting opinions is an opinion that reflects opinions of both entities in a fair and equal way. The consensus operator, denoted as $\oplus$, produces a consensus belief that combines the two separate beliefs into one $\omega = \omega_1 \oplus \omega_2$ as it is defined in [11]. In context of DTNs, assume that both s_1 and $s_2$conform binding of identity c to s, that is, issuing $[s \to c]s_1$ and $[s \to c]s_2$. Then, trustworthiness of binding identity c to subject s can be estimated as a new opinion $\omega = \omega_1 \oplus \omega_2$ by applying consensus operator.

Formally, assuming that $\omega_i = \{t_i, d_i, u_i, a_i\}$, $i = 1, 2$, the consensus opinion ω is calculated as following [11]:

$$\omega = \omega_1 \oplus \omega_2 = \{t, d, u, a\}$$

where

$$t = \begin{cases} (t_1 u_2 + t_2 u_1)/k, & k \neq 0 \\ (u_2 t_1/u_1 + t_2)/(u_2/u_1 + 1), & k = 0 \end{cases}$$

$$d = \begin{cases} (d_1 u_2 + d_2 u_1)/k, & k \neq 0 \\ (u_2 d_1/u_1 + d_2)/(u_2/u_1 + 1), & k = 0 \end{cases}$$

$$u = \begin{cases} u_1 u_2/k, & k \neq 0 \\ 0, & k = 0 \end{cases}$$

$$a = \begin{cases} \frac{a_1 u_2 + a_2 u_1 - (a_1 + a_2) u_1 u_2}{u_1 + u_2 - 2 u_1 u_2}, & k \neq 0 \\ ((u_2 a_1)/u_1 + a_2)/(u_2/u_1 + 1), & k = 0 \end{cases}$$

and

$$k = u_1 + u_2 - u_1 u_2$$

Consider the case when both opinions $\omega_i = \{t_i, d_i, u_i, a_i\}$, $i = 1, 2$ are highly trustful with low uncertainty, for example, $\omega_1 = \{0.7, 0.17, 0.13, 0.5\}$ and $\omega_2 = \{0.63, 0.23, 0.14, 0.5\}$ (when both s_1 and s_2 know well identity of s). The consensus opinion expressing trustworthiness binding identity c to s is estimated as $\omega = \omega_1 \oplus \omega_2 = \{0.71, 0.21, 0.07, 0.5\}$ shows that by using two reliable identifiers reduce uncertainty and increase trust.

However, it is more challenging to find consensus when opinions are contradicting. Assume that ω_1 expresses high trust with low uncertainty,
$\omega_1 = \{0.7, 0.17, 0.13, 0.5\}$, while ω_2 expresses low trust, that is high distrust, with low uncertainty, $\omega_2 = \{0.12, 0.7, 0.18, 0.5\}$. The consensus opinion expressing trustworthiness of binding identity c to s is estimated as $\omega = \omega_1 \oplus \omega_2 = \{0.5, 0.42, 0.08, 0.5\}$ shows decreasing (w.r.t. highest trust) of both uncertainty and trust.

Consider the case when ω_1 expresses high trust with low uncertainty and ω_2 expresses low trust with high uncertainty: $\omega_1 = \{0.7, 0.17, 0.13, 0.5\}$ and

$\omega_2 = \{0.08, 0.48, 0.44, 0.5\}$. The consensus opinion expressing trustworthiness of binding identity c to s is estimated as $\omega = \omega_1 \oplus \omega_2 = \{0.62, 0.27, 0.11, 0.5\}$ showing that highly uncertain distrustful opinion influence trust level of consensus only slightly.

In case when ω_1 expresses high trust with high uncertainty and ω_2 expresses low trust with low uncertainty: $\omega_1 = \{0.51, 0.07, 0.42, 0.5\}$ and $\omega_2 = \{0.22, 0.68, 0.1, 0.5\}$ the censuses opinion about trustworthiness of binding identity c to s is $\omega = \omega_1 \oplus \omega_2 = \{0.3, 0.61, 0.09, 0.5\}$ will low trust with low uncertainty.

5.3 Transitive opinions

Assume that s_0 has issued a credential c to s_1, that is, it has issued a certificate $[s_1 \to c]s_0$. To support flexibility and usability, s_0 (which may be not available in crisis situation), may grant s_1 a permission to delegate c further to other subjects on its own discretion. Formally, it is indicated in the issued certificate: $[s_1 \to c']s_0$.

Assume that ω_0 and ω_1 are opinions about trustworthiness of s_0 and s_1, respectively where $\omega_i = \{t^i, d^i, u^i, a^i\}, i = 0, 1$. The delegation permission can be interpreted that s_1 recommends s_2 as an entity trusted for using (when delegated) credential c. Trustworthiness of c (when used by s_2) will depend on trustworthiness of s_0 and trustworthiness of recommendations of s_1.

In subjective logic notation, $\omega_1^0 = \{t_1^0, d_1^0, u_1^0, a_1^0\}$ denotes an opinion of s_0 about trustworthiness of delegations (recommendations) of s_1. In context of DTNs we may assume that $\omega_1^0 = \omega_0$. Now, assume that s_1 delegate c to s_2, that is, for example by issuing a certificate $[s_2 \to c]s_1$. The opinion about trustworthiness of c when used by s_2 is denoted as ω_2. The opinion ω_2 can be found as combination of ω_1 with ω_1^0 . For estimation of indirect opinion ω_2, the recommendation operator $\otimes$ proposed to used (as defined in [13]): $\omega_2 = \omega_1^0 \otimes \omega_1$.

More specifically, according to [8,13], indirect opinion ω_2 can be calculated as following:

$$\omega_2 = \omega^{0,1} = \omega_1^0 \otimes \omega_1 = \{t^2, d^2, u^2, a^2\}$$

where

$$t^2 = t_1^0 t^1$$
$$d^2 = t_1^0 d^1$$
$$u^2 = d_1^0 + u_1^0 + t_1^0 u^1$$
$$a^2 = a^1$$

Consider the case when both opinions $\omega_i = \{t_i, d_i, u_i, a_i\}$, $i = 0, 1$ are both highly trustful with low uncertainty with, for example, $\omega_0 = \{0.79, 0.11, 0.1, 0.5\}$ and $\omega_1 = \{0.75, 0.14, 0.12, 0.5\}$. Then, trustworthiness of delegated credential c originally issued by s_0 to s_1 is expressed by opinion $\omega_2 = \{0.63, 0.12, 0.25, 0.5\}$ showing that trustworthiness of c when used by s_2 will be slightly discounted with respect of trustworthinesses of both s_0 and s_1.

Assume that $omega_0$ is highly trustful (high trust and low uncertainty, for example, a TA) and ω_1 is trustful but with high uncertainty, that is, $\omega_0 = \{0.84, 0.11, 0.05, 0.5\}$ and $\omega_1 = \{0.5, 0.2, 0.3, 0.5\}$. Then, trustworthiness of delegated credential c originally issued by s_0 to s_1 is expressed by opinion $\omega_2 = \{0.43, 0.17, 0.4, 0.5\}$ with lower trust and higher uncertainty than both s_0 and s_1.

Conclusion and future work

In this paper, we propose an new approach to enforce security in disruption-tolerant networks when they are used in disaster setting. Such networks are known to be particular difficult to provide security. Our framework is designed to be used in settings where centralised trusted authorities are not easily accessible and therefore many existing traditional solutions will not work. The framework applies a trust model based on subjective logic to dynamic trust assessment of security credentials in DTNs. The presented examples illustrate how to use subjective logic based trustworthiness to keep track on trustworthiness of credentials in dynamic ad hoc environments to provide usable adaptive trust-aware approach to security.

The future work is to elaborate use of subjective logic by selecting (or even propose new) operators that reflect the nature of trust in DTNs in the most appropriate way. For example, since several trust discounting operators for subjective logic are described in the literature [9,10] the study of which of them would be the most suitable for dealing with trust in DTNs is needed. Another important issue is to develop suitable identity and attribute-based schemes that can be used in DTNs to cryptographically enforce subjective logic trust, issuing, generation, delegation of credentials and their trust estimation [18,19].

References

1. Asokan, N., Kostiainen, K., Ginzboorg, P., Ott, J. and Luo, C. Applicability of identity-based cryptography for disruption-tolerant networking. In: MobiOpp 07, ACM, 2007, pp. 52-56.
2. Costa, P., Mascolo, C., Musolesi, M. and Picco, G. Socially-ware routing for publish-subscribe in delay-tolerant mobile ad-hoc networks. IEEE Journal on Selected Areas in Communications, 2008, 26, 5, pp. 748-760.
3. Defrawy, K.E., Solis, J. and Tsudik, G. Leveraging social contracts for message confidentiality in delay tolerant networks. In Proceedings of 33rd IEEE International Computer Software and Applications Conference, 2009, pp. 271-279.
4. Fall, K. A delay-tolerant networks architecture for challenged internets. SIGCOMM03, 2003, 27-33.
5. Fall, K. and Farrell, S. (2008) DTN: an architectural retrospective. IEEE Journal on Selected areas in communications, 2008, 26, 5, pp. 828-836.
6. Freudenthal, E., Pesin, T., Port, L., Keenan, E. and Karamcheti, V. dRBAC: distributed role-based access control for dynamic coalition environments, In: Proceedings 22nd International Conference on Distributed Computing Systems, 2002, pp. 411-420.

7. Jia, Z., Lin, X., Tan, S.H., Li, L. and Yang Y. Public-key distribution scheme for delay-tolerant networks based on two-channel cryptography. J. of Networks and Computer Applications, 2012, 35, 3, pp. 905-913.
8. Jøsang, A. Subjective Logic: A Formalism for Reasoning Under Uncertainty. Springer, 2016.
9. Jsang, A., Azderska, T. and Marsh, S. Trust transitivity and conditional belief reasoning. In T. Dimitrakos, R. Moona, D. Patel, and D.H. McKnight, editors, Proceedings of the 6th IFIP International Conference on Trust Management (IFIPTM 2012), volume 374 of IFIP Advances in Information and Communication Technology, pp. 6883. Springer, Berlin, 2012.
10. Jøsang, A., Pope, S. and Marsh, S. Exploring different types of trust propagation. In K. Stølen, W.H. Winsborough, F. Martinelli, and F. Massacci, editors, Proceedings of the 4th International Conference on Trust Management (iTrust), LNCS 3986, pp. 179192. Springer, Berlin, 2006.
11. Jøsang, A. The Consensus Operator for Combining Beliefs. Artificial Intelligence Journal, 2002, 142, 1-2, pp. 157-170.
12. Jøsang, A. A Logic of Uncertain Probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9, 3, pp. 279-311.
13. Jøsang A. An Algebra for Assessing Trust in Certification Chains. In Proceedings of the Networks and Distributed Systems Security (NDSS99), 1999.
14. Ma, D. and Tsudik, G. Security and Privacy in Emerging wireless networks. IEEE Wireless Communications, 2010, 12-21.
15. Manoj, B. S. and Hubenko Baker, A. Communication challenges in emergency response. Comm. of ACM, 50, 2007, 3, pp. 51-53.
16. Oleshchuk, V. A Novel Framework for Security Enforcement in Networks for Disaster and Crisis Management. In: Proceedings of the International Conference on Information Systems for Crisis Response and Management, 2016, 1-6, ISCRAM.
17. Omar, M., Challa, Y. and Bonabdallah A. Reliable and fully distributed trust model for mobile ad hoc networks. Computer &Security, 2009, 29, 3-4, pp. 199-214.
18. Pussewalage, H. S. G. and Oleshchuk, V. A. A Distributed Multi-Authority Attribute Based Encryption Scheme for Secure Sharing of Personal Health Records. In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies. ACM, New York, NY, USA, pp. 255-262, 2017.
19. Pussewalage, H. S. G. and Oleshchuk V.A. A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using Cloud Computing, 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), Pittsburgh, PA, 2016, pp. 46-53.
20. Seth, A. and Keshav, S. Practical security for disconnected nodes. In: First Workshop on Secure Network Protocols (NPSec), 2005.