Reliable Anonymous Multicasting in Disruption Tolerant Networks

Kamalavasan Srinivasan and Parameswaran Ramanathan

Department of Electrical and Computer Engineering
University of Wisconsin, Madison, WI 53706–1691
Email: {ksriniva, parmesh}@ece.wisc.edu

Abstract—**Disruption Tolerant Networks (DTNs) are characterized by opportunistic connectivity due to frequent network partitioning. Protocols used in wired and wireless networks have assumed the existence of end-to-end paths from a source to a destination, which is not true in DTNs applications. Our focus in this work is to propose a scheme that deterministically guarantees message delivery to all multicast receivers in DTNs making controlled use of non-multicast nodes to reduce message delivery latency. The paper also introduces a new measure called termination delay and simulation results show that our scheme has much smaller termination delay than schemes in literature. Second, we extend our reliability scheme to provide anonymity of multicast receivers in the group. We show through simulations that even in the presence of malicious nodes the performance degradation of message delivery latency and termination latency is not any worse than schemes currently proposed in literature.**

I. Introduction

Disruption Tolerant Networks (DTNs) are based on the premise that the network is often highly partitioned and there is no connected end-to-end path between most pairs of nodes at any given time instant. For example, vehicular battlefield network of sensing devices carried by troops or vehicles in a battlefield [1], providing infrastructure access to isolated villages through communication equipped rural buses [2], and wildlife monitoring through devices attached to animals under study could be considered as a DTN.

Many of the afore-mentioned applications involve distribution of data to a group of devices in the network. This could be implemented by sending separate unicast messages to each receiver. However, this approach does not work well in many situations as shown by Zhao et. al. in [3]. They compare the performance of several schemes, namely Static Tree-Based Routing, Dynamic Tree-Based Routing, Group-Based Routing, Broadcast-Based Routing, and Unicast-Based Routing under different knowledge models and traffic conditions in DTNs. There have been other work on probabilistic delivery for multicasting in DTNs similar to [4].

Reliable multicasting for ad-hoc networks has been studied by [5], [6] to name a few. However, they are not well suited for DTNs as they assume end-to-end connectivity or they do not exploit opportunistic node meetings. A complementary area of research is on security of DTNs. These networks are vulnerable to spoofing, denial of service and traffic analysis attacks due to the open nature of wireless communication [7]. Prior work in DTNs have addressed authentication of communicating nodes, key distribution and secure multicast group adapting to changes with time [8]–[10].

In this paper, we focus on preserving the identities of the multicast receivers. The source node would be the only node aware of the multicast receiver identity in the network. No other node (including group members) must be able to identify any multicast group member. Onion routing [11], Crowds [12] and mix networks [13] are well-known techniques for anonymous communication with fixed paths. In the presence of dynamic topology and the absence of a fixed infrastructure, route maintenance schemes does not suit well for DTNs. Anonymous multicasting was considered by Perng et. al. in [14]. Their scheme relies on the availability of multiple mix infrastructure nodes in the network between the producer and the consumer. Xiao et al. proposed the Mutual Anonymous Multicast protocol, where they construct static anonymous multicast tree [15] that does not make use of opportunistic node meetings.

Contribution: We focus on guaranteed anonymous message delivery in the context of DTNs. The key features of the proposed scheme are as follows. First, it does not rely on a fixed multicast tree to guarantee anonymous message delivery. Instead, it utilizes changes in connectivity as they occur to deliver the messages. Second, it makes controlled use of non-multicast nodes to substantially improve the average latency of message delivery when there are no malicious nodes in the network. Even in the presence of large number of malicious nodes, the average latency is comparable (if not slightly better) than other schemes in literature. Third, in addition to delivery latency, the scheme also controls a measure called termination delay. We consider a message to have terminated when all non-malicious nodes know that the message has been successfully delivered to all the receivers. Simulation results show that the proposed scheme does significantly better than other schemes in terms of message delivery latency and termination delay when there are no malicious nodes. In the presence of malicious nodes, the schemes have comparable performance and we perform as good as a flooding scheme.

II. Model and Assumptions

A. Network Model

The network is comprised of N mobile nodes. There is limited connectivity between a pair of nodes at any given time instant. Whenever nodes come within range of each other

978-1-4244-2324-8/08/$25.00 © 2008 IEEE.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2008 proceedings.

they remain in contact for a finite non-zero period that is long enough to transfer the necessary data.

All nodes move within the same region in such a way that there is a non-zero probability for each node to come in contact with every other node. We assume that nodes do not have any prior knowledge of the contact information and multicast group changes are infrequent. Our reliable multicasting scheme can be extended to deal with the case where all nodes do not necessarily move within the same territory. However, such extensions are discussed in a complementary paper [16].

B. Security Model

Table I introduces various notations used through the rest of the paper.

ID_i : The pseudonym identity of Node i
K_i : Symmetric Session Key for Node i
GK : Multicast Group Key
$E_{GK}(M)$: Message M is encrypted with group key GK
N_i : Random Nonce generated by node i
$N_i^{'}$: Message response to Random Nonce generated by Node i
$H_{GK}(M)$: HMAC computed over message M using secure GK
$E(M)||E(M')$: Encryption of message M concatenated with encryption of message M'

TABLE I
NOTATIONS

We assume the existence of two different keys in the network.

- Group Key (GK): This key is established between multicast receivers for every new multicast session in the network. Group key is generated by a key generation server.
- Individual Key (IK): We assume that all nodes in the network share a pairwise key with the key server. This key is used for secure message exchanges with the key server.

Any multicast receiver could anonymously join the group by authenticating with a key generation server. At that time instant, the group key is updated and all multicast receivers are assured to receive the group key update message. There is a mutual trust between all group members, as they share a secret group key. In this work, we are concerned with anonymity of multicast receivers. Yet, we do not want a malicious node to compromise the security during key exchange or key update from the authentication server to the various nodes in the network. We use algorithms similar to the scheme by Lam [17] in DTNs context for key updates.

We consider all non-multicast nodes to be untrusted. One or more non-multicast nodes in the network could be malicious nodes. All group members, are considered honest, but curious nodes. They follow the protocol and do not misbehave. Yet, they could potentially reveal identity of other multicast nodes if compromised.

We assume that nodes use pseudonyms instead of their real identifiers in the multicast message distribution process. Each node must use a dynamically changing, statistically unique cryptographically verifiable pseudonym that is collision resistant [18].

1) Anonymity Goals: The proposed scheme is designed to achieve *multicast group anonymity*. In other words, both multicast and non-multicast nodes should not be able to identify any multicast receiver identity. Our scheme provides a robust method for preserving the identities in the following contexts:

- Any communication exchange between a set of nodes should preserve the identity of multicast receivers while guaranteeing message delivery.
- Malicious nodes should not be able to collude information gathered from multiple receivers to reveal the identity of any multicast receiver.

2) Threat Model: We consider the following threats that could compromise anonymity of our multicast group members.

Restricted Adversary: Attacks mounted by an external adversary are classified as a restricted adversary attack. An outsider to the network is allowed to monitor the communication channels and be a passive eavesdropper.

Internal Adversary: A stronger attack is by an internal non-multicast network node called Byzantine adversary. These nodes could compromise the identity of the multicast group members by colluding information or replaying messages or eavesdropping.

We focus our anonymity scheme to protect the identity of multicast receivers in the face of *Restricted Adversary* and *Internal Adversary* attacks.

III. Review of Two Reliable Forwarding Schemes

In this section, we briefly review two possible multicast schemes for DTNs. We primarily focus on their drawbacks to better understand the design challenges addressed by the proposed scheme.

A. Reliable Group Based Forwarding (RGBF)

This scheme was discussed and characterized in [3]. The scheme involves flooding of the multicast message among all the multicast receivers in group M. In order to ensure all receivers get the message, each node in the multicast group maintains custody of the message until it has met all the other nodes.

There are two key drawbacks to this approach. First, the scheme does not utilize non-multicast nodes in the network to possibly reduce the latency of termination. Second, the termination latency of RGBF may be large because each node must wait until it meets all other nodes in M before relinquishing the custody.

B. Source Assured Reliability (SAR)

This scheme is a modification of $RGBF$, where only the source node is responsible for reliability assurance. Message forwarding is similar to RGBF. The source completes its custodial responsibilities when it has met all the nodes in M. All other nodes in M do not have any custodial responsibilities. SAR also does not exploit opportunistic node meetings in the network to improve the termination latency.

IV. Proposed Reliable Multicasting Solution

Consider a typical message m in the multicast stream. Let M denote the set of multicast receivers for message m. Let k denote the design parameter that represents the maximum number of non-multicast nodes which can be used in delivering the message. These non-multicast nodes are used to potentially reduce the latency of delivering the message. We refer to the proposed scheme with parameter k as Single Territory Reliable Anonymous Protocol (STRAP-k). We introduce a parameter l that controls the number of nodes a custodial node has to meet before it could terminate the multicast message m.

Our problem of reliable multicasting is to devise a scheme that has low delivery latency, termination latency, and energy consumed in delivering the message. However, it may not be feasible to simultaneously reduce all three of these measures. Our goal is exploit the trade off between these measures while devising our scheme. An interested reader can refer to our technical report for a formal definition of this problem [19].

A. Reliable Multicasting Solution

To ensure reliable delivery of m to all nodes in M, STRAP-k employs a scheme in which nodes have certain "custodial" responsibilities for delivering the message. During the course of message delivery, a multicast node may be assigned custodial responsibility for delivering the message to certain number of nodes. When a node is assigned custodial responsibilities for delivering the message to d other nodes, it fulfills the responsibility in one of two ways: (i) by directly delivering the message to some $x \leq d$ nodes, and (ii) by transferring custodial responsibilities for the remaining $d-x$ nodes to other nodes. When a node completes its custodial responsibility for a message m, it can remove the message from its buffer and we say that the node has *terminated* with respect to the message.

In the proposed scheme, each node in the network periodically broadcasts a beacon and nodes within communication range of the sender reply with their sequence number and the state (to be defined later) of each message in their queue. Further interactions for a particular message depends on its state at the two nodes.

In STRAP-k, any node i can be in one of the following four possible states with respect to message m.

- *Not Yet Received Message* (NYRm)
- *Received Message No Custody* (RmNC)
- *Received Message Have Custody* (RmHC)
- *Terminated Message* (Tm)

When node i begins interaction with node j there are 16 possible state combinations for each message. For simplicity of presentation, we look at the interesting cases, one can refer to [19] for a more detailed illustration and proof of correctness.
Case 1: ($i \in$ RmNC$, j \in$ NYRm): If $j \in M$, node i forwards the message to node j and node j transitions to state RmNC.
Cases 2, 3: $i \in$ RmHC and $j \in \{$NYRm$,$ RmNC$\}$: This is one of the most interesting cases. Only multicast nodes can have custodial responsibility, as a result, node $i \in$ RmHC implies that node $i \in M$. The actions executed by node i depends on whether or not node j is a multicast node.

- Subcase A: $i \in M$ and $j \in M$: There are four key steps executed by node i. First, if node j is in NYRm then node i forwards the message to node j. Second, node i transfers some of its custodial responsibilities to node j. More specifically, let d_m be the number of nodes for which node i was originally given the custodial responsibilities. Let, $c_m = \min\{d_m - 1, l\}$. Then, node i transfers custodial responsibilities for approximately $(d_m - 1)/c_m$. It is approximate because $(d_m - 1)/c_m$ may not be an integer. There are simple ways of dealing with this situation. For instance, let $r = (d_m - 1) \bmod c_m$. Then, for the first r nodes, transfer custody for $\lfloor (d_m - 1)/c_m \rfloor + 1$. For the remaining $c_m - r$ nodes transfer custody of $\lfloor (d_m - 1)/c_m \rfloor$. This results in a net transfer of custody for $d_m - 1$ nodes.
  Third, the nodes also pass along information to bound the number of non-multicast nodes that can be used. In particular, when node i was given custody (i.e., when it transitioned to RmHC), it was also given another parameter s_m which specifies the maximum number of non-multicast nodes it can use to deliver the multicast message. When node i transfers custody to node j, it also allocates approximately s_m/c_m non-multicast nodes to node j.
  Finally, if j is the c_m^{th} node to which it transferred custody, then node i terminates for m, i.e., it transitions to Tm. If node j receives custody for only one node, then node j transitions to Tm. Otherwise, node j transitions to RmHC.
- Subcase B: $i \in M$ and $j \notin M$: When node i is given custody, it was also given another parameter s_m which specifies the maximum number of non-multicast nodes it can use for message delivery. If $s_m > 0$, based on the state of node j one of the following actions would be performed. If $s_m = 0$, then node j is ignored.
  - Node $j \in$ NYRm - Node i forwards the multicast message to node j. Also, node j sets a timer t_v, which specifies the time to live factor of the message at node j. When this timer expires, the message is deleted by node j and node j transitions to Tm.
  - Node $j \in$ RmNC - No further action is taken.

B. Reliable Anonymous Multicasting

In this section, we extend our reliability scheme to achieve anonymity of multicast receivers in STRAP-k. We preserve multicast receiver identities during interactions with other nodes in the network. Generally, our anonymity goal could be stated as follows: given a node i, no other node in the network should be able to predict if it is a multicast receiver from the message interactions it has had in the past.

Our reliability scheme has certain attributes that ensure anonymous communication. First, we do not explicitly specify the multicast receiver addresses. Every custodial node that provides guarantee to other multicast receivers are only informed of the number of multicast receivers and not the identity of the receivers. Second, our authentication scheme described below enables any node i to authenticate a multicast group member j without revealing identities of either nodes.

1) Anonymous Authentication: When any node i in the network meets the source node, it securely gets a pair $(K_i, E_{GK}(K_i))$. Here, K_i is the individual session key for node i and $E_{GK}(K_i)$ is the individual session key encrypted with the group key. Note that, all nodes in the network receive this pair. Only multicast receivers would be able to modify $E_{GK}(K_i)$, non-multicast nodes would be able to use the key to decrypt or encrypt messages, but cannot modify the contents of this message.

When two nodes i and j interact at any instant of time for reliable multicasting scheme described above, we need to authenticate if one of them is a multicast node without revealing the identity of nodes i and j. The procedure for this authentication is as follows.

Actions Performed by Node i: Node i generates a new pseudonym for communication with node j. It sends the following challenge message to node j $(E_{GK}(K_i)||E_{K_i}(N_i))$.

Actions Performed by Node j: If node j is not a multicast node, it cannot create a meaningful response, since Group Key GK is not known to a non-multicast node. If it is a malicious non-multicast node, the response is unpredictable.

If node j is a multicast node, the following action is taken. Node j decrypts the message from node i. It first retrieves key K_i from the message. Here, $D_K(m)$ denotes, decryption of the message m with the key K represented as: $(D_{GK}(E_{GK}(K_i)))$.

It then retrieves the random nonce sent from node i by decrypting the message with key K_i given by: $(D_{K_i}(E_{K_i}(N_i)))$.

Finally, Node j computes the response $N_i^{'}$. Here $H_{K_i}(m)$, denotes the secure keyed hash function (approximated by *HMAC-SHA1* [20]). The response for the random nonce N_i can be created only by node i and other multicast receivers $(N_i^{'} = H_{K_i}(N_i))$.

Node j generates a random pseudonym and sends $E_{K_i}(N_i^{'})$ to node i. If node i receives an appropriate response $N_i^{'}$ from node j, it validates node j to be a multicast node. If it received any other response from node j, it ignores node j.

C. Analysis of STRAP-k

We analyze our RAP solution against the threat model.

1) Anonymity: In this section, we discuss four kinds of attacks that could compromise anonymity of multicast receivers.

Dropping Packets: The simplest attack is to drop packets that were received from a legitimate node in the network. This attack would affect the packet delivery latency and the termination latency.

This attack is thwarted by the use of trusted multicast group members for assuring reliability and a controlled use of non-multicast nodes that could opportunistically forward packets.

Replay Attack: Malicious adversaries could capture and store authentication message exchanges between any two nodes. Our scheme is protected against this attack due to the following:

- Neither K_i nor GK is explicitly sent over the air. Thus, malicious adversaries cannot retrieve GK or K_i through eavesdropping. If they cannot obtain these keys, they cannot decipher the message exchanges in polynomial time and send appropriate replies to the challenge.
- A random nonce is used for every message exchange to preserve freshness. This prevents a malicious adversary from pretending to be another multicast node by resending eavesdropped messages during a later interaction.
- We make use of random pseudonyms that two interacting nodes pick for every message exchange.

Collusion Attack: A malicious node could collude information gathered from interactions with multicast nodes. This information should not reveal any more than what the malicious node could have determined by interaction with the multicast node.

STRAP-k efficiently thwarts this by use of pseudonyms for every interacting node. Also, our reliability scheme does not require explicit multicast receiver information from being sent to custodial nodes.

For the same reasons, a multicast receiver cannot identify another receiver from the group.

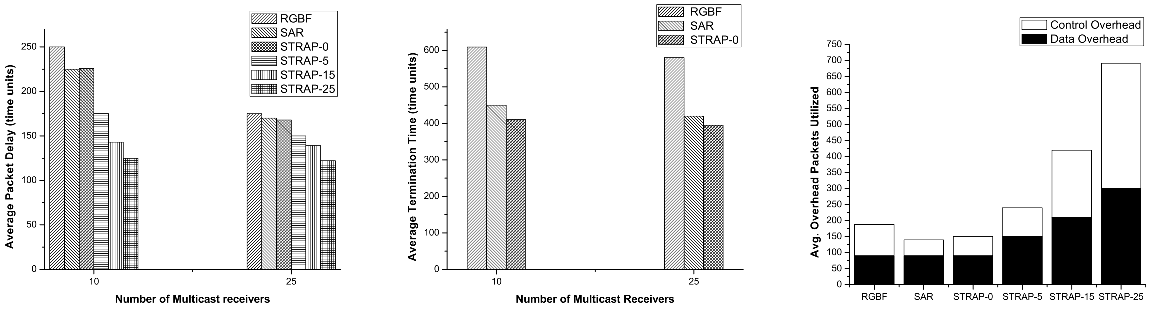
V. Performance Evaluation

To characterize the effectiveness of our Reliable Anonymous Protocol, we present simulation results comparing its performance to that of RGBF and SAR. The simulations are done using a DTN simulation tool called *dtnsim* developed by us.

We have 50 nodes moving in a 100x100 region and follow a random waypoint mobility model. The communication range was chosen such that on the average the strongest connected component has fewer than 50% of the nodes. The results are averaged over 10 runs of 10000 multicast messages per run. One set of simulation results correspond to a scenario in which the multicast group consists of 10 pre-selected nodes, while the other corresponds to a group of 25 nodes. The number of non-multicast nodes is varied to characterize the effect of k on the performance. The performance as shown in Figures 1(a)–1(c) is characterized using average delivery latency, average termination latency, and average energy (packets) consumed in the data and control transmissions.

In each figure, there are two bars for every scheme. The bar on the left (right) shows the results for 10 (25) nodes in the multicast group. Figure 1(a) shows the results for RGBF, SAR, STRAP-0, STRAP-5, STRAP-15, and STRAP-25. The average delivery latency reduces with increase in number of multicast receivers. Further, note that the average delivery latency decreases as k, the number of non-multicast nodes participating increases. For large k the latencies are much smaller than that for the flooding schemes like RGBF and SAR because more non-multicast nodes are being utilized for forwarding. Even in the presence of 25 malicious non-multicast nodes the performance of our scheme does not degrade more than SAR or $RGBF$ in terms of packet delivery latency.

In Figure 1(b), observe that the average termination delay of the STRAP scheme is much smaller than RGBF and SAR.



(a) Average Packet Delay (b) Average Termination Time (c) Average Overhead Energy

Fig. 1. Performance Evaluation of STRAP-k

This again demonstrates the enhancements achievable using the proposed scheme. The proposed scheme benefits from participating non-multicast nodes. The presence of malicious nodes do not affect the termination latency under the threat model described in this paper. We only have STRAP-0 scheme as the non-multicast nodes do not participate in custodial responsibilities.

Improvements in packet delay and the termination latency occur at the expense of additional energy consumption (see Figure 1(c)). For simplicity of presentation, the plot only shows a ratio of $1 : 10$ packets, that is 1 unit of control overhead is equivalent to 10 units of data overhead. As expected, both the data energy and control energy increases with k. Therefore, there is a trade off between energy consumed and the latencies achieved. However, comparing the results for RGBF, SAR, STRAP-0, and STRAP-5, we observe that STRAP-5 is better than RGBF and SAR because the latencies and energy are comparable. This provides us a qualitative way of choosing the number of non-multicast nodes participating in the proposed scheme.

VI. Conclusion

This paper proposed an algorithm for reliable anonymous multicast packet delivery in DTNs. The proposed algorithm is designed to overcome the shortcomings of frequent network partitioning that characterizes DTNs. Comparative simulation studies of *STRAP-k* against RGBF and SAR showed that our algorithm outperforms others in terms of the termination delay and message latency. Although, we assumed the presence of key distribution and key management techniques, it is a topic for further research in disconnected networks.

References

[1] K.-C. Wang and P. Ramananthan, "Collaborative sensing using sensors of uncoordinated mobility," in *Proceedings of International Conference on Distributed Computing in Sensor Systems*, 2005.

[2] A. Pentland, R. Fletcher, and A. Hasson, "A road to universal broadband connectivity," in *Proceedings of the 2nd International Conference on Open Collaborative Design for Sustainable Innovation (dyd 02)*, December 2002.

[3] W. Zhao, M. Ammar, and E. Zegura, "A message ferrying approach for data delivery in sparse mobile ad hoc networks," in *Proceedings of MobiHoc*, May 2004.

[4] J. H. J. Luo, P.T. Eugster, "Route driven gossip: Probabilistic reliable multicast in ad hoc networks," in *INFOCOM'03, San Francisco, CA*, March 2003, pp. 2229–2239.

[5] S. Floyd, V. Jacobson, S. McCanne, C.-G. Liu, and L. Zhang, "A reliable multicast framework for light-weight sessions and application level framing," in *SIGCOMM '95*. New York, NY, USA: ACM Press, 1995, pp. 342–356.

[6] T. Gopalsamy, M. Singhal, D. Panda, and P. Sadayappan, "A reliable multicast algorithm for mobile ad hoc networks," in *ICDCS '02*. Washington, DC, USA: IEEE Computer Society, 2002, p. 563.

[7] S. Farrell and V. Cahill, "Security considerations in space and delay tolerant networks," in *SMC-IT '06: Proceedings of the 2nd IEEE International Conference on Space Mission Challenges for Information Technology*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 29–38.

[8] S. Capkun, J. Hubaux, and L. Buttyan, "Mobility helps peer-to-peer security," 2005. [Online]. Available: citeseer.ist.psu.edu/capkun05mobility.html

[9] S. Seth, A. Keshav, "Practical security for disconnected nodes," in *Secure Network Protocols, 2005. (NPSec). 1st IEEE ICNP Workshop on*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 31–36.

[10] S. Symington, "Secure multidestination delivery in dtn," Tech. Rep., 2005.

[11] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Proxies for anonymous routing," in *ACSAC '96: Proceedings of the 12th Annual Computer Security Applications Conference*. Washington, DC, USA: IEEE Computer Society, 1996, p. 95.

[12] M. K. Reiter and A. D. Rubin, "Anonymous Web transactions with crowds," *Communications of the ACM*, vol. 42, no. 2, pp. 32–48, 1999. [Online]. Available: citeseer.ist.psu.edu/reiter99anonymous.html

[13] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[14] M. R. G.Perng and C. Wang, "M2: Multicasting mixes for efficient and anonymous communication," in *ICDCS 2006*, July 2006, pp. 59–59.

[15] L. Xiao, Y. Liu, W. Gu, D. Xuan, and X. Liu, "Mutual anonymous overlay multicast," *J. Parallel Distrib. Comput.*, vol. 66, no. 9, pp. 1205–1216, 2006.

[16] K.Srinivasan and P.Ramanathan, "Reliability assurance protocol for multicasting in disruption tolerant networks," Transactions on Mobile Computing (In review).

[17] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *IEEE/ACM Trans. Netw.*, vol. 8, no. 1, pp. 16–30, 2000.

[18] G. Montenegro and C. Castelluccia, "Statistically unique and cryptographically verifiable," 2002.

[19] K.Srinivasan and P.Ramanathan, "Reliable anonymous protocol for multicasting in disruption tolerant networks," UW-Madison WANDER lab Technical Report - 2007.

[20] M. B. H.Krawczyk and R. Canetti, "Hmac: Keyed-hashing for message authentication." [Online]. Available: http://www.faqs.org/rfcs/rfc2104.html