Keynote: From groupware to large-scale trustworthy distributed collaborative systems
Claudia-Lavinia Ignat

To cite this version:
Claudia-Lavinia Ignat. Keynote: From groupware to large-scale trustworthy distributed collaborative systems. CRIWG 2018 - 24th International Conference on Collaboration and Technology, Sep 2018, Costa de Caparica, Portugal. hal-01875534

HAL Id: hal-01875534
https://hal.science/hal-01875534
Submitted on 17 Sep 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
From groupware to large-scale trustworthy distributed collaborative systems

Claudia-Lavinia Ignat, Inria, France
Douglas Engelbart: Augmenting Human Intellect

The Mother of all Demos, December 9, 1968

NLS: Online System
https://archive.org/details/dougengelbartarchives
Groupware, early 1990s

- « Computer-based systems that support groups of people engaged in a common task (or goal) and that provide an interface to a shared environment. » [EGR91]

- Lotus Notes, one of the first commercial groupware allowing remote group collaboration
Groupware Time Space Matrix [J88]

- **Face to face interactions**
  - decision rooms, single display groupware, shared table, wall displays, roomware, …

- **Continuous task**
  - large public display, team rooms, shift work groupware, project management, …

- **Remote interactions**
  - video conferencing, instance messaging, chats/MUDs/virtual worlds, shared screens, multi-user editors, …

- **Communication + coordination**
  - email, bulletin boards, blogs, asynchronous conferencing, group calendars, workflow, version control, wikis, …

- **same time**
  - synchronous

- **different time**
  - asynchronous

- **same place**
  - co-located

- **different place**
  - remote
Groupware: supported solutions

- **Turn taking**: allow only one active participant at a time
  - e.g. RTCAL [SG88], SHARE [G90]

- **Locking**: concurrent editing allowed only if users lock and edit different objects
  - e.g. Colab [SFBKLS88]

- **Operational transformation**
  - e.g. GROVE [EG89]
Google Drive

March 2006
Writely
(Google Docs)

June 2006
XL2Web
(Google Sheets)

September 2007
Google Slides

2012
Google Drive
“Isn’t it chaotic to all edit in the same document, even the same paragraph, at the same time?”

“Why would a group ever want to edit in the same line of text at the same time?” [EGR91]
Collaborative Systems: from users to community of users

2013: MOOC “Fundamentals of Online Education: Planning and Applications” with 40,000 participants
2016: Nuit debout, more than 70 people edit a pad
2018: online CSCW PC meeting with 120 members
Collaborative Systems:
from users to community of users

Real-time Wikipedia

<table>
<thead>
<tr>
<th>Ponte Morandi: Revision history</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View logs for this page (view filter log)</strong></td>
</tr>
<tr>
<td><strong>Search for revisions</strong></td>
</tr>
<tr>
<td>From year (and earlier): 2016</td>
</tr>
</tbody>
</table>

For any version listed below, click on its date to view it. For more help, see Help:Page history and Help:Edit summary.

External tools: Revision history statistics · Revision history search · Edit by user · Number of watchers · Page view statistics · Fix dead links

(cure) = difference from current version, (prev) = difference from preceding version, m = minor edit, → = section edit, ++ = automatic edit summary

(newest | oldest) View (newer 24 | older 24) (20 | 50 | 100 | 250 | 500)

<table>
<thead>
<tr>
<th>Compare selected revisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• (cure) 12:22, 14 August 2018 Pigionthewing (talk</td>
</tr>
<tr>
<td>• (cure) 12:22, 14 August 2018 Pigionthewing (talk</td>
</tr>
<tr>
<td>• (cure) 12:22, 14 August 2018 Pigionthewing (talk</td>
</tr>
<tr>
<td>• (cure) 12:21, 14 August 2018 Pigionthewing (talk</td>
</tr>
<tr>
<td>• (cure) 12:21, 14 August 2018 Pigionthewing (talk</td>
</tr>
<tr>
<td>• (cure) 12:20, 14 August 2018 Pigionthewing (talk</td>
</tr>
<tr>
<td>• (cure) 12:20, 14 August 2018 37.159.80.23 (talk) . . (4,656 bytes) (0) . . (undo) Tags: Mobile edit, Mobile web edit</td>
</tr>
<tr>
<td>• (cure) 12:19, 14 August 2018 Themandrak (talk</td>
</tr>
<tr>
<td>• (cure) 12:19, 14 August 2018 Avaya1 (talk</td>
</tr>
<tr>
<td>• (cure) 12:19, 14 August 2018 Prionym (talk</td>
</tr>
<tr>
<td>• (cure) 12:19, 14 August 2018 Gianluigi02 (talk</td>
</tr>
<tr>
<td>• (cure) 12:18, 14 August 2018 Denimadept (talk</td>
</tr>
<tr>
<td>• (cure) 12:17, 14 August 2018 37.14.150.97 (talk) . . (4,370 bytes) (+167) . . (ca) (undo)</td>
</tr>
<tr>
<td>• (cure) 12:16, 14 August 2018 Pigionthewing (talk</td>
</tr>
<tr>
<td>• (cure) 12:15, 14 August 2018 Avaya1 (talk</td>
</tr>
<tr>
<td>• (cure) 12:14, 14 August 2018 Avaya1 (talk</td>
</tr>
<tr>
<td>• (cure) 12:14, 14 August 2018 Prionym (talk</td>
</tr>
<tr>
<td>• (cure) 12:13, 14 August 2018 Prionym (talk</td>
</tr>
<tr>
<td>• (cure) 12:13, 14 August 2018 Urbourbo (talk</td>
</tr>
<tr>
<td>• (cure) 12:12, 14 August 2018 Avaya1 (talk</td>
</tr>
<tr>
<td>• (cure) 12:12, 14 August 2018 Pierreofmetalwork (talk</td>
</tr>
<tr>
<td>• (cure) 12:12, 14 August 2018 Prionym (talk</td>
</tr>
<tr>
<td>• (cure) 12:12, 14 August 2018 Pierreofmetalwork (talk</td>
</tr>
<tr>
<td>• (cure) 12:12, 14 August 2018 Prionym (talk</td>
</tr>
</tbody>
</table>
Limitations of Central Authority Systems
Peer-to-Peer Collaborative Systems
Collaboration Modes – Concurrent Changes
Collaboration Modes – Offline Work

Conflicts
Collaboration Modes – Ad-hoc Collaboration
Research issues

1. How to maintain consistency of different copies in the face of concurrent modifications?

2. How to evaluate the design of collaborative systems and approaches?

3. How to secure collaboration data?
Research issues

1. How to maintain consistency of different copies in the face of concurrent modifications?

2. How to evaluate the design of collaborative systems and approaches?

3. How to secure collaboration data?
Optimistic Replication [SS05]

- Trade-off between consistency and availability
  - Optimistic replication: allows replicas to diverge

- Strong Eventual Consistency
  - Eventual delivery: An update executed at some correct replica eventually executes at all correct replicas
  - Strong convergence: Correct replicas that have executed the same updates have equivalent states
  - No consensus in background, no need to rollback

- Intention preservation
  - « Effect of each operation should be observed on all copies »
Operational transformation (OT) [EG89]

• $n$ copies of an object hosted at $n$ sites
• An object is modified by applying operations

• Each operation is
  • generated at a site (local execution), and applied immediately on the local copy
  • broadcasted to other sites
  • integrated at those sites (remote execution)

• System is correct if when it is idle all copies are identical (SEC)
Operational transformation (OT)

• General architecture with two main components:
  • An integration algorithm (diffusion, integration)
  • A set of transformation functions (conflict resolution)

• Running example for textual document = sequence of characters

  Site 1
  Site 2

• Operations:
  • ins(p, c)
  • del(p)

T(ins(p1,c1), ins(p2,c2)) :-
  if (p1<p2) return ins(p1,c1)
  else return ins(p1+1,c1)
endif
Operational transformation
Correctness [EG89]

\[(TP1) \quad \text{op}_1 \circ T(\text{op}_2, \text{op}_1) \equiv \text{op}_2 \circ T(\text{op}_1, \text{op}_2)\]

Site 1

Site 2

T(\text{op}_2: \text{operation}, \text{op}_1: \text{operation}) = \text{op}'_2

\begin{itemize}
  \item \text{op}_1 \text{ and } \text{op}_2 \text{ concurrent, defined on a state } S
  \item \text{op}'_2 \text{ same effects as } \text{op}_2, \text{ defined on } S.\text{op}_1
\end{itemize}
Operational transformation
Correctness [RNG96]

\[(TP2) \quad T(op_3, op_1 \circ T(op_2, op_1)) = T(op_3, op_2 \circ T(op_1, op_2))\]
Operational transformation (OT)
Existing approaches

- Two main families:
  - Transformation functions satisfying both TP1 and TP2: SOCT2 [SCF97] + TTF [OUMI06]
  - Control algorithms avoiding (needs of) TP2: SOCT4 [VCFS00], Jupiter [NCDL95]
Operational transformation (OT)

Summary

• Transforms non commuting operations to make them commute
• Genericity
• Time complexity
  • Average: $O(H \cdot c)$ \hspace{1cm} H: #ops
  • Worst case: $O(H^2)$ \hspace{1cm} c: avg. #conc. ops
• Difficult to write correct transformation functions
• State vectors used for detecting concurrency ⇒ scalability limitations
• **Not very suitable for large scale peer-to-peer collaboration**
Conflict-free Replicated Data Types (CRDT) [SPBZ11]

• Design operations to be commutative by construction

• Abstract data types
  • Designed to be replicated at multiple sites
  • Any replica can be modified without coordination
  • State convergence is guaranteed

• State-based and operation-based approaches
Conflict-free Replicated Data Types (CRDT)
State-based Replication

- **Algorithm**
  - Periodically, replica at \( p_i \) sends its current state to \( p_j \)
  - Replica \( p_j \) merges received state into its local state by executing \( m \)
  - After receiving all updates (irrespective of order), each replica will have same state
Conflict-free Replicated Data Types (CRDT)
State-based Replication

• Merge operator:
  • **Commutative:** \( x \cdot y = y \cdot x \)
  • **Associative:** \( (x \cdot y) \cdot z = x \cdot (y \cdot z) \)
  • **Idempotent:** \( x \cdot x = x \)

• A semi-lattice is a Partial order \( \leq \) set \( S \) with a least upper bound (LUB), denoted \( \sqcup \)
  • \( m = x \sqcup y \) is a LUB of \( \{ x, y \} \) under \( \leq \) if and only if
    \[ \forall m', x \leq m' \land y \leq m' \Rightarrow x \leq m \land y \leq m \land m \leq m' \]
  • It follows that \( \sqcup \) is commutative, associative and idempotent
Conflict-free Replicated Data Types (CRDT)
Convergent Replicated Data Type (CvRDT)

• Example

\[
\{5\} \cup \{3\} = \{3, 5\} \quad \{3, 5\} \cup \{5, 7\} = \{3, 5, 7\}
\]

\[
\{5\} \cup \{3, 5\} = \{3, 5\}
\]

\[
\{3, 5\} \cup \{5, 7\} = \{3, 5, 7\}
\]

\[
\{5\} \cup \{7\} = \{5, 7\} \quad \{5, 7\} \cup \{3, 5\} = \{3, 5, 7\}
\]
Conflict-free Replicated Data Types (CRDT)

Operation-based Replication

- An update split into \((t, u)\): \(t\) is a side-effect-free prepare-update method and \(u\) is an effect-update method.

Algorithm
- Updates delivered to all replicas
- Causally-ordered broadcast, every message delivered to every node exactly once w.r.t. happen-before order

Commutativity holds for concurrent updates
Conflict-free Replicated Data Types (CRDT)  
Commutative Replicated Data Type (CmRDT)

• Example

\[
\begin{align*}
\{5\} & \cup \{3\} = \{3, 5\} & \{3, 5\} & \cup \{7\} = \{3, 5, 7\} \\
\{5\} & \cup \{7\} = \{5, 7\} & \{5, 7\} & \cup \{3\} = \{3, 5, 7\} \\
\end{align*}
\]
Conflict-free Replicated Data Types (CRDT)  
CvRDT vs. CmRDT

• Both approaches are equivalent  
  • A state-based object can emulate an operation-based object, and vice-versa

• Operation-based:  
  • More efficient since you only ship small updates  
  • But require exactly once causally-ordered broadcast

• State-based:  
  • Only require reliable broadcast  
  • Communication overhead of shipping the whole state

• Delta State-based [ASB18]:  
  • Small messages  
  • Dissemination over unreliable communication channels
Consistency Maintenance
Conflict-free Replicated Data Types (CRDT)

- Register
  - Last-Writer Wins
  - Multi-Value
- Set
  - Grow-Only
  - 2-Phase
  - Observed-Remove
  - Observed-Update-Remove

- Map
- Counter
- Graph
  - Directed
  - Monotonic DAG
  - Edit graph

- Sequence
Conflict-free Replicated Data Types (CRDT) (Text) Sequence [PMSL09] [WUM09]

- Document = linear sequence of elements
  - Each element has a unique identifier
  - Identifier constant for the lifetime of the document
  - Dense total order of identifiers consistent with element order:
    \[ \forall \, id_x, id_y: \, id_x < id_y \Rightarrow \exists \, id_z: \, id_x < id_z < id_y \]

- Different approaches for generating identifiers:
  - TreeDoc, Logoot, LogootSplit, ...
Conflict-free Replicated Data Types (CRDT)

Logoot [WUM09]

- Logoot identifiers: \(<p_1,s_1,h_1>, <p_2,s_2,h_2>, \ldots, <p_k,s_k,h_k>\)
  - \(p_i\): integer
  - \(s_i\): site identifier
  - \(h_i\): logical clock at site \(s_i\)

- Time complexity
  - Average: \(O(k \log(n))\)
  - Worst case: \(O(H \cdot \log(H))\)
    - \(H\): number of operations
    - \(n\): document size (non-deleted characters)
    - \(k\): average size of Logoot identifier

- No need for concurrency detection
- Identifiers storage cost
- New design for each data type
- Suitable for large-scale collaboration
Conflict-free Replicated Data Types (CRDT)
LogootSplit [AMOI13]

LogootSplit identifiers

Base

| p₁  | ... | pₙ  | site_id | clock | begin | end |

Interval

1,1,[0,16] concurrency contrl
Insert r between “concur” and “ency contrl”

1,1,[0,5] concur
1,1,5,2,1,[0,0] r
1,1, [6,16] ency contrl

Insert o between “ency contr” and “l”

1,1,[0,5] concur
1,1,5,2,1,[0,0] r
1,1, [6,15] ency contr
1,1,15,3,1,[0,0] o
1,1,[16,16] l
OT vs. operation-based CRDT

- CRDT: more formalised approach
- OT: more generic and guided
  - Generic concurrency control algorithm
  - Operation transformations specific to application domain
- CRDT: different solutions for concurrency handling for different data types
- CRDT: Metadata overhead
Delays in MUTE [NEOIC17] https://coedit.re/
Delays in GoogleDocs [DI16]
Research issues

1. How to maintain consistency of different copies in the face of concurrent modifications?

2. How to evaluate the design of collaborative systems and approaches?

3. How to secure collaboration data?
User Study: The effect of delay on users

- Delays in seeing modifications of other users
  - Network delay
  - Time complexity of consistency maintenance algorithms
  - Types of architecture

- How does delay influence group performance?
Experiment design

- 20 groups of 4 students
  - Perform several collaborative editing tasks
    - A proofreading task
    - A sorting task
    - **A note taking task**
  - Use the provided collaborative editor (Etherpad) + chat
  - Each group experienced a **certain delay** (0, 4, 6, 8, 10 s)
- Registration of user keyboard inputs
- Video recording of user activities on desktop
Note-taking [IOFSC15]
Delay reduces Group Performance

- Delay increases error rate and redundancy
Delay reduces Group Performance

- Delay decreases proportion of keywords
Design implications

• Reduce the delay by the choice of the architecture and synchronisation algorithms

• Make users aware of existing delays such that they can compensate for the delay by coordination strategies

• Analyse real collaboration traces to understand collaboration patterns and behavior [NI18]
Research issues

1. How to maintain consistency of different copies in the face of concurrent modifications?

2. How to evaluate the design of collaborative systems and approaches?

3. How to secure collaboration data?
Security in peer-to-peer collaboration

- How to learn and verify the other party’s key?
- Trust-based access control
Trust establishment

• How to learn and verify the other party’s key before establish a secure communication channel?
  • Out of band trust establishment
  • Trust establishment by the provider
Out of band trust establishment

- Unintuitive, error-prone

Alice, is FGY345 your public key?

Bob, what is a public key?

My key fingerprint is 43:51:af:77:66:fc:ac:df:b1....something
Trust establishment by the provider
Centralized key server

- Clients query providers for keys of other users
- Users have to trust provider, e.g., WhatsApp

Alice

Client A

Register Alice with $PK_A$

Secure Message Provider

1

Alice’s key $PK'_A$

Client B

2

Bob
Transparent log

Alice
PK_A

Bob
PK_B

Key Server

Register

Query

Users
Certificate transparency \cite{L14}/CONIKS \cite{MBBFF15}

- Gossiping
- No client incentive
- Subject to Sybil and Eclipse attacks
Trusternity: Blockchain-based Auditing of Transparent Log Servers [NEIP18]
Trust-based access control

• Dynamic trust values among users

• How to define an access control based on trust and how to compute trust based on collaborative experience?
Trust computation

- Respect/Violation of contracts
  - Contracts in collaborative editing (share, edit)

- Reporting of fake news in Facebook
- Quality of user contributions
Validation of trust-based collaboration

- Using game theory (trust game) [BDM95]

**Balance: 10€**

**User 1 sends 8€ to User 2**

**Balance: 10€**

**User 2 receives 3 \times 8€ = 24€**

**New balance: 2€**

**User 2 sends back 17€ to User 1**

**Balance: 34€**

**Final balance: 19€**

**New balance: 34€**

**Final balance: 17€**
Validation of trust-based collaboration

- Proposal of a trust metric reflecting user behavior [DI16]
- User studies on various trust game variations
  - Trust can replace knowing the identity of collaborators
  - People take into account the trust value of the partner in their future collaboration
Large-scale trustworthy distributed collaborative systems

- New uses and new practices due to large scale adoption
- New challenges
  - Consistency of replicated data
  - User studies
  - Trust and Security
References

References

- **[EG89]** Concurrency Control in GroupWare Systems, C.A. Ellis and S.J. Gibbs. ACM SIGMOD Record 18(2), 1989.
References


- **[PMSL09]** A commutative replicated data type for cooperative editing, N. Preguica, M. Joan, M. Shapiro, and M. Letia. ICDCS 2009.

References

References

- **[NI18]** An Analysis of Merge Conflicts and Resolutions in Git-Based Open Source Projects. Hoai Le Nguyen, Claudia-Lavinia Ignat. Journal of Computer Supported Cooperative Work, 2018
- **[L14]** Certificate transparency. B. Laurie. Queue 12(8), 2014
- **[NEIP18]** Blockchain-Based Auditing of Transparent Log Servers. Hoang-Long Nguyen, Jean-Philippe Eisenbarth, Claudia-Lavinia Ignat, Olivier Perrin. DBSec 2018
References

Thank you

COAST Team

http://team.inria.fr/coast/