LoST: Local State Transfer
And BSPL, the Blindingly Simple Protocol Language

Munindar P. Singh
North Carolina State University

Spring 2012
Interactions and Protocols
Distributed systems of autonomous, heterogeneous agents

- Enable interoperation
- Maintain independence from internal reasoning (policies)
- Support composition of distributed systems
Properties of Participants

- **Autonomy**
- **Myopia**
  - All choices must be local
  - Correctness should not rely on future interactions
- **Heterogeneity: local ≠ internal**
  - Local state (projection of global, which is stored nowhere)
    - Public or observable
    - Typically, must be revealed for correctness
  - Internal state
    - Private
    - Must never be revealed to avoid false coupling
- **Shared nothing representation of local state**
  - Enact via messaging
Traditional Specifications

Low-level, procedural approaches leading to over-specified protocols

▶ Traditional approaches
  ▶ Emphasize arbitrary ordering and occurrence constraints
  ▶ Then work hard to deal with those constraints

▶ Our philosophy: The Zen of Distributed Computing
  ▶ Necessary ordering constraints fall out from *causality*
  ▶ Necessary occurrence constraints fall out from *integrity*
  ▶ Unnecessary constraints: simply *ignore* such
BSPL, the Blindingly Simple Protocol Language

Main ideas

- Only two syntactic notions
  - Declare a message schema: as an atomic protocol
  - Declare a composite protocol: as a bag of references to protocols

- Parameters are central
  - Provide a basis for expressing meaning in terms of bindings in protocol instances
  - Yield unambiguous specification of compositions through public parameters
  - Capture progression of a role’s knowledge
  - Capture the completeness of a protocol enactment
  - Capture uniqueness of enactments through keys

- Separate structure (parameters) from meaning (bindings)
  - Capture many important constraints purely structurally
Key Parameters in BSPL
Marked as "key"

- All the key parameters *together* form the key
- Each protocol must define at least one key parameter
- Each message or protocol reference must have at least one key parameter in common with the protocol in whose declaration it occurs
- The key of a protocol provides a basis for the uniqueness of its enactments
Parameter Adornments in BSPL

Capture the essential causal structure of a protocol

- $\text{\textit{in}}$: Information that must be provided to instantiate a protocol
  - Bindings must exist locally in order to proceed
  - Bindings must be produced through some other protocol

- $\text{\textit{out}}$: Information that is generated by the protocol instances
  - Bindings can be fed into other protocols through their $\text{\textit{in}}$ parameters, thereby accomplishing composition
  - A standalone protocol must adorn all its public parameters $\text{\textit{out}}$

- $\text{\textit{nil}}$: Information that is absent from the protocol instance
  - Bindings must not exist

Ignoring data types of parameters for simplicity: assume strings everywhere
The **Hello** Protocol

Hello \(\{\)

\[\begin{array}{ll}
\textit{role} & \text{Self, Other} \\
\textit{parameter} & \text{out greeting key}
\end{array}\]

\text{Self} \rightarrow \text{Other: hi}[\text{out greeting key}]

\}

- At most one instance of **Hello** for each greeting
- At most one **hi** message for each greeting
- Enactable standalone: no parameter is \(\text{in}\)
- The key of **hi** is explicit; often left implicit on messages
The Pay Protocol

Pay \{ 
  \textcolor{red}{\text{role}} \text{ Payer , Payee} \\
  \textcolor{blue}{\text{parameter}} \text{ in ID key , in amount} \\

  \text{Payer } \mapsto \text{ Payee : payM[}\text{ in ID , in amount}] \\
\}

- At most one \textit{payM} for each ID
- Not enactable standalone: \textbf{why}?
- The key of \textit{payM} is implicit; could be made explicit
- Eliding \textbf{\(\lnot\)} means \textbf{\(\lnot\)} clauses in this paper
The Offer Protocol

Offer \{ 
\begin{align*}
\textit{role} & \text{ Buyer, Seller} \\
\textit{parameter} & \text{ in ID key, out item, out price}
\end{align*}
\}

Buyer $\mapsto$ Seller: rfq[$in$ ID, $out$ item]  
Seller $\mapsto$ Buyer: quote[$in$ ID, $in$ item, $out$ price]

- The key ID uniquifies instances of \textit{Initiate Offer, rfq, and quote}
- Not enactable standalone: at least one parameter is $\textit{in}$
- An instance of \textit{rfq} must precede any instance of \textit{quote} with the same ID: \textit{why}?
- No message need occur: \textit{why}?
- \textit{quote} must occur for \textit{Offer} to complete: \textit{why}?
The *Initiate Order* Protocol

\[ \text{Initiate } \text{Order } \{ \]

\[ \text{role } B, S \]

\[ \text{parameter } \text{out} \text{ ID } \text{key} , \text{out} \text{ item} , \text{out} \text{ price} , \text{out} \text{ rID} \]

\[ B \leftrightarrow S : \text{ rfq } [ \text{out} \text{ ID} , \text{out} \text{ item} ] \]

\[ S \leftrightarrow B : \text{ quote } [ \text{in} \text{ ID} , \text{in} \text{ item} , \text{out} \text{ price} ] \]

\[ B \leftrightarrow S : \text{ accept } [ \text{in} \text{ ID} , \text{in} \text{ item} , \text{in} \text{ price} , \text{out} \text{ rID} ] \]

\[ B \leftrightarrow S : \text{ reject } [ \text{in} \text{ ID} , \text{in} \text{ item} , \text{in} \text{ price} , \text{out} \text{ rID} ] \]

\[ \} \]

- The key ID uniquifies instances of *Order* and each of its messages
- Enactable standalone
- An *rfq* must precede a *quote* with the same ID
- A *quote* must precede an *accept* with the same ID
- A *quote* must precede a *reject* with the same ID
- An *accept* and a *reject* with the same ID cannot both occur: *why?*
The *Purchase* Protocol

Purchase { 

role B, S, Shipper

parameter out ID key, out item, out price, out outcome

B ↦ S: rfq [out ID, out item]
S ↦ B: quote[in ID, in item, out price]
B ↦ S: accept[in ID, in item, in price, out address, out resp]
B ↦ S: reject[in ID, in item, in price, out outcome, out resp]

S ↦ Shipper: ship[in ID, in item, in address]
Shipper ↦ B: deliver[in ID, in item, in address, out outcome]
}

- At most one item, price, and outcome binding per ID
- Enactable standalone
- reject conflicts with accept on response (a private parameter)
- reject or deliver must occur for completion (to bind outcome)
Possible Enactment as a Vector of Local Histories

Buyer

rfq

quote

accept

deliver

Seller

rfq

quote

accept

ship

deliver

Shipper

ID, item

ID, price

ID, address

ID, item, address

ID, item, address, outcome
Knowledge and Viability

When is a message viable? What effect does it have on a role’s local knowledge?

- Knowledge increases monotonically at each role
- An \( \text{out} \) parameter creates and transmits knowledge
- An \( \text{in} \) parameter transmits knowledge
- Repetitions through multiple paths are harmless and superfluous
Realizing BSPL via LoST

LoST = Local State Transfer

- Does not assume FIFO or reliable messaging
- Provides
  - Unique messages
  - Integrity checks on incoming messages
  - Consistency of local choices on outgoing messages
Implementing LoST

Think of the message logs you want

- For each role
  - For each message that it sends or receives
    - Maintain a *local* relation of the same schema as the message
  - Receive and store any message provided
    - It is not a duplicate
    - Its integrity checks with respect to parameter bindings
  - Send any unique message provided
    - Parameter bindings agree with previous bindings for the same keys for *\textit{in}* parameters
    - No bindings for *\textit{out}* and *\textit{nil}* parameters exist
Comparing LoST and WS-CDL

- **Similarity**: both emphasize interaction

- **Differences**: WS-CDL is
  - **Procedural**
    - Explicit constructs for ordering
    - Sequential message ordering by default
  - **Agent-oriented**
    - Includes agents’ internal reasoning within choreography (specify what service an agent executes upon receiving a message)
    - Relies on agents’ internal decision-making to achieve composition (take a value from Chor A and send it in Chor B)
  - No semantic notion of completeness
## Comparing LoST and ReST

<table>
<thead>
<tr>
<th></th>
<th>ReST</th>
<th>LoST</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Modality</strong></td>
<td>Two-party; client-server; synchronous</td>
<td>Multiparty interactions; peer-to-peer; asynchronous</td>
</tr>
<tr>
<td><strong>Computation</strong></td>
<td>Server computes definitive resource state</td>
<td>Each party computes its definitive local state and the parties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>collaboratively and (potentially implicitly) compute the definitive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interaction state</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Server maintains no client state</td>
<td>Each party maintains its local state and, implicitly, the relevant</td>
</tr>
<tr>
<td></td>
<td></td>
<td>components of the states of other parties from which there is a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>chain of messages to this party</td>
</tr>
</tbody>
</table>
## Comparing LoST and ReST

<table>
<thead>
<tr>
<th></th>
<th>ReST</th>
<th>LoST</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transfer</strong></td>
<td>State of a resource, suitably represented</td>
<td>Local state of an interaction via parameter bindings, suitably represented</td>
</tr>
<tr>
<td></td>
<td>For some verbs, especially <strong>GET</strong></td>
<td>Always; repetitions are guaranteed harmless</td>
</tr>
<tr>
<td><strong>Idempotent</strong></td>
<td>Programmer can specify if cacheable</td>
<td>Always cacheable</td>
</tr>
<tr>
<td><strong>Caching</strong></td>
<td>Of resources via <strong>URIs</strong></td>
<td>Of interactions via (composite) keys, whose bindings could be <strong>URIs</strong></td>
</tr>
<tr>
<td><strong>Uniform interface</strong></td>
<td><strong>GET, POST, ...</strong></td>
<td><strong>in</strong>, <strong>out</strong>, <strong>nil</strong></td>
</tr>
<tr>
<td><strong>Naming</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Benefits

▶ Technical
  ▶ Statelessness
  ▶ Consistency
  ▶ Atomicity
  ▶ Natural composition

▶ Conceptual
  ▶ Make protocol designer responsible for specifying causality
  ▶ Avoid contortions of traditional approaches when causality is unclear
Remark on Control versus Information Flow

- Control flow
  - Natural within a single computational thread
  - Exemplified by conditional branching
  - Presumes master-slave relationship across threads
  - Impossible between mutually autonomous parties because neither controls the other
  - May sound appropriate, but only because of long habit

- Information flow
  - Natural across computational threads
  - Explicitly tied to causality
### Send-Receive and Send-Send Constraints on a Role

Considering two or more schemas with the same parameter

<table>
<thead>
<tr>
<th></th>
<th>Sends in</th>
<th>Sends out</th>
<th>Sends nil</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sends <strong>in</strong></td>
<td>Unconstrained</td>
<td>Send <strong>out</strong> first</td>
<td>Send <strong>nil</strong> first</td>
</tr>
<tr>
<td>Sends <strong>out</strong></td>
<td></td>
<td>Send <strong>at most one</strong></td>
<td></td>
</tr>
<tr>
<td>Sends <strong>nil</strong></td>
<td></td>
<td>Unconstrained</td>
<td></td>
</tr>
<tr>
<td>Receives <strong>in</strong></td>
<td>Receive at least one instance before send</td>
<td>Receive may occur after send</td>
<td>Send before receive</td>
</tr>
<tr>
<td>Receives <strong>out</strong></td>
<td>Receive at least one instance before send</td>
<td>Impossible</td>
<td>Send before receive</td>
</tr>
<tr>
<td>Receives <strong>nil</strong></td>
<td>Unconstrained</td>
<td>Unconstrained</td>
<td>Unconstrained</td>
</tr>
</tbody>
</table>
### Summarizing Approaches for Interaction

<table>
<thead>
<tr>
<th></th>
<th><strong>Declarative</strong> (Explicit)</th>
<th><strong>Procedural</strong> (Implicit)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Meaning</strong></td>
<td>Commitments and other norms</td>
<td>Hard coded within internal reasoning heuristics</td>
</tr>
<tr>
<td><strong>Operation</strong></td>
<td>Temporal logic, BSPL</td>
<td>State machines, Petri nets, process algebras</td>
</tr>
</tbody>
</table>

- **Declarative approaches for meaning**
  - Improve flexibility
  - Under-specify enactment: potential of interoperability failures

- **Procedural or declarative approaches for operations**
  - Operationally clear, but
  - Tend to emphasize control flow
  - Tend to over-specify operational constraints
  - Yield nontrivial interoperability and endpoint projections

singh@ncsu.edu (NCSU)  
LoST: Local State Transfer  
Spring 2012  23 / 40
Well-Formedness Conditions

- A parameter that is adorned \(\textit{in}\) in a declaration must be \(\textit{in}\) throughout its body
- A parameter that is adorned \(\textit{out}\) in a declaration must be \(\textit{out}\) in at least one reference
  - When adorned \(\textit{out}\) in zero references, not enactable
  - When adorned \(\textit{out}\) in exactly one reference, consistency is guaranteed
  - When adorned \(\textit{out}\) in two or more references, no more than one can execute
- A private parameter must be \(\textit{out}\) in at least one reference and \(\textit{in}\) in at least one reference
New Contributions
Taking a declarative, information-centric view of interaction to the limit

▶ Specification
  ▶ A message is an atomic protocol
  ▶ A composite protocol is a set of references to protocols
  ▶ Each protocol is given by a name and a set of parameters (including keys)
  ▶ Each protocol has *inputs* and *outputs*

▶ Representation
  ▶ A protocol corresponds to a relation (table)
  ▶ Integrity constraints apply on the relations

▶ Enactment via LoST: Local State Transfer
  ▶ Information represented: local ≠ internal
  ▶ Purely decentralized at each role
  ▶ Materialize the relations *only* for messages
Information Centrism

Characterize each interaction purely in terms of information

- Explicit causality
  - Flow of information coincides with flow of causality
  - No hidden control flows
  - No backchannel for coordination

- Keys
  - Uniqueness
  - Basis for completion

- Integrity
  - Must have bindings for some parameters
  - Analogous to NOT NULL constraints

- Immutability
  - Durability
  - Robustness: insensitivity to
    - Reordering by infrastructure
    - Retransmission: one delivery is all it needs
Advanced Topics
Safety: *Purchase Unsafe*

Remove conflict between *accept* and *reject*

Purchase Unsafe {  
  *role* B, S, Shipper  
  *parameter*  
  out ID key, out item, out price, out outcome  

B \rightarrow S: rfq [ out ID, out item ]  
S \rightarrow B: quote [ in ID, in item, out price ]  
B \rightarrow S: accept [ in ID, in item, in price, out address ]  
B \rightarrow S: reject [ in ID, in item, in price, out outcome ]  

S \rightarrow Shipper: ship [ in ID, in item, in address ]  
Shipper \rightarrow B: deliver [ in ID, in item, in address, out outcome ]  
}

- B can send both *accept* and *reject*
- Thus outcome can be bound twice in the same enactment
Liveness: **Purchase No Ship**

Omit *ship*

**Purchase No Ship**

- **role** B, S, Shipper
- **parameter** *out* ID *key*, *out* item, *out* price, *out* outcome

B $\mapsto$ S: rfq [*out* ID, *out* item]
S $\mapsto$ B: quote [*in* ID, *in* item, *out* price]
B $\mapsto$ S: accept [*in* ID, *in* item, *in* price, *out* address, *out* resp]
B $\mapsto$ S: reject [*in* ID, *in* item, *in* price, *out* outcome, *out* resp]

Shipper $\mapsto$ B: deliver [*in* ID, *in* item, *in* address, *out* outcome]

- If B sends *reject*, the enactment completes
- If B sends *accept*, the enactment deadlocks
Encode Causal Structure as Temporal Constraints

- **Reception.** If a message is received, it was previously sent.

- **Information transmission** (sender’s view)
  - Any \textit{in} parameter occurs prior to the message
  - Any \textit{out} parameter occurs simultaneously with the message

- **Information reception** (receiver’s view)
  - Any \textit{out} or \textit{in} parameter occurs before or simultaneously with the message

- **Information minimality.** If a role observes a parameter, it must be simultaneously with some message sent or received

- **Ordering.** If a role sends any two messages, it observes them in some order
Verifying Safety

- Competing messages: those that have the same parameter as \textit{out}
- \textit{Conflict}. At least two competing messages occur
- \textit{Safety} iff the causal structure $\wedge$ conflict is unsatisfiable
Verifying Liveness

- **Maximality.** If a role is enabled to send a message, it sends at least one such message
- **Reliability.** Any message that is sent is received
- **Incompleteness.** Some public parameter fails to be bound
- **Live** iff the causal structure ∧ the occurrence is unsatisfiable
Current and Future Directions

- Methodology for specifying practical protocols
- Expansion of the language to handle role hierarchies
- Treatment of recursive protocols
- For more information
  - BSPL: AAMAS 2011
  - LoST: ICWS 2011
  - Semantics: AAMAS 2012
in-out Polymorphism

price could be \(\textit{in}\) or \(\textit{out}\)

\[
\text{Flexible-Offer} \ \{ \\
\textit{role} \ B, S \\
\textit{parameter} \ \textit{in} \ ID \ \textit{key}, \ \textit{out} \ \textit{item}, \ \textit{price}, \ \textit{out} \ qID \\
B \mapsto S: \ rfq[ID, \ \textit{out} \ \textit{item}, \ \textit{nil} \ \textit{price}] \\
B \mapsto S: \ rfq[ID, \ \textit{out} \ \textit{item}, \ \textit{in} \ \textit{price}] \\
S \mapsto B: \ quote[ID, \ \textit{in} \ \textit{item}, \ \textit{out} \ \textit{price}, \ \textit{out} \ qID] \\
S \mapsto B: \ quote[ID, \ \textit{in} \ \textit{item}, \ \textit{in} \ \textit{price}, \ \textit{out} \ qID] \\
\}
\]

- The price can be adorned \(\textit{in}\) or \(\textit{out}\) in a reference to this protocol
The *Bilateral Price Discovery* protocol

BPD \{ 

*role* Taker, Maker  

*parameter* `out` reqID, `out` key, `out` query, `out` result

Taker \(\mapsto\) Maker: `priceRequest`[`out` reqID, `out` query]  

Maker \(\mapsto\) Taker: `priceResponse`[`in` reqID, `in` query, `out` result]

\}
The *Generalized Bilateral Price Discovery* protocol

GBPD \{ 
  \textit{role} T, M \\
  \textit{parameter} \textit{reqID} \textit{key}, \textit{query}, \textit{res} \\

  T \rightarrow M: \textit{priceRequest}[\textit{out reqID}, \textit{out query}] \\
  T \rightarrow M: \textit{priceRequest}[\textit{in reqID}, \textit{in query}] \\

  M \rightarrow T: \textit{priceResponse}[\textit{in reqID}, \textit{in query}, \textit{out res}] \\
  M \rightarrow T: \textit{priceResponse}[\textit{in reqID}, \textit{in query}, \textit{in res}] 
\}
The **Multilateral Price Discovery** protocol

MPD {
  role Taker, Exchange, Maker
  parameter out reqID, key, out query, out res

  GBPD(Taker, Exchange, out reqID, out query, in res)
  GBPD(Exchange, Maker, in reqID, in query, out res)
}

singh@ncsu.edu (NCSU)  LoST: Local State Transfer  Spring 2012  37 / 40
Standing Order

As in insurance claims processing

Insurance—Claims { role Vendor, Subscriber
  parameter out policyNO key, out reqForClaim key, out claimResponse

Vendor \leftrightarrow Subscriber: createPolicy[out policyNO]
Subscriber \leftrightarrow Vendor: serviceReq[in policyNO, out reqForClaim]
Vendor \leftrightarrow Subscriber: claimService[in policyNO, in reqForClaim, out claimResponse]
}

- Each claim corresponds to a unique policy and has a unique response
- One policy may have multiple claims
- Could make \{policyNO, reqForClaim\} both key
Flexible Sourcing of out Parameters

Buyer or Seller Offer

Buyer→Seller: rfq[\textit{in} ID, \textit{out} item, \textit{nil} price]
Buyer→Seller: rfq[\textit{in} ID, \textit{out} item, \textit{out} price]

Seller→Buyer: quote[\textit{in} ID, \textit{in} item, \textit{out} price, \textit{out} confirmed]
Seller→Buyer: quote[\textit{in} ID, \textit{in} item, \textit{in} price, \textit{out} confirmed]

- The BUYER or the SELLER may determine the binding
- The BUYER has first dibs in this example
Shopping Cart

Shopping Cart {  
  \textbf{role} B, S  
  \textbf{parameter} out ID \texttt{key}, out lineID \texttt{key}, out item, out qty, out price, out finalize  

B \rightarrow S: \texttt{create}[out ID]  
S \rightarrow B: \texttt{quote}[in ID, out lineID, in item, out price]  
B \rightarrow S: \texttt{add}[in ID, in lineID, in item, out qty, in price]  
B \rightarrow S: \texttt{remove}[in ID, in lineID]  

S \rightarrow B: \texttt{total}[in ID, out sum]  
B \rightarrow S: \texttt{settle}[in ID, in sum, out finalize]  
B \rightarrow S: \texttt{discard}[in ID, out finalize]  
}