Secure Content Centric Mobile Network

Mooi Choo Chuah
CSE Department
Lehigh University
Bethlehem, PA 18015, USA
chuah@cse.lehigh.edu

Xiong Xiong
CSE Department
Lehigh University
Bethlehem, PA 18015, USA
xix209@lehigh.edu

***Abstract*—**Rapid advancements of wireless technologies allow users to access real-time data, and stay connected with friends and business while they are on the move. However, most emerging mobile applications assume users have cellular data services, and hence not everyone can enjoy new mobile applications. In addition, some emerging mobile applications e.g. mobile recommender system are data-centric but existing IP oriented communication paradigms are not flexible enough to support such applications. In this paper, we present a new secure content centric mobile network that supports content centric communication paradigm. Users can exchange information using peer to peer mode without having to rely on cellular data services. Content-centric security solution is provided where data owners can share encrypted published data items with others without knowing a priori who the interested users may be. Our preliminary prototype deployed in the ORBIT testbed demonstrates some of the key features we have designed.

Keywords- future internet, content centric, security, intentional name message delivery

I. INTRODUCTION

Search engines such as Yahoo or Google allow us to locate useful information amidst the large volume of data found in the Internet. In addition, online users from vastly distributed geographical areas enjoy interacting with one another in cyberspace, and stay connected via many popular social networking sites such as Facebook [1], Linkedin[2], and MySpace [3]. Through these sites, the users share personal journals, photographs, videos, and make social connections. The rapid advancement of the wireless technologies provides new opportunities for mobile users to have similar easy access to the real-time data, derive useful social information, and stay connected with business partners, colleagues and friends. Towards this end, mobile social networking applications have recently emerged to meet these needs [4-6]. Several interesting mobile social network projects are also described in [8-10]. In addition, the concept of participatory sensing [11-12] has been introduced where people participate in sensing and analyzing aspects of their lives via the use of sensors (e.g. cameras, motion sensors and GPS) built into their mobile phones. Participatory sensing [12] emphasizes the involvement of regular people and community groups in the process of sensing and documenting where they live, work and play.

Emerging mobile applications as described above are attractive. However, their adoptions by mobile users sometimes face certain hurdles. For example, many mobile applications assume that the users have cellular data services, making them un-accessible to mobile users without such services. Furthermore, emerging mobile applications are also data centric but current mobile Internet communication paradigms are not flexible enough to support new content centric features e.g. allowing messages to be sent to some mobile users with certain attributes. In addition, intermittent connectivity often occurs in mobile scenarios but current networking technology does not work well in such environments.

Current mobile applications e.g. social networking related applications, accessed either via Internet or mobile phones, also raise security and privacy concerns. For instance, studies in [13] show that Facebook's application platform sends far more personal information than is necessary to the plug-ins' developers. Thus, an identity thief can develop an application to grab personal information from Facebook. Although, privacy settings can be provided to allow users control over who can browse through their contents [14], users' sensitive data can still be exposed if the server is compromised since the data is stored as clear texts. We note that traditional security solutions [15-17] that require constant access to an Authentication Authorization Accounting server (AAA) server or certificate authorities do not apply in intermittently connected network environments. Thus, effective security solutions that can work in intermittently connected network environments do not exist. We argue that a data centric solution is desirable for future mobile applications since it allows data owners to have full control over who can view their published data.

In summary, future mobile content distribution systems should support a few key features: (i) efficient peer to peer communications, (ii) disruption tolerant networking, (iii) efficient content and user interests' advertisements, and (iv) data-centric security. Peer to peer mode allows close-by users to exchange interesting information without having to rely on cellular data services. Since human contact based networks often have intermittent connectivity because people move around and may turn on/off their wireless devices, disruption tolerant networking (DTN) features [18,19] need to be supported. The intentional naming feature in DTN allows users to send messages based on attributes and not just based on fixed end point identifiers like IP addresses. Furthermore, to support emerging mobile applications, efficient content centric advertisements and search mechanisms need to be designed such that mobile users can quickly find contents (plaintext or encrypted) that they are interested in. Data centric

security allows publishers to control who can access their published data items without knowing apriori who interested users are.

To support efficient and secure real-time mobile content distribution systems, in this paper, we present our vision of next generation secure content centric mobile network(SECON)s that support the following features:

- ***Intentional-named Message Delivery without apriori knowledge of recipients:*** Users can send intentional-named messages, i.e. senders need not know apriori who the recipients are, e.g. sending a ride-sharing query to all users that are located close-by.
- ***Efficient Content Advertisement and Access:*** A user can push his published contents to wireless storage nodes which in turn advertise contents to other users. A user can search storage nodes for contents of interest to him using keywords. A user can also decide if he wants to cache the data items obtained from storage nodes for others to access.
- ***Achieving data confidentiality and privacy-preserving:*** Users can publish information at untrusted wireless storage servers (e.g. those that are deployed in rural areas or shopping malls), control the access of their published encrypted data items which are stored at wireless storage servers.

The rest of the paper is organized as follows: In Section II, we describe the SECON architecture and its unique features. Then, we describe the three major types of messages supported in SECON and how they are used to support the new SECON features. In Section III, we describe how users send and receive intentional named messages. In Section IV, we discuss related work. We conclude in Section V with some discussions on the near future work that we intend to conduct.

II. INNOVATIVE FEATURES IN SECON

A. *Overview of SECON Architecture*

Fig. 1 depicts our SECON architecture. Two new network entities are introduced: content router(CR)s and content resolution server(CRS)s. Content routers support content caching, intentional name resolution & forwarding, and content-centric networking. By content-centric networking, we mean aggregation and advertisement of the meta-data descriptions of cached contents, and forwarding of users' content interest packets. In addition to these functions, Content Resolution Servers further support some additional features: translations of meta-data descriptions from different data schemas, and additional intentional name resolutions that cannot be performed by content routers such as mapping of some geographically based intentional names into a list of endpoint identifiers e.g. a list of hotels within 500m of Hotel Westin Ottawa. Different domains, e.g. P-Lab, ORBIT, in Fig 1 can decide if they want to deploy content resolution servers (CRS) in their domains. Each domain may have flat or hierarchically organized CRSes e.g. a two-level system with a top-level CRS and multiple CRSes in the second tier.

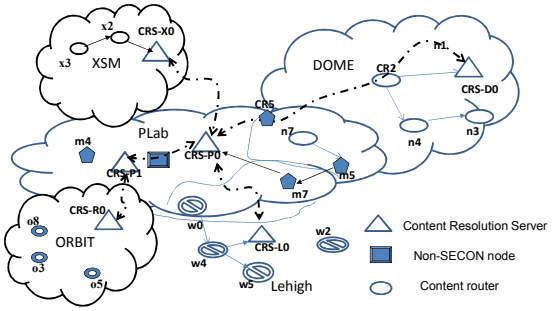


Fig 1: SECON Architecture

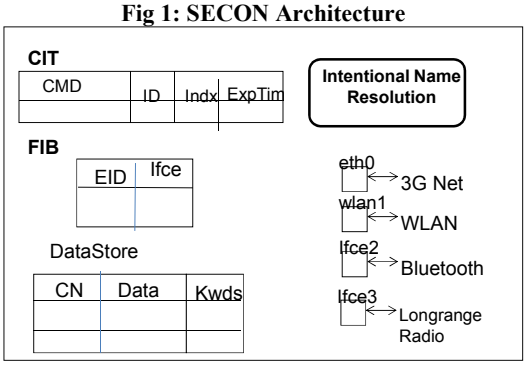


Fig 2: Content Centric Mobile Router

Fig 2 shows the key components of a content-centric mobile router (CCMR). Such routers can be deployed by wireless service provider(WSP)s or they can also be powerful mobile devices carried by users . A router may have multiple network interfaces e.g. 3G, WLAN, long range radio or Bluetooth. In order to be energy efficient, a router can be configured such that information discovery can be done via 3G interface but content transfer is done via the WLAN interface whenever WiFi is available. Cached Interest Table (CIT) contains all the users' interest advertisement packets that have not expired. The forwarding information block (FIB) contains forwarding entries for different content-centric identifiers. All published data items will be stored in the data store. Since the nodes may often be disconnected, all nodes support disruption tolerant networking (DTN) [18,19]. We assume typical DTN forwarding schemes such as RAPID [20], Prophet [21], geographical forwarding scheme [22] are supported by CCMRs. The intentional name resolver supports progressive resolution of intentional names.

In SECON, mobile devices can be in either peer-to-peer (P2P) mode or infrastructure mode. When set in P2P mode, users' mobile devices periodically send out beacons such that they can discover one another. The beacons broadcast by a device contain its end-point identifier (in the form of a URI e.g. secon://msnbc.ca.com) and its capability e.g. whether it is a storage node or a content resolution server. Note that any SECON node can be a storage node. Upon discovering beacons from a nearby server running SECON services, a user can flip his device from the P2P mode to the infrastructure

mode so as to utilize additional services, e.g. data schema translation, provided by the SECON server.

Next, we describe three major types of messages that are exchanged between SECON nodes, and what these messages are used for.

B. Content Publish Announcements

Any data owner who wishes to publish contents sends a content publish announcement (CPA) message before it starts sending content data (CD) messages. The publish announcement message format and an example are as shown in Figs 3(a) &3(b). The publish announcement contains the publisher name (expressed as a URI), meta-data descriptors of its published contents e.g. politics, weathers, finance. The destination field contains information about where the publisher intends its contents to be stored at e.g. the two content resolution servers of wireless service provider WSP1 (denoted as CRS11 and CRS12 of WSP1 in Fig 3(b)). Since we support intentional name resolution, a publisher can specify "role:"CRS", location(LocA, 100)) if he wants every CRS within that target region to store its contents. The publish announcement message is signed for security reason, and a nonce is provided to prevent replay attacks.

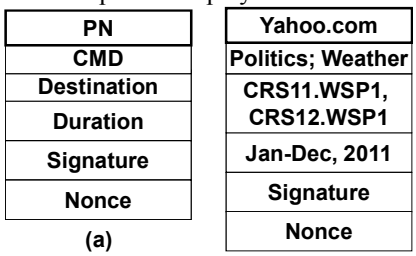


Fig 3:Publish Announcement Message

When intermediate nodes receive such content publish announcement messages, they create new or update existing entries in their forwarding information block (FIB). Then, they forward these CPA messages to the destinations specified in the messages using the underlying routing protocols. Note that one can map the destinations listed in a publish announcement message to an IP multicast address. Any content resolution server that subscribes to this multicast address will check the destination field to see if it is one of the intended recipients.

C. Content Data (CD) Packets

When a node wishes to publish new data items, it sends content data packets. A publisher can specify storage nodes that need to store its published data items by using unique destination identifiers or intentional named destinations e.g. all storage servers within 100m of Location A. For security reason, intermediate nodes can refuse to accept any CD packets if a publisher has not previously sent any CPA message regarding its intention to publish certain categories of data items. Furthermore, each intermediate node or CRS can set a rate limit for accepting content data packets to prevent possible DDoS attacks from malicious publishers.

The content data packet format and an example are shown in Fig 4. Each data item is described by some meta-data descriptors (CMDs) e.g. weather, sport, entertainment, movie and a URI-like content identifier. The meta-data descriptors can be used for matching with cached user expressed interests (to be described in Section II.D). The publisher identifier may be included in the signed information field. The data content can be in plaintext or encrypted. We will discuss further the security topic in Section II.F. Each data item can be described by a unique content identifier (CID) based on some published schemas. For example, a movie review article can be described as "yahoo/movie/review/art12345". Each data content packet is signed and a nonce is included to prevent replay attacks.

The insertion of a new data item into the data store of a SECON node will trigger that node to check if a new data item matches any entries in the cached user interest table so that this node knows if it should alert those nodes that have expressed interests in such data items. To prevent frequent notification, content data packets can be cached and sent as an aggregated packet after a sufficient number of packets have been accumulated. Alternatively, a user can set a flag in the user interest packet to prevent storage nodes from pushing new contents. Instead, the storage node only periodically sends that node a matched content list (MCL) using the CPA packet format, and the user can choose which items among the list he will retrieve. We provide an example of how this is done in Section II.D.

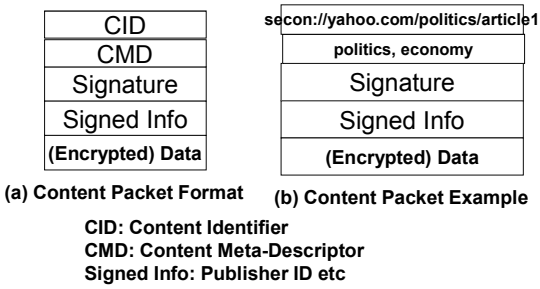


Fig 4: Content Data Packets

D. User Interests Advertisements

A user can express his/her interests for certain types of contents by sending a user interest advertisement (UIA) message from his/her mobile device. The UIA packet format and an example are shown in Fig 5. The content meta data descriptors include keywords of data items that are of interest to this particular user e.g. movie, weather, sports, music etc. The Selector field contains several sub-fields: (a) the identifier of the schema used for the meta data descriptions e.g. Yahoo or MSN, (b) any treatment preference for the specified keywords in the meta-data descriptors e.g. highest preference first, conjunctions etc, (c) specific publishers that are of interest to this user, (d) the scope of the advertisements i.e. how many hops a user wishes his/her interests to be

forwarded by others. The scope can also be expressed as a target region e.g. (LocA, 100m) means that this UIA packet should be disseminated within 100m of Location A. When a node receives such a UIA packet, it will forward using geographical forwarding until this message reaches a node inside the target region. Then, this message is flooded within that target region. A user's interest may change from time to time or from one location to another. Thus, each interest packet has a lifetime so that any expired interest entries can be purged from the cached interest table (CIT) of a node. A nonce is also included for security reasons.

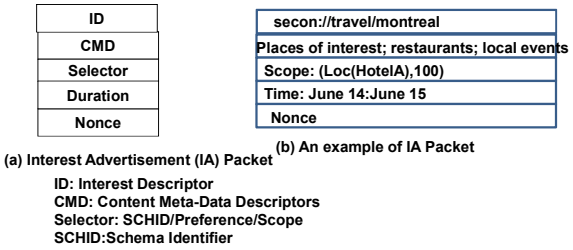


Fig 5:User Interest Advertisement (UIA) Packet

When an intermediate SECON node, let say Node A, receives a UIA packet, it will search through its data store to see if it carries any data items of interest to this newly encountered node. Matching can be done via longest prefix match lookup in the data store or based on keywords. If there are interested data items, then the node will send a matched content list (MCL) to that node. This list contains the top 5 or 10 matched data items based on the prefix-matched of URI-like content names or keyword matching from users' interest packets. A user can decide whether it wants to retrieve all or some of these data items.

If Node A does not have any data items of interest to this newly encountered node, then Node A will discard the UIA packet if its lifetime is 0. Otherwise, it inserts this UIA packet into its cached interest table (CIT) if its lifetime exceeds 0, and/or its scope limit has not yet been exceeded. If a node decides to cache other nodes' UIA packets, then it will combine all the interests (including its own) in the UIA packet it advertises to other nodes.

An example of when an UIA packet is sent and how it is processed is described as follows: a professor may visit Montreal to attend a technical conference. She may have a half-day break when she can tour the city. She can send a UIA packet to find useful information that can help her plan where she can visit and have food. An example of her UIA packet is shown in Fig 5(b). She indicates that she is interested in places of interest and local events at Montreal for a particular time interval. She may not know where to send this UIA packet to. Thus, she utilizes the intentional name provided in SECON. The destination of her UIA packet is set to an intentional name:secon:intent//travel/Montreal/role='CRS', Loc(HotelA,100m). This packet will be sent by intermediate SECON nodes towards a top-level CRS in Montreal that takes care of the travel category. The top-level CRS caches this UIA packet, and then disseminates this packet to all content resolution servers that are located within 100m of that Montreal hotel. The CRSes in that target region each generates a content response. This top-level CRS then consolidates all responses and sends an aggregated response to that professor. In Fig 6, we show how the UIA and the CPA messages are exchanged between the various nodes. The device from Professor A sends the UIA packet as shown. This packet is forwarded using geographical forwarding until it reaches CRS-M which is in Montreal. CRS-M disseminates this UIA to CRS-11 and CRS-12 that are within the target region. CRS-11 and CRS-12 each responds with its own CPA message. CRS-M aggregates this message and sends a merged CPA message to Professor A. Professor A can then send a new UIA message that specifically asks for the data item related to event1. Note that to minimize the round trip retrieval time, an additional field can be provided in the UIA message to retrieve all contents if the total matched items are less than K such that the professor needs not send another UIA message to retrieve a specific item.

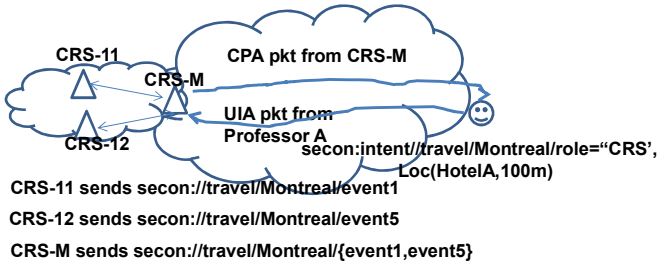


Fig 6: Illustration of how UIA and CPA messages are used.

E. Publishing Secured Data Items

Since some publishers may only allow certain people to access their data items, they have to encrypt these data items such that only authorized personnel can access them. We propose using cipher-text attribute-based encryption approach [24-25] to provide such a security feature. Each publisher creates unique attributes for different categories of data items they publish e.g. appliances, clothing, sport-equipment, lawn care etc. Data items that belong to more than one category, e.g. lawn mower belongs to both "lawn care" and "appliances" categories, will be encrypted such that any user who is interested in either "appliances" or "lawn care" will be able to retrieve such data items from the storage nodes. Details of our enhanced CP-ABE design which includes new features such as supporting dynamic attributes, negative attributes and user revocation can be found in [26]. The dynamic attributes will be useful for region-based content distribution e.g. certain encrypted data items (e.g. store coupons) can only be accessed by subscribers that are currently in a certain geographical region. The current user revocation design is not as scalable as we desire, and hence we hope to enhance it using key delegation approach in the near future.

III. DISSEMINATING INTENTIONAL NAMING MESSAGES

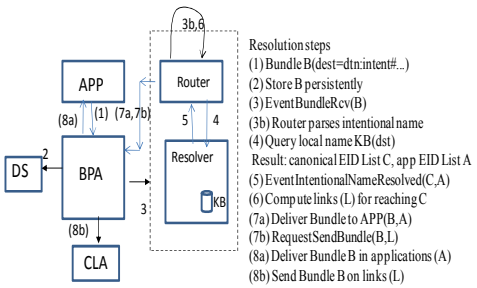
In this section, we describe how the content centric routers in SECON support the intentional named message delivery (INMD) feature where the destination of a message can be

described using node or user attributes e.g. roles, services or location or predicates of node attributes rather than using specific network identifiers. To support INMD, the routers need to support a late binding feature. With this late binding feature, the resolution of an intentional name to specific end point identifiers can be deferred until the message is routed to a node that is capable of completing the binding process. For example, assuming that a student is kidnapped by a stranger, and another student witnesses the event. The witnessed student can snap a photo of the incident, and quickly disseminate it to any police officers that are located within 500m of the scene. The student does not know who these officers are. He/she only clicks on a button that says "send an emergency message to the law enforcement personnel" on its mobile phone. Any nearby police officers equipped with mobile devices that run our software can receive such an emergency message. The intentional name message delivery with the late binding feature is very attractive for networks with intermittent connectivity.

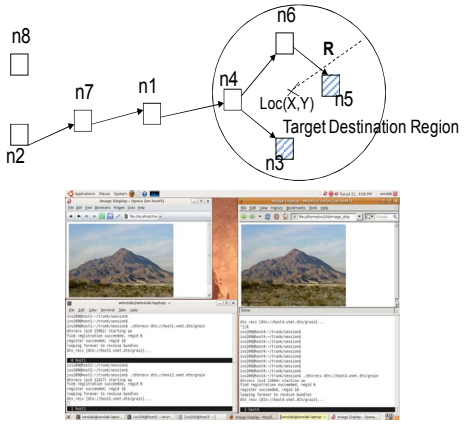
In Fig 7(a), we show the software architecture of an intentional name capable router we have developed [26]. An application that supports intentional name messages will prepare a data bundle, and pass it to the bundle processing agent (BPA) which triggers a bundle receive event. The bundle receiving event is captured by the external router module which queries the knowledge base within the resolver to progressively resolve the intentional name to some node identifiers that can be mapped to some existing neighboring nodes. The data bundle is then replicated and sent to all these identified nodes. Similarly, when an intentional named message is received, the convergence layer will pass it to the BPA which again triggers a bundle receive event. The router upon consulting the resolver will determine if this bundle is meant for the current node. If that is the case, the bundle will be delivered to the application. Otherwise, the resolver will provide a next-hop node for the router to forward to next.

In Fig 7(b), we show a testbed constructed at OBRIT [23] that we used to demonstrate this intentional name delivery feature. Assume that an encrypted data item is sent with an intentional name that says that all nodes inside the target destination region that have a node attribute that matches "track captain" can receive this message. The message was sent from node n2. The node n2 will forward the message to n7 using geographical forwarding [22]. Subsequently, node n7 will forward it to n1, and n1 will forward to n4. Once the message arrives at a node that is inside the target destination region, that node can use "flooding" to send the message to all nodes within its transmission range. Nodes n3 and n6 both hear the message but only node n3 has the right attribute to decrypt the message. Node n6 relays the message to node n5. Node n5 also has the right attribute to decrypt the message. Our prototype as described in [26] was initially built using DTN reference implementation version 2.6 [7]. This prototype supports the enhanced CP-ABE content-centric security feature described in [26]. Our enhanced CP-ABE features support negative attributes and user revocation. Our evaluation using an Intel Core TM 2 Quad 2.4 GHz workstation reveal that the key setup takes only 0.076 sec with 20 attributes, the encryption takes on the average 1.332 sec with 15 positive and 10 negative attributes. The decryption time is on the average 1.98 sec.

Right now, we are re-implementing this intentional name delivery feature using a lighter weight implementation. Our current prototype only supports basic SECON features e.g. it interprets UIA message but does not perform UIA aggregation yet.



(a) Intentional Name Capable Router



(b) Current Prototype

***Fig 7: Intentional Name* Message Forwarding**

More details of the SECON design such as how to minimize redundant data replications, and provide incentive for nodes to cooperate in peer to peer mode can be found in [30]. Preliminary performance evaluations of SECON compared to NDN can also be found in [30].

IV. RELATED WORK

Intentional Named Message Delivery/Content Centric Networking: In existing Internet, the mapping from a name to an address happens at the beginning of a communication session. However, in sparsely connected mobile networks, nodes and services can appear, move and disappear dynamically. Thus, recently disruption tolerant networking protocols [18,19] have been designed to enable communication services in sparsely connected environments. One of the key features in DTN is late binding. In a DTN, resolving a name may not be possible at the source. Thus, progressive resolution is carried out to route a bundle from the source to the destination. [22] is the first paper that describes

an implementation of a late-binding router. We have also developed a late binding router [26] in our DARPA funded project. In [27], the authors built and evaluated declarative policy-based routers that can adaptively select which MANET routing schemes they want to use. Declarative policy-based routers can be enhanced to provide intentional named message delivery. In [28], the authors propose a data-oriented network architecture (DONA) where DONA names are of the form (P:L) where P is the cryptographic hash of the principal's public key and L is a label chosen by the principal who ensures that these names are unique. The principal is the one that host the data item. The DANA network stores intelligence to let the intermediate nodes know where to locate a copy of the data item when a query is sent. Their approach assumes querying users know the exact labels of the data items which is not desirable. The closest to our SECON design is the idea presented in [29]. However, there are some significant differences: (a) in CCN, a publisher is allowed to publish data items only after prior interest packets have been received. However, in real life, there are situations where users express interests only after they are made aware of certain published data items e.g. new movies, (b) the authors in [29] assume users know unique content identifiers and include such information in their users' interest packets while we allow users to specify keywords in their users' interest packets, (c) SECON provides intentional named message delivery and content-centric security features.

V. Concluding Remarks

In this paper, we have described our new secure content-centric mobile network. Our new network supports several new features, namely secure intentional named message delivery, content announcements and retrievals. Our preliminary prototype that supports some basic SECON features is deployed using ORBIT testbed. Our near future work is to conduct a larger scale experiment for evaluating our content delivery feature using ORBIT. Then, we intend to deploy our prototype to DieselNet [20], a real-life vehicular adhoc network. Finally, we intend to design additional security features in SECON.

Acknowledgment

The authors wish to thank Bryan Herbst for his contribution in the earlier prototyping effort. This work was supported in part by US NSF under grant CNS-1049845.

References

[1] Facebook http://www.facebook.com

[2] LinkedIn http://www.linkedin.com/

[3] MySpace http://www.myspace.com/

[4] Dodgeball http://www.dodgeball.com

[5] M. Terry, E. D. Mynatt, K. Ryall, D. Leigh, "Social Net: Using patterns of physical proximity over time to infer shared interests", Proceedings of Human Factors in Computing Systems (CHI 2002) pp 816-817, 2002.

[6] Microsoft'sSLAM http://arstechnica.com/journals/microsoft.ars/2006/10/10/5573

[7] DTN2 Reference Implementation, http://dtnrg.org

[8] E. Miluzzo et al, "Sensing Meets Mobile Social Networks: The Design, Implementation and Evaluation of the CenceMe Application", Proceedings of ACM Sensys, Nov, 2008

[9] S. Gaonkar et al, "Microblog: Sharing and Querying Content Through Mobile Phones and Social Participation", Proceedings of ACM Mobisys, June, 2008.

[10] C. Borcea et al "The MobiSoc Middleware for Mobile Social Computing: Challenges, Deisgn, Early Experiences", Proceedings of ACM Mobiware, Feb 2008.

[11] J. Burke, D. Estrin et al, "Participatory sensing", Workshop in World-Sensor-Web, 2006.

[12] J. Goldman, et al, "Participatory Sensing: A citizen-powered approach to illuminating the patterns that shape our world", Woodrow Wilson Center for International Scholars Report, May 2009.

[13] J. R. Young, "Study raises new privacy concerns about Facebook", Chronicles of Higher Education, Feb 4, 2008 http://chronicle.com/free/2008/02/1489n.htm

[14] J. Hightower, S. Consolvo, A. LaMarca, I. Smith and J. Hughes, "Learning and recognizing the places we go". In Proceedings of the Seventh International Conference on Ubiquitous Computing (Ubicomp 2005), Lecture Notes in Computer Science, pages 159-176, Springer-Verlag

[15] B. Anton, B. Bullock, J. Short, "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming", Wi-Fi Alliance, Feb, 2003

[16] J. Leu et al, "Running Cellular/PWLAN services: practical considerations for Cellular/PWLAN architecture supporting interoperator roaming", IEEE Communications Magazine, Vol 44, No 2, July pp 73-84

[17] M. Shi et al, "A service agent based roaming architecture for WLAN/Cellular Integrated Networks", IEEE Transactions on Vehicular Technology, Vol 56, No 4, July, 2007 pp 3168-3181

[18] K. Fall, "A delay tolerant network architecture for challenged networks", Proceedings of ACM Sigcomm, 2003.

[19] V. Cerf et al, "Delay Tolerant Networking Architecture", RFC4838, April, 2007.

[20] A.Balasubramanian, B Levine, A. Venkataramani, "DTN Routing as a Resource Allocation Problem", Proceedings of ACM Sigcomm, Aug, 2007

[21] A. Lingren et al, "Probabilistic Routing in Intermittently Connected Networks", Proceedings of Workshop on Service Assurance with Partial and Intermittent Resources, Aug, 2004.

[22] B. Basu, R. Krishna, D.W. Brown, "Persistent Delivery With Deferred Binding to Descriptively Named Destinations", Proceedings of IEEE Milcom, Nov, 2008.

[23] ORBIT http://www.orbit-lab.org

[24] V. Goyal et al, "Attribute-Based Encryption for fine-grained access control of encrypted data", Proceedings of ACM CCS, pp 89-98, 2006

[25] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption", Proceedings of 28th IEEE Symposium on Security and Privacy, 2007

[26] M. Chuah, S. Roy, I. Stoev, "Secure Descriptive Message Dissemination in Disruption Tolerant Networks", Proceedings of ACM MobiOpp, Feb 2010.

[27] Changbin Liu et al, "Declarative Policy-based Adaptive MANET Routing", Proceedings of IEEE ICNP, Oct, 2009.

[28] T. Koponen et al, "A Data-Oriented (and Beyond) Network Architecture", Proceedings of ACM Sigcomm, 2007.

[29] V. Jacobson et al, "Networking Named Content", Proceedings of ACM CONEXT, Dec, 2009.

[30] M. Chuah, X. Xiong, "Secure Content Centric Publish/Subscribe System", Lehigh CSE Technical Report, Aug, 2011.