Shodhshauryam, International Scientific Refereed Research Journal
© 2019 SHISRRJ | Volume 2 | Issue 2 | ISSN : 2581- 6306

Secure Data retrieval based on DTN

K. Malarvizhi
PG Scholar, Akshaya College of Engineering and Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Keywords : Disruption-tolerant network , CP-ABE, decentralized

I. INTRODUCTION

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network. Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors is blocked from carrying out exploits and threats.

Two types of network includes wired and wireless network. The common vulnerability that exists in both wired and wireless networks is an "unauthorized access" to a network. An attacker can connect his device to a network though unsecure hub/switch port. In this regard, wireless network are considered less secure than wired network, because wireless network can be easily accessed without any physical connection.

Network security is a big topic and is growing into a high profile Information Technology (IT) specialty area. Security-related websites are tremendously popular with savvy Internet users. The popularity of security-related certifications has expanded. Esoteric security measures like biometric identification and authentication have become commonplace in corporate America. Many organizations still implement security measures in an almost haphazard way, with no well-thought out plan for making all the parts fit together. Computer security involves

many aspects, from protection of the physical equipment to protection of electronic bits and bytes that make up the information that resides on the network.

1.2 DISRUPTION TOLERANT NETWORK:

A disruption-tolerant network (DTN) is a network designed so that temporary or intermittent communications problems, limitations and anomalies have the least possible adverse impact. There are several aspects to the effective design of a DTN, including:

- The use of fault-tolerant methods and technologies.
- The quality of graceful degradation under adverse conditions or extreme traffic loads.
- The ability to prevent or quickly recover from electronic attacks.
- Ability to function with minimal latency even when routes are ill-defined or unreliable.

Fault-tolerant systems are designed so that if a component fails or a network route becomes unusable, a backup component, procedure or route can immediately take its place without loss of service. At the software level, an interface allows the administrator to continuously monitor network traffic at multiple points and locate problems immediately. In hardware, fault tolerance is achieved by component and subsystem redundancy.

Graceful degradation has always been important in large networks. One of the original motivations for the development of the Internet by the Advanced Research Projects Agency of the U.S. government was the desire for a large-scale communications network that could resist massive physical as well as electronic attacks including global nuclear war. In graceful degradation, a network or system continues working to some extent even when a large portion of it has been destroyed or rendered inoperative.

Electronic attacks on networks can take the form of viruses, worms, Trojans, spyware and other destructive programs or code. Other common schemes include denial of service attacks and malicious transmission of bulk email or spam with the intent of overwhelming network servers. In some instances, malicious hackers commit acts of identify theft against individual subscribers or groups of subscribers in an attempt to discourage network use. In a DTN, such attacks may not be entirely preventable but their effects are minimized and problems are quickly resolved when they occur. Servers can be provided with antivirus software and individual computers in the system can be protected by programs that detect and remove spyware.

As networks evolve and their usage levels vary, routes can change, sometimes within seconds. This can cause temporary propagation delays and unacceptable latency. In some cases, data transmission is blocked altogether. Internet users may notice this as periods during which some web sites take a long time to download or do not appear at all. In a DTN, the frequency of events of this sort is kept to a minimum.

II. LITERATURE SURVEY

1. Node Density-Based Adaptive Routing Scheme for Disruption Tolerant Networks

Traditional ad hoc routing protocols do not work in intermittently connected networks since end-to-end paths may not exist in such networks. Hence, routing mechanisms that can withstand disruptions need to be designed. A store-and-forward approach has been proposed for disruption tolerant networks. Recently, several approaches have been proposed for unicast routing in disruption-prone networks e.g. the 2-hop relay approach, delivery probability based routing, and message ferrying. In our earlier paper, we have evaluated a combined multihop and message ferrying approach in disruption tolerant networks. In that paper, we assume that a special node is designated to be a message ferry. A more flexible approach is to let

regular nodes volunteer to be message ferries when network dynamics mandate the presence of such ferries to ensure communications. Thus, in this paper, we design a node-density based adaptive routing (NDBAR) scheme that allows regular nodes to volunteer to be message ferries when there are very few nodes around them to ensure the feasibility of continued communications. Our simulation results indicate that our NDBAR scheme can achieve the highest delivery ratio in very sparse networks that are prone to frequent disruptions

Packet-switched network communication has been studied for decades. Important progress has been made in robustness and scalability in the TCP/IP protocol suite based primarily on principles of end-to-end protocols and services [9]. However, there are many scenarios in which an end-to-end connection is not guaranteed or even possible, and so an intermediary is needed, perhaps to translate between protocols or to provide temporary storage (e.g., in mail servers).

In these cases, without such intermediaries, communication would fail. In other cases, communication may fail not because of a lack of instantaneous connection, but because the connection properties fall beyond the expected bounds (excessive round-trip-time or high packet loss probability). Solutions have been proposed to deal with some specific situations, e.g., using link layer retransmissions to deal with high packet loss probability in wireless environments [4]. However, these solutions still do not work in situations where there are no end-to-end paths. DakNet [3] deploys physical transport devices, e.g., buses and motorcycles, to carry mobile access points between village kiosks and hubs with Internet connectivity so that the data carried by the physical transport devices can be automatically uploaded and/or downloaded when the physical transport devices are in the wireless communication range of a kiosk or a hub.

Similar techniques are proposed in [1],[2]. In the past year, considerable amount of research focusing on delay/disruption-tolerant networking and communications has been published (e.g.[5],[6], [13],[15]). DieselNet [14] is a vehicular-based disruption tolerant network where connections between nodes are short-lived and occasional. A common approach used to address delays and disruptions is via the use of a store-and-forward mechanism similar to electronic mail [10]. This makes communication possible, even when an instantaneous end-to-end path does not exist. Several routing schemes have been proposed for DTNs.

They can be categorized into three categories: (i) using message ferries or data mules to connect partitioned nodes [15],[20], (ii) using history-based information to estimate delivery probability of peers and pass the message to the peer that can best deliver the message [22], [26], and (iii) using 2-hop relay forwarding schemes where a source can send multiple copies to different relay nodes and have the relay nodes deliver to the destination when they encounter the destination [19],[21]. In our earlier work [25], we have evaluated the performance of a multihop routing scheme with custody transfer feature in a single domain DTN.

We also have explored using message ferrying and high-power backhaul links for interdomain message delivery. Our work revealed that in a single domain environment, even with the custody transfer feature, the delivery ratio drops when the nodes are sparsely connected. So, in this paper, we propose a node-density based adaptive routing (NDBAR) scheme that provides better performance than previous approaches.

2. Performance Evaluation of Content-Based Information Retrieval Schemes for DTNs

Content based information dissemination There are three main components in our content-based information retrieval system, namely (a) data caching, (b) query dissemination, and (c) message routing e.g.

routing query responses. Our system supports both push and pull mechanisms that work in disruption tolerant network environment. Thus, contents can be searched and retrieved in our system even when connectivity is disrupted. Using the late-binding [2], and content-based routing features in our system, queries can be issued without prior knowledge of where the content lies.

A.Data Caching Schemes For the push mechanism, we investigate two data caching schemes for DTNs, namely (a) K-copy random caching, and (b) K-copy intelligent caching. 1)K-copy Random Caching For K-copy random caching, each node, j, will pass a copy of the data item to a node that j encounters next. Such an action is repeated K times so K nodes will store this data item. 2)K-copy Intelligent Caching In [11], the authors propose a spray and wait routing scheme where a source node generates L tokens for any message it generates. During the spraying phase, a node, n1, that carries a message copy with c tokens is allowed to spawn to spawn a message copy, allocate some of the tokens (say m where m< c) to that message copy and send it to another node n2. The node n1 retains (c-m) tokens for its own copy.
Any node that receives a message copy with only one token can only forward this message to the destination itself (this is referred to as the wait phase). Since the nodes may move with different maximum speed, the nodes that move faster can encounter more nodes and hence are good candidates for relaying or the storage nodes for messages. Thus, we propose having each node measures the number of unique nodes that it observes within each observation window (set to be the same as the beacon interval in this paper) and maintains a metric called friendliness metric (FM) which is merely a smoothed estimate of the average number of unique nodes it encountered.

Let T be the observation window interval, tn =[(n-1)T, nT] be the nth observation window, Si (n) be the number of unique nodes observed by node i, and iS˜ be the FM of node i.

Then, ∂=iS˜iiSnS˜)1()(∂–+ ---------- Eq(1)

Periodically, each node issues beacons and include the FM value in its beacon messages. Thus, for the K-copy intelligent caching, each source node will select a node with a FM value that exceeds FM_threshold to be a storage node. The source node repeats this action K times for each data item that it generates.

K is set to 3 in the picture. Let us assume that Node N10 is the generator of a data item, d. Thus, N10 needs to select three storage nodes for the data item, d. N10 first selects the first node it encounters, N4, to store the data since the FM value of N4 exceeds the FM_threshold. Then, N10 moves and encounters N5 which also has an FM value that exceeds FM_threshold. Thus, N5 is also selected as a storage node for the data item, d. As N10 moves along, it encounters nodes N7, N1 but since their FM values are below FM_threshold, N10 does not select them as storage nodes for the data item d. When N10 encounters N8 with a FM value that exceeds the FM_threshold, N10 selects this node to be the last storage node for the data item, d. N4, N5, and N8 will then include description of the data item d in their beacons that are broadcast periodically.

B.Query Dissemination Schemes

As indicated earlier, periodically each node broadcasts a beacon message. Several pieces of information are included in the beacon message, namely (a) a list of data items that are currently stored in this particular node, (b) a list of data items that are within its L-hop neighborhood of this node In this paper, we explore a L-hop local neighborhood query spraying (LNS) scheme. In the LNS scheme, each node that has a query broadcasts a query message after setting the TTL of the query message to

be L. If a node does not have the data item requested in the query, that node immediately relays such a query after decrementing the TTL of the query message. In addition, it will also store the query message. Any node, j, that receives a query message with a TTL of one will not relay the query further even if node j does not have that requested data item. If a node has the requested data item, it will immediately generate a query response. In Figure 2, we illustrate the LNS approach.

N8 generates a query and broadcasts it with a TTL of L=3. N6 that receives this query first stores the query since N6 does not have the requested data item. Then, N6 relays the query to N3 because the TTL still exceeds one after decrementing. N3 does not have the data item so it also stores and relays the query to N1 and N2. Since N2 knows N7 has the data item (from the periodic beacon N7 broadcasts), N2 requests for the data item and sends a query response to N8. If N2 does not have the requested data item, N2 merely stores the query but does not relay the query further since the TTL of the query that N2 receives is one.

Query Dissemination Schemes Note that since a query is stored at multiple nodes, multiple query responses may be generated. To increase the efficiency of the information retrieval system, each node can cache the identifiers of the query responses it has generated so that it does not relay any redundant query responses. C.DTN Message Routing Scheme Once a query response is generated by a node, the query response will be delivered to the querying node using the underlying DTN message routing scheme. In this paper, we consider two DTN routing scheme, namely (a) Prophet [3], and (b) Highest Encountered First Routing (HEFR) scheme. 1)Prophet Prophet uses the history of encounters and transitivity to route messages for intermittently connected networks. In this scheme, each node broadcasts a beacon periodically. This probabilistic routing scheme establishes a probabilistic metric called delivery predictability at every node A for each known destination B. This metric indicates how likely it is that node A will be able to deliver a message to that destination. The delivery predictability ages with time and also has a transitive property, i.e., a node A that encounters node B which encounters node C allows node A to update its delivery predictability to node C based on its (A's) delivery predictability to node B and node B's delivery predictability to node C. In Prophet, a node will forward a message to another node it encounters if that node has higher delivery predictability to the destination than itself. Such a scheme was shown to produce superior performance than epidemic routing [10].

3. Secure, selective group broadcast in vehicular networks using dynamic attribute based encryptio

Ciphertext-policy attribute-based encryption (CP-ABE) provides an encrypted access control mechanism for broadcasting messages. Basically, a sender encrypts a message with an access control policy tree which is logically composed of attributes; receivers are able to decrypt the message when their attributes satisfy the policy tree. A user's attributes stand for the properties that he currently owns. A user should keep his attributes up-to-date.

However, this is not easy in CP-ABE because whenever one attribute changes, the entire private key, which is based on all the attributes, must be changed. In this paper, we introduce fading function, which renders attributes "dynamic" and allows users to update each attribute separately. We study how choosing fading rate for fading function affects the efficiency and security. We also compare our design with CP-ABE and find our scheme performs significantly better under certain circumstance.

A. Attribute Based Encryption

Sahai and Waters et al. [2], [3] introduced Attribute BasedEncryption (ABE) as a new mechanism for

encrypted accesscontrol. There are several versions of ABE; the one discussedin this paper is so-called Cipher-Policy Attribute Based En-cryption (CP-ABE) [1].CP-ABE utilizes identity based encryption [7], [8] andthreshold secret sharing scheme [6]. To some extent, CP-ABEis an extension of conventional PKI to groups: An authoritygenerates public and private keys. Public key is for encryptionwhile users keep their own private keys to decrypt. In CP-ABE,public and private keys are a not one-to-one pair, instead, thereis only one public key and a potentially large number of privatekeys, one for each user in the target group.

A user's private key is associated with an arbitrary numberof attributes. One attribute corresponds to one property. Prop-erties such as name, ages and employers are different fromperson to person, so users have different attributes associatedwith their private keys. The publisher uses a policy tree, i.e.,the logical combination of various attributes, and the publickey to encrypt a message. Only clients with those attributesassociated with their private keys satisfy the policy tree candecrypt the message.In Fig. 1, the policy tree is logically composed of five differ-ent attributes. Two users try to decrypt. Kevin has attributesCA resident, UC student and AAA member so that he candecrypt the cipher while Sarah cannot.

B. Situation Aware Trust

Xiaoyan Hong et al. developed Situation Aware Trust (SAT)to provide adaptive and proactive security in mobile scenarioslike VANET. Attributes in SAT identify a group of entities(e.g., taxis associated with a company, police cars in a city), atype of events (e.g., accidents, congestions), or the property of events (location-based services, road traffic updates). They canbe further classified as dynamic attributes and static attributes,depending on whether the attributes change frequently or not[5].In SAT, vehicles fulfill a set of attributes form a "policygroup". A policy group is specified by the information sourceand is organized automatically without relying on a trust partyto manage the group [5].

For example, a company A's taxidriver can broadcast a message encrypted with policy tree"company AANDWestwood Blvd.AND10-11am" to tellhis colleagues that conventioneers will be waiting for pickup at Westwood Blvd. Hotels. The message may be broadcastto a very large area of the city. However, only company A'staxicabs that have been "certified" to be near Westwood Blvd.in the time window 10-11am can decrypt the message. Thuscompetitive advantage is ensured. At the same time, companyA's taxi drivers likely to work the morning shift in remoteareas will not be notified and will not waste time and gasunnecessarily.

4.Ciphertext-PolicyAttribute-Based Encryption

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised.

In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous attribute-based encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

Thus, our methods are conceptually closer to traditional access control methods such as role-based access control (RBAC). In addition, we provide an

implementation of our system and give performance measurements.

Bilinear Maps

We present a few facts related to groups with efficiently computable bilinear maps.LetG0andG1be two multiplicative cyclic groupsof prime orderp. Letgbe a generator ofG0andebea bilinear map,e:G0×G0→G1. The bilinear mapehas the following properties:1. Bilinearity: for allu,v∈G0anda,b∈Zp, wehavee(ua,vb) =e(u,v)ab.2. Non-degeneracy:e(g,g) 6= 1.We say thatG0is a bilinear group if the group op-eration inG0and the bilinear mape:G0×G0→G1are both efficiently computable. Notice that the mapeis symmetric sincee(ga,gb) =e(g,g)ab=e(gb,ga)

5. Key establishment in large dynamic groups using one-way function trees

We present, implement, and analyze a new scalable centralized algorithm, called OFT, for establishing shared cryptographic keys in large, dynamically changing groups.

Our algorithm is based on a novel application of one-way function trees. In comparison with the top-down logical key hierarchy (LKH) method of Wallner et al., our bottom-up algorithm approximately halves the number of bits that need to be broadcast to members in order to rekey after a member is added or evicted. The number of keys stored by group members, the number of keys broadcast to the group when new members are added or evicted, and the computational efforts of group members, are logarithmic in the number of group members.

Among the hierarchical methods, OFT is the first to achieve an approximate halving in broadcast length, an idea on which subsequent algorithms have built. Our algorithm provides complete forward and backward security: Newly admitted group members cannot read previous messages, and evicted members cannot read future messages, even with collusion by arbitrarily many evicted members.

In addition, and unlike LKH, our algorithm has the option of being member contributory in that members can be allowed to contribute entropy to the group key. Running on a Pentium II, our prototype has handled groups with up to 10 million members. This algorithm offers a new scalable method for establishing group session keys for secure large-group applications such as broadcast encryption, electronic conferences, multicast sessions, and military command and control.

III. CONCLUSION & FUTURE WORK

Proposed an efficient privacy preserving and secure data retrieval method using Advanced Encryption Standard technique for decentralized DTNs where key authorities manage their attributes independently.The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted .In addition ,the fine -grainedkey revocation can be done for each attribute group.we demonstrate how to apply the proposed mechanism to securly and efficiently manage the confidential data distributed in the disruption-tolerent military network.So the mentioned work of our idea DTN technologies are becoming successful solutions in military applications that allow wireless services to communicate with each other and access the confidential information reliably by exploiting external storange nodes.

The DTN community encourages all DTN imlementation to inter-operate with the reference implementations.When the security mechanisms are re-leased in the reference implementation,a useful future work would be to test this implementation against it.In the presents work we implemented a secure data transmission technique that provides all security services altogether:encryption ,data protection and authenticity. The future can extends

user validation for set of attribute in authendication of multi authority network environment. We can hide the attribute in access control policy of a user.Different users are allowed to decrypt different poeces of data per the securely policy.

IV. REFERENCES

[1]. J. Burgess, B. Gallagher, D. Jensen, B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks", Proc. IEEE INFOCOM, pp. 1-11, 2006.

[2]. M. Chuah, P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks", Proc. IEEE MILCOM, pp. 1-6, 2006.

[3]. M. M. B. Tariq, M. Ammar, E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes", Proc. ACM MobiHoc, pp. 37-48, 2006.

[4]. S. Roy, M. Chuah, “Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs”, 2009.

[5]. M. Chuah, P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs", Proc. IEEE MILCOM, pp. 1-7, 2007.

[6]. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu, "Plutus: Scalable secure file sharing on untrusted storage", Proc. Conf. File Storage Technol., pp. 29-42, 2003.

[7]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application", Proc. WISA, pp. 309-323, 2009.

[8]. N. Chen, M. Gerla, D. Huang, X. Hong, "Secure selective group broadcast in vehicular networks using dynamic attribute based encryption", Proc. Ad Hoc Netw. Workshop, pp. 1-8, 2010.

[9]. D. Huang, M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks", Ad Hoc Netw., vol. 7, no. 8, pp. 1526-1535, 2009.

[10]. A. Lewko, B. Waters, “Decentralizing attribute-based encryption”, 2010.

[11]. A. Sahai, B. Waters, "Fuzzy identity-based encryption", Proc. Eurocrypt, pp. 457-473, 2005.

[12]. V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", Proc. ACM Conf. Comput. Commun. Security, pp. 89-98, 2006.

[13]. J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption", Proc. IEEE Symp. Security Privacy, pp. 321-334, 2007.

[14]. R. Ostrovsky, A. Sahai, B. Waters, "Attribute-based encryption with non-monotonic access structures", Proc. ACM Conf. Comput. Commun. Security, pp. 195-203, 2007.

[15]. S. Yu, C. Wang, K. Ren, W. Lou, "Attribute based data sharing with attribute revocation", Proc. ASIACCS, pp. 261-270, 2010.

[16]. A. Boldyreva, V. Goyal, V. Kumar, "Identity-based encryption with efficient revocation", Proc. ACM Conf. Comput. Commun. Security, pp. 417-426, 2008.

[17]. M. Pirretti, P. Traynor, P. McDaniel, B. Waters, "Secure attribute-based systems", Proc. ACM Conf. Comput. Commun. Security, pp. 99-112, 2006.

[18]. S. Rafaeli, D. Hutchison, "A survey of key management for secure group communication", Comput. Surv., vol. 35, no. 3, pp. 309-329, 2003.

[19]. S. Mittra, "Iolus: A framework for scalable secure multicasting", Proc. ACM SIGCOMM, pp. 277-288, 1997.

[20]. P. Golle, J. Staddon, M. Gagne, P. Rasmussen, "A content-driven access control system", Proc. Symp. Identity Trust Internet, pp. 26-35, 2008.

[21]. L. Cheung, C. Newport, "Provably secure ciphertext policy ABE", Proc. ACM Conf.

Comput. Commun. Security, pp. 456-465, 2007.

[22]. V. Goyal, A. Jain, O. Pandey, A. Sahai, "Bounded ciphertext policy attribute-based encryption", Proc. ICALP, pp. 579-591, 2008.

[23]. X. Liang, Z. Cao, H. Lin, D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption", Proc. ASIACCS, pp. 343-352, 2009.

[24]. M. Chase, S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption", Proc. ACM Conf. Comput. Commun. Security, pp. 121-130, 2009.

[25]. M. Chase, "Multi-authority attribute based encryption", Proc. TCC, pp. 515-534, 2007.

[26]. S. S. M. Chow, "Removing escrow from identity-based encryption", Proc. PKC, pp. 256-276, 2009.

[27]. M. Belenkiy, M. Chase, M. Kohlweiss, A. Lysyanskaya, "P-signatures and noninteractive anonymous credentials", Proc. TCC, pp. 356-374, 2008.

[28]. M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Hysyanskaya, H. Shacham, "Randomizable proofs and delegatable anonymous credentials", Proc. Crypto, pp. 108-125.

[29]. D. Naor, M. Naor, J. Lotspiech, "Revocation and tracing schemes for stateless receivers", Proc. CRYPTO, pp. 41-62, 2001.

[30]. C. K. Wong, M. Gouda, S. S. Lam, "Secure group communications using key graphs", Proc. ACM SIGCOMM, pp. 68-79, 1998.

[31]. A. T. Sherman, D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees", IEEE Trans. Softw. Eng., vol. 29, no. 5, pp. 444-458, May 2003.

[32]. K. C. Almeroth, M. H. Ammar, "Multicast group behavior in the Internet's multicast backbone (MBone)", IEEE Commun. Mag., vol. 35, no. 6, pp. 124-129, Jun. 1997.

[33]. “The Pairing-Based Cryptography Library”, Accessed Aug. 2010.