Dissemination of Anonymised Context Information by Extending the DCXP Framework

Stefan Forsström, Victor Kardeby, Jamie Walters, Roger Norling, and Theo Kanter

Department of Information Technology and Media
Mid Sweden University
SE-851 70 Sundsvall, Sweden
{stefan.forsstrom,victor.kardeby,jamie.walters,
roger.norling,theo.kanter}@miun.se

Abstract. The increasing ubiquity of context aware services and systems has been primarily underpinned by the use of centralised servers employing protocols that do no scale well for real time distribution and acquisition of neither sensor data nor dependent services. Any shift from this generic sensor framework mandated a new thinking where sensor data was capable of being propagated in real time using protocols and data models which serve to reduce unnecessary communication overhead. DCXP is proposed as an alternative architecture for the real time distribution of context information to ubiquitous mobile services. As a P2P based distributed protocol, it inherently poses the challenge of user anonymity across the system. In this paper we briefly present DCXP along with further work to enable the anonymised dissemination of sensor information within the architecture. Such a solution would have a negligible impact on the overall scalability and performance of DCXP.

1 Introduction

Previous systems exist that provide ubiquitous access to context information both centralised [1,2] and distributed[3,4,5]. Common among these systems is that they lack the options of providing anonymisation services to their users.

Anonymisation is the act of removing all information about the sender from a transmitted message such that the recipient or the system cannot ascertain the identity of the sender. Anonymisation has been long sought after in many different situations even before the existence of computers, such as anonymous charity, anonymous tips to law enforcement agencies or the press [6].

The need for anonymity has progressed onto the Internet with various attempts at addressing it. One of the earliest anonymisation methods is the Chaum Mix [7] named after its creator David Chaum. In P2P systems several Chaum mixes, or derivatives provide one or all of the anonymity services discussed in [8]: receiver anonymity, sender anonymity and receiver-sender unlinkability.

Several concurrent research into anonymous P2P exists; some utilise a central authority to distribute public/private key pairs [9,10] others provide optional

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 57–66, 2010.

encryption [11] or no encryption at all [12]. There exists some anonymity P2P systems that uses probabilistic random walks through the structured network [12] whereas other systems uses pre-calculated routes [10]. However none of these systems are niched toward real-time dissemination of context information within sensor networks. This paper presents an extension to the novel Distributed Context eXchange Protocol (DCXP) presented in [13], to enable anonymous dissemination of context information. The goal is to provide receiver anonymity, sender anonymity and receiver-sender unlinkability through the anonymisation grade "Probable Innocence" as described in [6].

A common problem with previous solutions towards achieving anonymity on P2P networks is the reliance on an increased network signalling overhead. This was necessary since solutions were being developed to address the issue in the much broader context. By gearing towards context dissemination; we are able to simplify the protocol. We employ a token ring based structure for intra-group communication which significantly reduces network traffic between groups permitting us to realise a more novel solution that maintains anonymity while ensuring real time exchange of context information.

As with the DCXP framework, this solution is targeted at a distributed platform for the dissemination and sharing of context information. Sensors are attached to more powerful computers as well as mobile phones which participate, either directly as an active node or indirectly through a proxy node, in a distributed P2P overlay.

Section 2 will present a brief overview of DCXP. Section 3 presents our proposal to extend DCXP to add anonymity to the dissemination of sensor information. Section 4 draws some conclusions and present future work.

2 Distributed Context eXchange Protocol

DCXP is an XML-based application level P2P protocol which offers reliable communication among nodes that have joined the P2P network. Any end-device on the Internet that is DCXP capable may register with the P2P network and share context information. The DCXP naming scheme uses Universal Context Identifiers (UCIs) to refer to Context Information (CI) such as sensors that are stored in the DCXP network.

2.1 Context Storage

A network that uses DCXP forms a Context Storage (CS) that utilises a Distributed Hash Table (DHT) to map between UCIs and source addresses. The current DHT design choice is Chord, presented in [14]. The logical positions of participating nodes are calculated by hashing their IP numbers and using this value as a key. In this way each node is responsible for the hashed keys which fall between itself and their numerically nearest predecessor in the key space, again in a circular fashion.

The advantage of using a DHT is that entries can be found in $\log(N)$ time. In addition, the CS also acts as a context exchange mechanism. Clients query

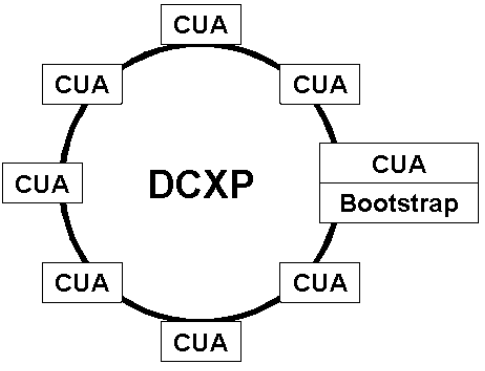

Fig. 1. DCXP architecture

the CS for an UCI to learn where the Context Information (CI) is located and the CS returns the address of the desired CI. The CS is able to resolve locations because it handles the resource registrations coming from the context sources. Thus, the CS maintains a repository of UCI/source-address pairs and provides a resolving service to the clients via DCXP. With the exception of storing CI, the operation of the CS is similar to the way that Dynamic DNS stores a mapping between a domain name and an IP address.

2.2 DCXP Topology

DCXP enables the exchange of context between sources and sinks. These sources and sinks, combined in a single end-point, is a Context User Agent (CUA). CUAs are allowed to join a context network by registering with a CS. A CUA corresponds to a node in the DHT ring that holds the CS. In particular, a CUA has a Application Programming Interface for applications and services to either resolve a UCI, get a UCI or register a UCI in the CS.

The ring in Fig. 1 symbolises the DCXP ring. Each box on the ring symbolises a node in the DCXP network, and each node has a CUA service. There can be any number of nodes in a single ring, or even a single node forming a ring with itself. The bootstrap node is the first node to be started on the DCXP network. It has to initialise and sustain the network, and each DCXP ring requires one bootstrap node.

2.3 DCXP Messages

DCXP is a SIMPLE-inspired protocol with five primitives, outlined in table 1. For more information on SIMPLE, see [15]. Fig. 2 provides an example of signaling for fetching a context value in the DCXP protocol. Each circle on the ring in the figure illustrates one Context User Agent (CUA) on the Context Storage (CS).

Table 1. The primitive messages of DCXP

REGISTER_UCI	A CUA uses REGISTER to register the UCI of a CI with the CS.
RESOLVE_UCI	In order to find where a CI is located, a CUA must send a RESOLVE to the CS.
GET	Once the CUA receives the resolved location from the CS, it GETs the CI from the resolved location.
SUBSCRIBE	SUBSCRIBE enables the CUA to start a subscription to a specified CI, only receiving new information when the CI is updated.
NOTIFY	The source CUA provides notification about the latest information to subscribing CUAs every time an update occurs or if asked for an immediate update with GET.

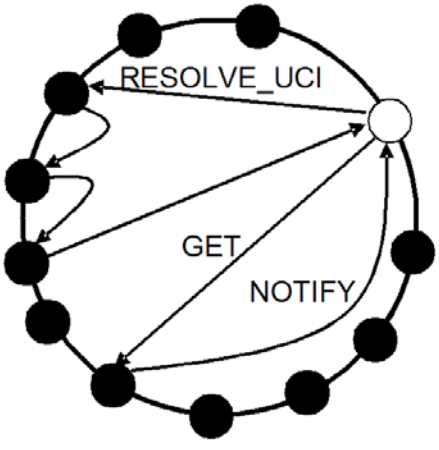

Fig. 2. DCXP signaling

2.4 Universal Context IDs

DCXP identifies each Context Information (CI) by a Universal Context Identifier (UCI) akin to a Uniform Resource Identifier (URI), as described in [16]. UCIs have the following syntax and interpretation:

```
dcxp://user@domain[/path]
```

where `dcxp` is the new URI scheme name and `domain` is a Fully Qualified Domain Name (FQDN) of the context domain. `user` provide means for ownership identification. `path` constitute a context namespace hierarchy, thus allowing for the organization and sorting of the items. An example of a fully qualified UCI would be:

```
dcxp://alice@miun.se/weather/temp
```

3 Enabling Anonymity in DCXP

In order to enable anonymous context exchange within DCXP; we propose a solution that employs a hybrid of two different anonymity approaches. Firstly, randomly selected users within the DCXP ring are grouped together communicating internally using a token ring based structure. Groups then communicate among each other in manner similar to Cashmere [9]. Since all information is sent and received as a group, individuals remain hidden inside the group. In doing so, a node achieves anonymity by the assumption of "probable innocence".

The anonymity represents an extension to the current DCXP framework as summarised in 1. The extension builds on the existing DCXP architecture, subsequently inheriting the core functionalities of system start up, initialisation and operation with the exception of the modifications detailed within this chapter.

3.1 Grouping

The grouping of users addresses some key challenges with obtaining anonymity. Users are hidden in groups making it impossible for an external user communicating with the group to identify the terminal recipient of any transmitted data. The sender's awareness is restricted to the destination's group and the random node with which it communicates. Composition of the group is achieved by subdividing the underlying DHT into smaller sub-groups. The group inherits node randomisation since the DHT's composition is determined by the hashing of node IP addresses across the network. Each group uses a token ring like protocol to construct a communication structure, such that each node is only aware of its predecessor and successor node in the token ring. By using this grouping scheme, anonymity is maintained if the group contains three or more nodes. To find the identity of an anonymous value, a malicious user must control both the predecessor or and the successor node, which is difficult to achieve since the node distribution is random by virtue of the DHT.

3.2 Changes to the UCI When Disseminating Anonymous Context

The UCIs previously mentioned in 2.3 and fully described in [17] require modification to allow for anonymity. The current UCI contains a username to identify the owner of the published context information. In order to anonymise the information, the trivial solution is to simply remove the username from the UCI. However, doing so will also remove the user context to the information thereby defeating one of the chief aims of the DCXP framework. Therefore we opt for an alternative approach of not removing the username but enabling the option of exchanging the username with an anonymous pseudonym. The pseudonym is either generated automatically to be completely anonymous or selected by the end user.

The benefits of the pseudonym is to allow a user to anonymise context information while still permitting the grouping of related context information, such as a location sensor and a co-located CO_2 sensor. The owner of the sensor remain

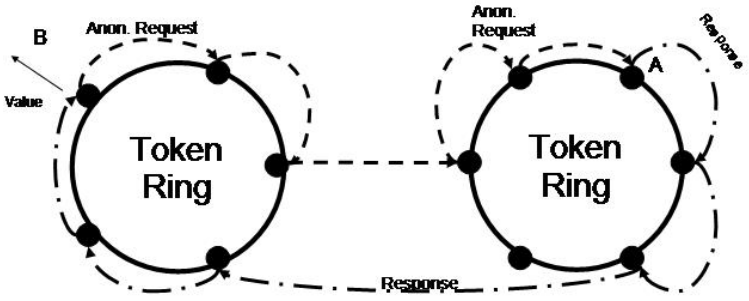

Fig. 3. DCXP Anonymous Signalling

anonymous, but the temperature sensor is given an additional context enabling a third party service monitoring CO_2 rates to benefit from the information.

3.3 Message Routing and Signaling

A token within the token ring carries both encrypted and plain text messages. On receiving a token, the node will attempt to decrypt any encrypted messages with its own private key. All successfully decrypted messages will be actioned after which all remaining encrypted messages are forwarded with the token. Plain text messages are first inspected to determine if their containing requests should be executed by this node. The remaining plain text messages are forwarded with the token as well.

However, forwarding of plain text messages may also entail delivery to the target group of the message, instead of forwarding it to the next token ring node. This choice is determined by "flipping a coin". The key benefit of this is that it increases the randomness in the structure without adding any significant overheads.

If the current node decides to deliver the message, it will further inspect and action the message depending on the message type. If however, the decision was to forward the token, then the current node simply delivers the token to its successive node which then undergoes the same decision making process.

When a node receives message from an external group, it awaits its turn for the token and delivers the message into the current token, subsequently passing the token onto the successive node. If a node encounters the same token message twice, the message is removed from the token, the assumption at this point being that the message, having made a complete round trip is either unclaimed or has been actioned.

The net outcome of this is that the source is completely unable to derive the terminal destination of the request or response data and members of the group itself are also unaware of the final recipient of the data, since nodes are simply forwarding tokens in a repeated non-discriminatory manner. Figure 3 illustrates an overview of the signalling process within the anonymity extension of DCXP.

Table 2. The primitive messages of the Token Ring

ANON_REGISTER_UCI	A CUA uses ANON_REGISTER to register the UCI of a CI with the CS anonymously.
ANON_RESOLVE_UCI	In order to anonymously find where a CI is located, a CUA sends an ANON_RESOLVE_UCI.
ANON_GET	If the resolved UCI is not anonymous the CUA uses an ANON_GET to request the CI.
ANON_SUBSCRIBE	ANON_SUBSCRIBE enables the CUA to start a subscription to an anonymous CI, only receiving new information when the CI is updated.
ANON_NOTIFY	The source CUA provides notification about the latest information to subscribing CUAs every time an update occurs or if asked for an immediate update with GET.
ANON_DIALOG_RESOLVE_UCI	In order to anonymously find where an anonymous CI is located, a CUA sends an ANON_DIALOG_RESOLVE_UCI.
ANON_DIALOG_GET	If the location of the UCI is anonymous the CUA sends an ANON_DIALOG_GET to the resolved location.
ANON_DIALOG_NOTIFY	The ANON_DIALOG_NOTIFY is used in reply to an ANON_DIALOG_GET or sent to subscribers whenever a CI value is updated if the CI is anonymous.

3.4 DCXP Anonymity Primitives

Then Anonymous Dialog messages is used for both sender and receiver anonymity while the non dialog messages only achieves receiver anonymity.

The same message names and structures as used in DCXP are adopted and extended to support the anonymous messaging protocol; see 2.3, 3.3. The primitives are detailed in table 2.

Anonymous Registration. The ANON_REGISTER_UCI, is much similar to a DXCP register except that message now contains the UCI along with its public key and it group. When a node wishes to anonymously register a UCI, it creates a register message and inserts it into the token when available. A random node in the local ring will complete the registration process with the DHT on behalf of the node.

Anonymous Resolve. An ANON_RESOLVE_UCI message is created and deposited into the token, and like the ANON_REGISTER_UCI is completed by a proxy node. The response messages are returned addressed to the group and deposited into the token to be digested by the originator.

Anonymous Get. The ANON_GET is put into the ring similar to the ANON_RESOLVE_UCI message, and is handled similarly.

Anonymous Notify. When a node executing the DCXP GET receives a reply, it constructs an ANON_NOTIFY message which is put into the token and is not removed once it has been read by the requester. The message instead traverses the ring once before it is removed. This increases anonymity in the ring and no other node is aware of the terminal recipient of the request.

Anonymous Dialogue Resolve. The resolve function when the CI provider wishes to remain anonymous differs from when only the requester desires so. The resolve is placed in the token ring as an Anonymous Resolve but the executing node retrieves the value once of the UCI it just have resolved, this value contains the group number and public key of the CI. The key and group number is posted in the token ring and allowed to circulate one lap.

Anonymous Dialogue Get. The ANON_DIALOG_GET message is much similar to an ANON_GET message with the exception that both the sender and the recipient remain anonymous. The originating node constructs the message, encrypted with the public session key of the target node along with the identification of the target group. The message is deposited in the token and passed on to the successive nodes as described in 3.3.

Anonymous Dialogue Notify. In an ANON_DIALOG_GET message, the node target node for a UCI creates a message in response to a ANON_GET. The message is encrypted using the public key of the requester and deposited in the token. The message is deposited in the token and passed on to the successive nodes as described in 3.3.

4 Conclusions and Future Work

In this paper we presented a solution for anonymously disseminating context information in a peer to peer network. We presented a solution that handles the provisioning of context data in a real-time reliable manner originating from fixed computing devices or more ubiquitous devices such as mobile phones, PDAs and laptops. We propose an extension to DCXP to provide for the distributed access of anonymous context information. This extension utilises the DCXP network to create randomised groups within which users can be anonymous under the pretence of "probably innocence". This anonymity is achievable since all users in a group act as a both proxies and terminal clients. The group uses a token ring scheme to communicate and execute data transmission operations revealing neither identities nor activity data. This results in nodes being untraceable by other nodes internal and external to the group and by extension achieving anonymity. Since there are no maximum amount of hops a message inside a token can take; a message can be carried around in the ring indefinitely. But

the coin flip algorithm will ensure that the chance of a message being delivered follows a binary distribution, therefore it is highly unlikely that a message will be indefinitely postponed.

The anonymous support presented is underpinned by a socio-technological mandate to enable the broadest participation in wide area context networks by individuals while providing the option of anonymity and privacy where required. As a distributed platform, DCXP is not afforded the centralised privacy and anonymity controls enjoyed by technologies such as the IMS infrastructure. The solution, while increasing data overhead provides a novel approach on par with centralised controls.

The token system assumes a mutual trust of all nodes inside each ring. However this exposes the ring to malicious attacks, such as denial of service. This can be achieved by always discarding the tokens or removing all messages from the tokens without forwarding them. However such denial of service attacks do not compromise anonymity within the system.

Our approach reinforces the importance of privacy regardless of the architectures employed in disseminating real-time context information and that neither has to be disadvantaged in achieving this. As we increasingly trend towards more ubiquitous computing paradigms, it gradually becomes more of a requirement to be able to involve already vast and expanding base of mobile computing users. DCXP provides an infrastructure for accomplishing this task and adding this anonymity extension allows for even greater participation of a mobile user base without requiring users to be actively involved in anonymity and privacy.

Further work to this research involves an implementation and simulation to test scalability involving issues introduced by the token ring network such as group and token sizes as well as the number of tokens in each ring.

Acknowledgment

The research is partially supported by the regional EU target 2 funds, regional public sector, and industry such as Ericsson Research and Telia.

References

1. Grosky, W.I., Kansal, A., Nath, S., Liu, J., Zhao, F.: Senseweb: An infrastructure for shared sensing. Multimedia 14, 8–13 (2007)
2. Krco, S., Cleary, D., Parker, D.: P2P mobile sensor networks. In: Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS), p. 324c (2005)
3. JXTA, `https://jxta.dev.java.net/`
4. Shim, E., Narayanan, S., Daley, G.: A P2P SIP architecture two layer approach, Panasonic Digital Networking Laboratory, Dallas, IETF draft (March 2006)
5. Kawakami, T., Ly, B.L.N., Takeuchi, S., Teranishi, Y.: Distributed sensor information management architecture based on semantic analysis of sensing data. In: Proceedings of the International Symposium on Applications and the Internet, pp. 353–356 (2008)

6. Kelly, D.: A taxonomy for and analysis of anonymous communications networks. PhD thesis, Air Force Institute of Technology (March 2009)
7. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 24(2) (Feburary 1981)
8. Pfitzmann, A., Waidner, M.: Networks without user observability – design options. In: Pichler, F. (ed.) EUROCRYPT 1985. LNCS, vol. 219, pp. 245–253. Springer, Heidelberg (1986)
9. Zhao, B.Y., Rowstron, A., Zhuang, L., Zhou, F.: Cashmere: Resilient anonymous routing. In: The 2nd Symposium on Networked Systems Design and Implementation, NSDI (2005)
10. Goldschlag, D.M., Reed, M.G., Syverson, P.F.: Hiding routing information. In: Proceedings of the First International Workshop on Information Hiding, London, UK, pp. 137–150. Springer, Heidelberg (1996)
11. Gaurav, A.M., Oberoi, G., Post, A., Reis, C., Druschel, P.: Ap3: Cooperative, decentralized anonymous communication. In: Proc. of SIGOPS European Workshop (2004)
12. Reiter, M.K., Rubin, A.D.: Crowds: anonymity for web transactions. ACM Trans. Inf. Syst. Secur. 1(1), 66–92 (1998)
13. Kanter, T., Pettersson, S., Forsström, S., Kardeby, V., Österberg, P.: Ubiquitous mobile awareness from sensor networks. In: Proceedings of the 2^{nd} International ICST Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications (MOBILWARE), Berlin, Germany (April 2009)
14. Stoica, I., Morris, R., Karger, D., Kaashoek, F.M., Balakrishnan, H.: Chord: A scalable peer-to-peer lookup service for internet applications. In: Proc. of the Conf. on Applications, Technologies, Architectures, and Protocols for Comp. Comm., August 2001, vol. 31, pp. 149–160. ACM Press, San Diego (2001)
15. Rosenberg, J.: SIMPLE made simple: An overview of the IETF specifications for instant messaging and presence using the session initiation protocol (SIP), IETF, Internet-draft (2008)
16. Fielding, R.T., Berners-Lee, T., Masinter, L.: Uniform resource identifiers (URI): Generic syntax, IETF, RFC 2396 (August 1998)
17. Kanter, T., Österberg, P., Walters, J., Kardeby, V., Forsström, S., Pettersson, S.: The mediasense framework. In: Proceedings of th IARIA International Conference on Digital Telecommunications (ICDT), Colmar, France (July 2009)