Radenkovic, Milena and Vaghi, Ivan and Zakhary, Sameh and Benslimane, Abderrahim (2013) AdaptAnon: adaptive anonymity for service queries in mobile opportunistic networks. In: 2013 IEEE International Conference on Communications (ICC), 9-13 June 2013, Budapest, Hungary.

AdaptAnon: Adaptive Anonymity for Service Queries in Mobile Opportunistic Networks

Milena Radenkovic[1] mvr@cs.nott.ac.uk
Ivan Vaghi[2] ivan@earlymorning.com
Sameh Zakhary[1] szz@cs.nott.ac.uk
Abderrahim Benslimane[3] abderrahim.benslimane@univ-avignon.fr

[1] *School of Computer Science, University of Nottingham, Nottingham, NG8 1BB, UK*
[2] *EarlyMorning, 20127 Milano, ITALY*
[3] *Avignon Computer Science Laboratory, Avignon University, FRANCE*

Abstract—**Social routing protocols are typically used to transfer messages among users and services in mobile opportunistic networks. Adaptive mechanisms are needed for achieving user anonymization and providing sufficient level of user anonymity due to the constant changes in underlying topology, mobility patterns and density of users and their queries. This paper describes a novel flexible and adaptive approach, AdaptAnon that is suitable for dynamic and heterogeneous mobile opportunistic networks. Our approach is multidimensional and combines multiple heuristics based on user profiles, analysis of user connectivity and history of anonymization in order to predict and decide on the best set of nodes that anonymize the sending node. Our results of extensive experiments show that AdaptAnon achieves higher quality of anonymization in terms of both the number of nodes and the diversity of nodes in the anonymization layer for varying query intensity and over different sender and destination degrees of connectivity while neither decreasing success ratios nor increasing latency. We show that AdaptAnon outperforms state of the art single dimensional anonymization approaches when run over three different real-life traces.**

Keywords-Mobile social networks; Anonymity; Adaptive networks

I. INTRODUCTION

Due to the recent wide penetration of mobile devices in everyday's life activities, there has been an intense research on how to design data dissemination protocols within mobile social opportunistic networks [1,2,3,4,12,17,18]. These protocols are typically based on the assumption that encounters between mobile devices are more likely to occur between people in the same social network than between random strangers – i.e. messages may be forwarded selectively only within the sender's social network. This paper addresses the problem of privacy in opportunistic network routing schemes and argues that using social network for forwarding can be damaging for maintaining sender's anonymity due to routing protocols repeatedly using similar (friendly) nodes for forwarding and anonymizing their messages. In particular, we explore how to design adaptive anonymous overlays in social opportunistic networks that aim to maximise the quality of anonymization while maintaining high success ratios of answered queries and low delays. As the underlying density of network may change dramatically and the user interests may also vary, it is important that the anonymization overlay is responsive both to the underlying topology as well as to the users' interests. We propose a multidimensional K-anonymity approach for designing anonymous overlays (paths) to hide the senders' identity from the service. Our approach aims to dynamically and adaptively balance the tradeoff between quality of anonymization, and success ratios and delays of answered queries. We refer to the quality of anonymization as a combined measure of the number of nodes and the diversity of the nodes used in the anonymization path for a given sender and a given service. As our networks are intermittently connected and potentially have large delays, discovering the entire "anonymization overlay" at any one time is not possible, and this paper, instead, focused on how to build an "anonymization path" that allows opportunistic, asynchronous discovery of nodes that can perform user anonymization.

Emerging research [23] on characteristics of mobile advertising shows that almost all advertisements are selected based on the users' profiles created over time or recent environmental context and that advertising traffic volume is significantly higher than that of the application traffic. This paper aims to address this by making users' context and long term profiles less predictable. Our proposal, AdaptAnon, manages to extend the length of the anonymity path and increase the diversity of the nodes in it. We propose a set of multiple heuristics for tracking anonymization history and adaptively selecting more suitable anonymizers. We show that increasing the length of the anonymity path leads to the increase of repetitive choice of the nodes on the path and thus decreases the quality of anonymization as it becomes more predictable. On the other hand, if we increase the diversity of chosen nodes, the length of the anonymization path decreases because the nodes have fewer appropriate next hop options but decreases predictability in the overlay improving anonymization.

The rest of the paper is organised as follows. After a review of the related work in Section 2, we describe a set of new heuristics that are at the core of AdaptAnon and give pseudo code of AdaptAnon in Section 3. In section 4, we describe results from extensive evaluation of AdaptAnon against three other anonymization protocols across a range of metrics over a real social mobility trace from Crawdad [20].

II. RELATED WORK

This section gives a brief overview of anonymity approaches in peer to peer communications, social opportunistic networks and mobile networks.

Peer to peer anonymity approaches such as Tor[13], Tarzan[14], Crowds[16] are all based on routing the traffic over virtual "circuits" that are established by randomly choosing a sequence of nodes but vary in the length of the

route and level of encryption. All of these schemes rely on a global list of all participants being shared among all the participants and thus have limited scalability. There are several proposals for anonymity schemes based on DHT overlays in the literature [5,6] but these schemes are not suitable for the opportunistic ad hoc and mobile scenarios that we target.

[7] considers social network routing that is based on disseminating information about the social network and describes the privacy concerns it introduces. It proposes two methods for enhancing privacy in social network routing by obfuscating the social network graphs used to inform routing decisions and show that it is possible to obfuscate the social network information without significantly decreasing routing performance. In [16], mobile users get classified in different areas according to their social behaviour and observe that under certain circumstances, that are common in real life situations, the effectiveness of dissemination predominantly depends on the number of users in each class rather than their social behaviour. [17] proposes PeopleRank approach in which nodes are ranked using a tuneable weighted social information that gives higher weight to nodes if they are socially connected to other important nodes of the network and manages to deliver messages with near optimal success rate.

[9] proposes AnonySense, a privacy-aware system for realizing pervasive applications based on collaborative, opportunistic sensing by personal mobile devices. However, they assume that the nodes who wish to participate in the AnonySense have to register with the registration authority as well as that the IP addresses and certificates of the task service (TS) and the report service are installed on the mobile nodes. [10] describes SMILE, a mobile social service in which trust is established solely on the basis of shared encounters and anonymous users' ability to prove to each other that they shared an encounter in the past. SMILE uses standard cryptographic primitives that assume existence of trusted third party.

[18] proposes software (SpotME) that can run on a mobile phone and is able to estimate the number of people in geographic locations in a privacy-preserving way: accurate estimations are made possible in the presence of privacy-conscious users who report, in addition to their actual locations, a very large number of erroneous locations. [21] proposes constructing a Privacy Analytics framework that uses the Dataware framework [20] to enable querying and measurements of large public datasets without leaking intermediate results and potentially compromising privacy. [21] aims to verify the query code, and then send it to the user community to perform measurement tasks, collect variable statistics, and perform aggregation and fuzzing while remaining within the community.

[23] proposes middleware, CAMEO, that uses predictive profiling of a user's device, network and usage context to anticipate the advertisements to be sent, and then modulates their delivery mechanism to enable effective and low cost mobile advertising. CAMEO manages to cache appropriate advertisements in advance for future display to each user. [19] proposed SLPD protocol based on social network driven K-anonymity for location privacy but showed that SLPD's query success ratios quickly drop below 20% for privacy level above 20%.

III. ADAPTANON PROPOSAL DESIGN OVERVIEW

Three challenges in the design of the anonymous overlay networks in social mobile opportunistic networks that we focus on concern the relationship between the level of security provided for different 1) the density of users and services, 2) length of the anonymization path (K) and 3) diversity of the users on the anonymization path. More specifically, this refers to how to "hide" a user among not only more users and but also more diverse users in order to provide higher quality anonymity for changing underlying topologies. Because improving anonymity can have negative impact on success ratio and latency of the user-service communication, it is important to dynamically balance the tradeoff between the anonymity and the actual quality of service.

This section proposes novel flexible, multi-dimensional approach to K-anonymity (AdaptAnon) that enables opportunistic identification and selection of the overlay anonymization nodes in order to allow for better tradeoff management between the length of the obfuscation path and the diversity of the nodes on it while not degrading success ratio and delays. We propose to dynamically combine three types of implicit fully localized heuristics that are rooted in social complex graph theory that enable better prioritisation of nodes based on their connectivity patterns, user and interest profile similarity, and anonymization history.

The choice of which connectivity, user profile and anonymization history heuristics to consider and how to combine them determines the effectiveness of our proposal. First we motivate and describe each of our heuristics in order to show how they are important for managing the tradeoffs.

A. Heuristics

Heuristics driven by the network topology and contact history analysis: Each node performs analysis of node's past interactions and consists of three locally evaluated components: a node's "betweenness" centrality[1,2,12], social "similarity"[1,2,12] and tie strength relationship[1,2,12] to the service (destination node). This is important because of two reasons: first, it allows AdaptAnon to be responsive to the changes in the network topology and mobility patterns; and second it allows the choice of the nodes in the anonymization overlay that support directional routing [12] to the service. For the purposes of this paper, AdaptAnon takes into consideration *SocialSimilarity* and *ServiceRecency*. *SocialSimilarity* refers to connectivity similarity between the Service and the source's neighbour. The similarity calculation, where *C(N)* and *C(S)* are the set of contacts held by node N and service S respectively, is given as follows:

$$SocialSimilarity(N,S) = |C(N) \cap C(S)| \qquad (1)$$

ServiceRecency is obtained by dividing the number of seconds of the node with the oldest contact with the Service by the number of seconds since the neighbour last saw the Service. The *ServiceRecency* indicator is based on how recently node N has encountered a Service and is calculated as length of time between node N last encountering Service S (denoted as *Recency(N,S)*) divided by the difference between the time node N has been on the network (T(N) and *Recency(N,S)*:

$$ServiceRecency(N,S) = \frac{Recency(N,S)}{T(N) - Recency(N,S)} \qquad (2)$$

Heuristics driven by interest and user profile analysis: We assume that each node has a dynamic set of L profile attributes where each of the attributes can include any of the following types of profiles: predetermined interest keywords and user demographic information, ad hoc and new interests in order to allow expansion of the existing interests, social networks and friends' lists. This metric is important because of two reasons: first it allows AdaptAnon to be responsive to the changes in the application and user preferences; and second it avoids extensive usage of the nodes that are not interested in certain services or content. Each node analyses the degree of interest and user similarity it shares with nodes that it meets based on the number of matched profile attributes (denoted as *LabelSimilarity*) versus the number of total attributes (L).

We use Jaccard's coefficient that takes into account not just similarity but also dissimilarity of the nodes' interests and is defined as the size of the intersection divided by the size of the union of the sample sets.

$$LabelSimilarity = \frac{|L(N) \cap L(M)|}{|L(N) \cup L(M)|} \qquad (3)$$

Combining social connectivity driven and profile driven metrics allows AdaptAnon to increase the length of the anonymization path (K) compared to using only one of these two metrics alone because it allows more options for the next hop anonymization node on the anonymization path. However, due to spatial and temporal locality of reference principles, this can result in predictable choices of the nodes in the anonymization layer and thus have negative impact on the anonymization quality.

In order to counterbalance the decidability of the previous two heuristics, we propose the third type of heuristics that is driven by the anonymization history analysis performed by every node and for every potential anonymizing node. This heuristics allows AdaptAnon to increase the diversity of the nodes in the K overlay in order to improve the utilisation of the overlay nodes. Our aim is to avoid overuse and underuse of some nodes in the anonymization layer. For example if the source frequently uses the same node(s) for anonymization, all the nodes become more predictable and more easily profiled (e.g. only 8 messages are sufficient to decide on who the source is [7] for a social mobility trace in St Andrews University Campus for 27 students over 79 days and thus the effectiveness of the overlay nodes' utilisation is significantly decreased). However, in cases when there are multiple sources that are repeatedly utilising the same overlay in such a way that a single source's usage forms a small fraction of the other sources' usage, the effectiveness of using the same nodes (or overlay) by the same source without being easily profiled is higher. Finally, even if one node alone uses the same node(s) repeatedly and in a predictable fashion, but uses them for different services in an unpredictable manner, such a quality of anonymization can also be high as it is less predictable and more difficult to profile.

In order to manage this dynamic tradeoff between these different dynamic anonymization criteria, when a node chooses the next hop node in the overlay, it has to address the following questions regarding the potential next hop anonymization node by introducing the following three heuristics:

Each node keeps track of how often a potential next hop has been on the anonymization path for any source node and for any service defined as *AnonCnt(N)*. The more popular the node is, the more desirable it is where other nodes are using it.

Each node keeps track of how often the potential next hop has been on the anonymization path for this origin defined as *OriginAnonymCnt(N)*. The more often it has been used by a particular source node, the less desirable it is for that node.

Each node keeps track of how often the potential next hop has been on the anonymization path for this service defined as *ServiceAnonymCount(S, N)*. The more often it has been used for a particular service, the less desirable it is for that service.

Each node keeps track of the ratio of the number of times the next hop has been used by the given origin and by all other sources in order to be able to make less greedy decisions. The lower this ratio is, the more desirable this next hop is as a particular source node is less predictable. This is defined as *NodeRatio* in heuristic 4:

$$NodeRatio\ (N) = \frac{NodeAnonRqst(N)}{\sum_{i \in N} NodeAnonRqst(i)} \qquad (4)$$

Where N represents the set of all nodes that has requested anonymization through this node. Each node keeps the ratio of the number of times the next hop has been on the anonymization path for the particular Service and has been used for all other services. This is important in order to make less greedy decisions. The lower this ratio is, the more desirable this next hop is as the given source node is less likely to be profiled. This is defined as *ServiceRatio* in heuristic 5:

$$ServiceRatio\ (S) = \frac{ServiceAnonRqst(S)}{\sum_{j \in S} ServiceAnonRqst(j)} \qquad (5)$$

Where S represents the set of all services for which the node has provided anonymization. Each node keep track of the ratio of the number of times the next hop has been used to anonymize this source for this service, and the number of times it has anonymized other nodes for this service. This is defined as *ServiceNodeRatio* in heuristic 6:

$$ServiceNodeRatio\ (N,S) = \frac{|NodeAnonRqst(N) \cap ServiceAnonRqst(S)|}{|ServiceAnonRqst(S)|} \qquad (6)$$

Each node monitors *AnonCnt*, *OriginAnonymCnt* and *ServiceAnonymCount*, and then performs statistical analysis described in heuristics 4, 5 and 6 in order to allow for adaptive reuse of anonymization nodes that keeps balance between reusing the same nodes and using nodes that already have experience in providing anonymization.

Note that in this paper we assume equal weights between heuristics but it is also possible to use different weighing models in order to prioritise some criteria over the others if that is suitable. For example, for highly social traces it would be desirable to assign lower weight to social heuristics as to minimise the repeatability of path choices. Similarly, for non-social traces social weighting might be increased. If there are only few nodes that share similar profiles, the weights of the labels heuristics should be decreased to avoid easy node identification. When the trace is highly predictable either due to the percentage of label similarity of nodes or strong social connectivities, adaptive history anonymization heuristics should be weighted the highest because of its intelligent diversification factor that ensures neither overutilization nor underutilisation of anonymization nodes.

B. *AdaptAnon pseudo code*

We now describe our AdaptAnon pseudo code in more detail (Figure 1).

```
Query query = null;
List Contacts = null;
If (Node.isOriginatingNode) Then:
  query = new Query();
Else
Query = recvQuery();
Query.AnonymizationHops++;
End If
Contacts = ScanNeighobourhood();
For Each Contact in Contacts Do:
  If (Contact.hasAnonymized(Query) Then
    Next;
  End If
  If (Contact.isService) Then
    If (query.Anonymization Hops <requiredAnonymization Hops)
    Then
        Next;
    End If
    Node.sendQuery(Contact);
    Break;
  End If
  Contact.LabelSimilarity = calculateLabelSimilarity();
  Contact.SocialSimilarity = calculateSocialSimilarity();
  Contact.ServiceRecency = Contact.timeHasSeenService();
  Contact.NodeRatio =
  Contact.cntAnon(query.Node)/Contact.cntAnon(query.Total);
  Contact.Service Ratio =
  Contact.cntAnon(query.Service)/Contact.cntAnon(query.Total);
  Contact.ServiceNodeRatio
  =Intersection(Contact.countAnon(query.Node),
    Contact.countAnon(query.Service)) /
    Contact.countAnonymization(query.Service);
  Contact.AdaptAnonUtility = α*Contact.SocialSimilarity +
    β*Contact.ServiceRecency + γ*Contact.ServiceNodeRatio+
    δ*Contact.LabelSimilarity;
  If (Contact.AdaptAnonUtility > Contacts[0]) Then
    Contacts.swap(Contacts,Contact[0], Contact);
  End If
End For
Node.sendQuery(Contacts[0]);
```

Figure 1 *AdaptAnon* pseudo code

Each node scans the neighbourhood, detects all nearby contacts and adds them to the list of current neighbours. If a node is not a source node of a query, it receives a query from a neighbouring node and increments the *AnonymizationHops* counter of the query for every node. Each node performs the following actions for each member of the list of neighbours: If the neighbour has already anonymized this query, then the neighbour should not be used so it gets skipped (step 1). If the neighbour is the location based service itself then the node checks if the query has been forwarded by sufficiently many nodes already, i.e. if its *AnonymizationHops* is higher than *requiredAnonymizationHop.s* If so, the query gets sent to the service, otherwise the node skips the neighbour (step 2) . The node monitors and calculates the three types of heuristics described in section 3.1 (step 3). The node then calculates the total anonymization utility based on the operation mode: For **Label** mode only *LabelSimilarity* is used for calculating the total utility. For **Social** mode the social utilities are used for calculating the total utility: *SocialSimilarity* and *ServiceRecency*. For **Mixed** mode the Label and Social utilities are both used for calculating the Total utility. For **AdaptAnon** mode mixed mode is extended with Anonymity heuristics and statistics. The node with the best total utility (the sum of all heuristics) is chosen and the query gets sent to it for anonymization. In the above code, we assume that heuristics are all equally weighted. More in depth analyses of different weighting heuristics is out of the scope of this paper.

To return the answer to the query, the service responds to the last node in the anonymization path, that node is aware of the source identity and uses label and social heuristics for routing the query back to the source without diversification.

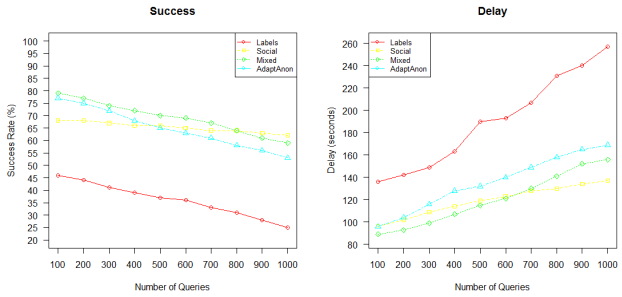
IV. EXPERIMENT SET-UP AND EVALUATION

This section describes a range of experiments that show AdaptAnon performance results over a real connectivity trace with varying underlying connectivity and query patterns across a range of metrics. Our metrics includes success ratio and latency of anonymized answered queries, anonymization path length and diversity factor of the nodes on the anonymization path. We use realistic social connectivity trace Infocom 2006 [20] and compare AdaptAnon to three other comparative algorithms: social connectivity only, label and mixed.

We perform analysis of the nodes' encounter rates, i.e., rates at which nodes come into contact with each other, and determine the median contact times via the notion of the angular node flux. Then we consider a number of scenarios where we select, first senders, and then services that have varying degrees of connectivity. We first explore the influence of varying load patterns on the four chosen metrics.

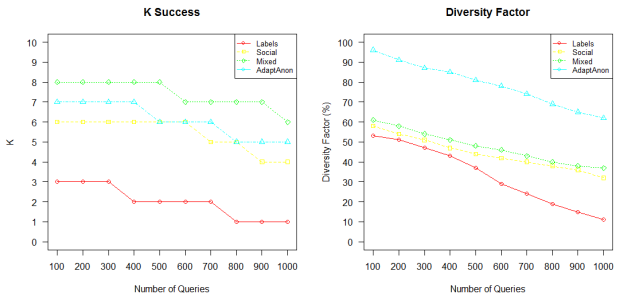
A. *Increasing the number of queries:*

With increasing number of queries and requests for anonymization, the number of nodes that anonymize other nodes rises and also the number of times that certain nodes anonymize queries for the same service increases in comparison to the total number of anonymization requests.



(a) (b)

Figure 2. Query success ratio and delay with increasing query rate



(a) (b)

Figure 3. Anonymization path length and diversity with increasing query rate

This in turn can damage the actual quality of anonymization as

the same nodes can be used repeatedly as described in Section III.

Figures 2 and 3 compare performance of AdaptAnon with mixed approach (combined social connectivity and label approach without randomisation), social connectivity and label/profile approaches for the increasing number of queries in terms of success ratio of answered queries, latency and number of nodes in the anonymization overlay (level of anonymity).

Figure 2a shows that AdaptAnon does not decrease success ratios of answered queries compared to Social and Mixed approaches but has about 60% higher success rates compared to the profile-based only approach. This is due to utilising multiple criteria for both routing and answering back the queries and thus utilising its better network knowledge. Figure 2b shows that AdaptAnon gracefully increases latency when compared to the social and mixed approaches. This is expected as AdaptAnon does not use the most direct path to the Service but includes label matching that allows better diversity of the nodes in the overlay. AdaptAnon is marginally slower than mixed approach because it includes randomisation factor that can delay the selection process for the next hop nodes. It is interesting to see that AdaptAnon manages 80% lower latency compared to the label approach. Figure 3a shows that AdaptAnon has 15% higher length of the anonymization path than the Social approach, and more than two times higher than for the Label approach. It is expected that the social approach performs significantly better than the Label approach as the trace we are using is a social trace and the label approach is not adaptive. Our mixed approach maintains highest anonymity levels because it is more flexible approach to K-anonymity that chooses the nodes according to one dimension and allows for a higher degree of optimization, and does not include diversification factor as AdaptAnon does. Figure 3b shows that AdaptAnon achieves more than two times better quality of diversity (higher diversity) than Social approach and more than three times higher diversity than Label only approach across all number of queries as it is the only one that monitors and intelligently to diversifies the previous node choices for the paths.

B. *Sender connectivity*

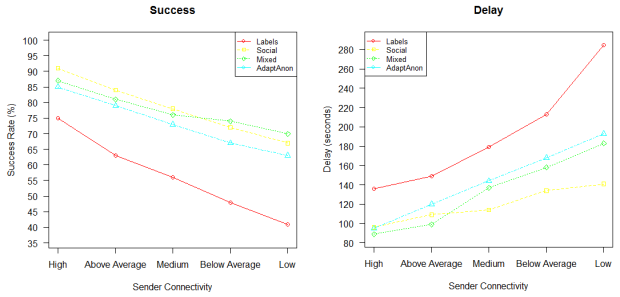
To investigate how the connectivity of the senders influences success ratios of answered queries, delays and the level of anonymity quality of anonymity and delay, we perform a number of experiments for five different categories of senders ranging from highly connected to low connectivity. For all the nodes in the Infocom connectivity trace we analyze each node's connectivity patterns (inter-contact times) and we classify the nodes into mean connectivity, 25% up and down of the mean, and top and bottom 25%. We then choose 10% of the nodes from each connectivity category to be senders. We randomly choose ten receivers that have above the average connectivity (in terms of node inter-contact times) so that they do not influence the results.

Figure 4a shows that better connected sender typically achieves higher success ratios of their answered queries for all four approaches to anonymization. AdapAnon does not lower the success ratio compared to the Social and Mixed approaches, and is 60% higher than the label approach. In terms of latency, Figure 4b shows that AdaptAnon is only 20% slower than the Social approach (which aims the most direct route to the service) and only 10% lower than mixed approach (that does not include diversification factor) while it is 90% faster than the label approach for all senders connectivity levels.

Figure 5a shows that AdaptAnon achieves higher number of nodes in the overlay than social and label approaches, but is particularly better for the medium senders' connectivity. AdaptAnon shows about marginally lower (5%) level of anonymity than the mixed approach. This is because AdaptAnon uses multiple criteria of choosing the K nodes and utilises better knowledge of the network and user profiles. Figure 5b shows that AdaptAnon achieves more than 80% better quality of diversity (higher diversity factor) than Social approach and more than three times higher diversity than Label only approach across all levels of sender connectivity. This is because it is the only one that intelligently diversifies the previous anonymization node choices.

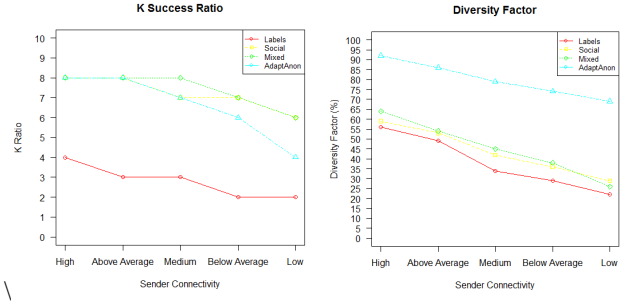
C. *Service connectivity*

To investigate how the connectivity of receivers influences the success ratios of answered queries, level of anonymity and



(a) (b)

Figure 4. Success ratio and delay with decreasing senders connectivity

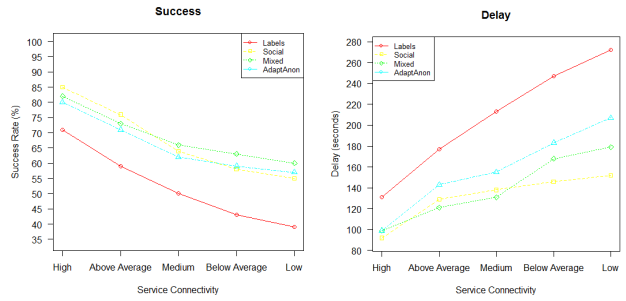


(a) (b)

Figure 5. Anonymization path length and diversity factor with varying sender connectivity

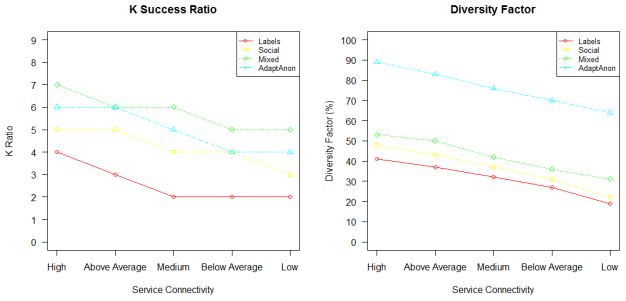
delays, we perform a number of experiments for five different categories of receivers ranging from highly connected to low connectivity. For these experiments, we randomly choose above average connected senders so that they do not influence the results. Figures 6 and 7 show similar results as with the increasing connectivity of the senders. AdaptAnon does not decrease success ratios compared to mixed, label and social approaches while it marginally increased delays.

Figure 7b shows that AdaptAnon achieves more than 90% better quality of diversity (higher diversity) than Social approach and more than two times higher diversity than Label only approach across all service connectivities.



(a) (b)

Figure 6. Success ratio and delay with varying service connectivity

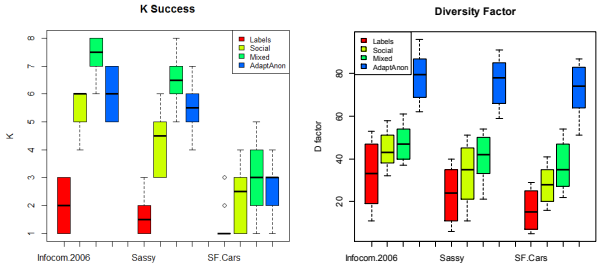


(a) (b)

Figure 7. Anonymization path length and diversity factor with varying service connectivity

Figure 8 compares quality of anonymization and diversification across three real traces Infocom2006[20].

Sassy[8], SF Cabs[11]. We observe that AdaptAnon achieves twice as good diversity factor compared to the Label,



(a) (b)

Figure 8. K and D factors

Social and mixed approaches while maintaining comparable levels of K – 3 times higher that Label, 20% higher than Social and 20% lower that the mixed approach.

V. CONCLUSIONS

This paper has two contributions: First, AdaptAnon achieves higher K (number of nodes in the overlay) compared to non-adaptive K-anonymity approaches over a wide range of query and connectivity patterns while keeping similar success ratios and delays to traditional approaches that use social connectivity only [1,2,4,12] or label only approaches[7,19]. Second, AdaptAnon achieves higher diversity of the nodes in the anonymization overlay compared to other single dimensional approaches due to our multidimensional criteria for a range of Ks than label-only and social connectivity -only approaches. We show that AdaptAnon achieves better utilisation of nodes and higher quality of anonymization even for low Ks (when K is equal to 2 and 3) that are the most realistic achievable Ks for realistic connectivity traces. Our results show what the critical connectivity of sender and services should be in order to allow different qualities of anonymization as well as what level of services (in terms of success ratios and delays of answered queries) can be expected for these anonymization levels. Our result can inform the decision of the number of placement of servers that allow different levels of anonymity while providing good services. For our future work, we plan to investigate the performance of AdaptAnon over heterogeneous realistic connectivity traces and the suitability of different models of weightings between the heuristics.

VI. REFERENCES

[1] M Radenkovic, A Grundy, "Congestion Aware Data Dissemination in Social Opportunistic Networks", in ACM SIGMOBILE Mobile Computing and Communications, Volume 14, Issue 3, July 2010

[2] M Radenkovic, A Grundy, "Framework for Utility Driven Congestion Control in Delay Tolerant Opportunistic Networks", In the Proc of IEEE IWCMC 2011

[3] E Bulut, B K Szymanski, "Exploiting Friendship Relations for Efficient Routing in Mobile Social Networks", IEEE Transactions on Parallel and Distributed Systems, 2012

[4] E Bulut, B K. Szymanski: Friendship Based Routing in Delay Tolerant Mobile Social Networks. GLOBECOM 2010: 1-5

[5] A Tran, N Hopper, and Y Kim. Hashing it out in public: common failure modes of DHT-based anonymity schemes. In Proc. OfWPES '09. ACM, NY, USAQ. Wang, N. Borisov: Octopus: A Secure and Anonymous DHT Lookup CoRR abs/1203.2668: (2012)

[6] I. Parris, T. Henderson: Privacy-enhanced social-network routing. Computer Communications 35(1): 62-74 (2012)

[7] G. Bigwood, D. Rehunathan, M. Bateman, et al, CRAWDAD data set st_andrews/sassy (v. 2011-06-03)

[8] Cory Cornelius, et al. 2008. Anonysense: privacy-aware people-centric sensing. In Proc. TheMobiSys. ACM, 211-224.

[9] J Manweiler, R,Scudellari, and Landon P. Cox. 2009. SMILE: encounter-based trust for mobile social services. In Proc. ACM CCS '09. ACM, New York, NY

[10] M. Piorkowski, N. Sarafijanovic-Djukic, M. Grossglauser,CRAWDAD data set epfl/mobility (v. 2009-02-24)

[11] E. Daly and M. Haahr, "Social network analysisfor information flow in disconnected Delay-Tolerant MANETs," IEEE Trans. Mob. Comp, 2009

[12] R. DingledineN. Mathewson, P. Syverson, "Tor: The Second-Generation Onion Router". Proc. 13th USENIX Security Symposium. San Diego, California.

[13] M. Freedman and R. Morris. 2002. Tarzan: a peer-to-peer anonymizing network layer. In Proc of the 9th ACM conference on Computer and communications security (CCS '02), Vijay Atluri (Ed.). ACM, 193-206.

[14] D. Goldschlag, M. Reed, and P. Syverson. 1999. Onion routing. Commun. ACM 42, 2 (February 1999), 39-41.

[15] G. Zyba, G. M. Voelker, S. Ioannidis, C. Diot: Dissemination in opportunistic mobile ad-hoc networks: The power of the crowd. INFOCOM 2011: 1179-1187

[16] A Mtibaa, M May, C Diot, and MAmmar. 2010. Peoplerank: social opportunistic forwarding. In Proc. IEEE INFOCOM'10. USA, 111-115.

[17] D Quercia, I Leontiadis, L McNamara, et al, 2011. SpotME If You Can: Randomized Responses for Location Obfuscation on Mobile Phones. In Proceedings of the IEEE ICDCS '11, Washington, DC, USA, 363-372.

[18] S Zakhary, M Radenkovic, "Utilizing Social Links for Location Privacy In Opportunistic Delay-Tolerant Networks", In the Proc ICC 2012, Ottawa, Canada

[19] J S R Gass and J Crowcroft,P. Hui, et al, "CRAWDAD" dataset cambridge/haggle (v. 2009-05-29)

[20] H Haddadi, R Mortier, S Hand, et al: "Privacy Analytics". ACM SIGCOMM Computer Communication Review, Apr 2012

[21] D McAuley, R. Mortier, J. Gouldling,"The Dataware manifesto", COMCNETS 2011, pp 1-6

[22] A. J. Khan, V. Subbaraju, Archan Misra, S. Seshan, " Mitigating the true cost of advertisement supported "free" mobile applications", HotMobile 2012

[23] M Radenkovic,, I Vaghi, Adaptive User Anonymity for Mobile Opportunistic Networks, , ACM MobiCom CHANTS 2012.