APUS: Fast and Scalable State Machine Replication on RDMA

Submission #256

***Abstract*—State machine replication (SMR) enforces the same inputs for a program being replicated on several computers (or replicas), tolerating various failures. Recent SMR protocols have greatly improved the availability of server programs (e.g., `Redis`) that store important data. Unfortunately, existing SMR protocols incur prohibitive performance overhead on server programs, because their protocol latency is high when going through OS and TCP/IP layers, or this latency increases almost linearly to the number of concurrent requests or replicas. This paper presents APUS, a new RDMA-based SMR protocol. APUS achieves high performance by: (1) carefully dividing RDMA workloads among replicas; and (2) making all replicas receive consensus messages purely on local memory, just like making threads receive other threads' data efficiently on bare metal memory.**

APUS is the first SMR protocol that achieves low overhead on diverse real-world server programs. Evaluation on nine widely-used server programs (e.g., `Redis` and `MySQL`) shows that APUS incurred merely a mean overhead of 4.3% on response time and 4.2% on throughput. APUS's protocol latency outperforms a recent fastest RDMA-based SMR protocol by 4.9x. APUS's protocol latency scales almost constantly to the number of concurrent requests and replicas. APUS is deployable: all source code and raw evaluation results are released at http://github.com/icdcs17-p256/apus.

I. INTRODUCTION

State machine replication (SMR) runs a program on several computer replicas and enforces same inputs for this program as long as a quorum majority of replicas still behave normally, tolerating various faults such as minor replicas failures and packet losses. To achieve this powerful fault-tolerance, SMR typically uses a distributed consensus protocol called PAXOS [52], [46], [45], [69]. Recent SMR systems [42], [35], [27] have greatly improved the availability of server programs that serve online requests and store important data.

Unfortunately, existing PAXOS protocols incur prohibitive performance overhead on server programs. For efficiency, PAXOS typically assigns one replica as the leader to invoke consensus requests, and the other replicas as backups to agree on requests. To agree on an input, at least one message round-trip is required between the leader and a backup. A round-trip causes big latency as it goes through TCP/IP layers such as OS kernel. This latency may be acceptable for leader election [21], [6] or heavyweight transactions [27], [42], but undesirable for key-value servers (e.g., `Redis` and `Memcached`).

As the number of concurrent requests or replicas increases, PAXOS consensus latency often increases linearly [33] due to the linearly increasing number of consensus messages. This limited scalability hurts the performance of server programs for two reasons. First, the performance of server programs is often scalable to number of CPU cores in a computer when serving concurrent client requests. Second, some advanced SMR systems (e.g., Azure [44]) deploy seven or nine replicas to handle replica failures or updates.

To improve PAXOS scalability, one approach is introducing parallel techniques such as multithreading [6], [19] or asynchronous IO [27], [65]. However, the high TCP/IP round-trip latency still exists, and synchronizations in these techniques frequently invoke expensive OS events such as context switches. We ran four parallel PAXOS protocols [6], [19], [27], [65] on a computer with 24 CPU cores and 40Gbps network, then we spawned 24 concurrent consensus requests. When the number of replicas increased from three to nine, the consensus latency of three protocols increased by 30.3% to 156.8%, and 36.5% to 63.7% of the increase was in OS kernel.

Another scalability approach is maintaining multiple instances of PAXOS, including batching requests [68], partitioning program states [33], [18], [55], splitting consensus leadership [50], [19], and hierarchical replication architecture [41], [33]. These systems have improved throughput. However, the core of these systems, PAXOS, still has an unscalable consensus latency. Prior work [33], [55], [41] explicitly desires a PAXOS protocol with a more scalable consensus latency.

To improve PAXOS performance, Remote Direct Memory Access (RDMA) becomes a promising solution as it becomes common in datacenters. RDMA not only bypasses OS kernel, but it also provides dedicated network hardware to achieve a fast round-trip. For instance, the fastest RDMA operation allows a process to directly write to a remote replica's process without involving the remote OS kernel or CPU ("one-sided" operation). Such a RDMA round-trip takes only about 3 μs [56].

However, due to the limited RDMA operation types, fully exploiting RDMA speed in software systems is widely considered challenging by the community [56], [40], [31], [63]. For instance, DARE [63], a recent fastest PAXOS protocol based on RDMA, presents a sole-leader,

two-round consensus: first, leader does RDMA writes consensus requests on each replica; second, leader does RDMA writes on each replica to update a global variable that points to the latest request. Unfortunately, such a global variable update *serializes* consensus requests: both DARE's and our evaluation (§VIII-B) confirmed that, as the number of concurrent requests increased, DARE's consensus latency increased almost linearly.

Our key observation is that we should carefully divide RDMA workloads among the leader and backups, especially in a scalability-sensitive context. Intuitively, we can let both leader and backups do RDMA writes directly on destination replicas' memory, and let all replicas poll their local memory to receive messages.

Although doing so will consume more CPU resources than a sole-leader protocol [63], it has two major benefits. First, both leader and backups participate in consensus, which makes it possible to reach consensus with only one round [52] without updating global variables. Second, all replicas now efficiently receive consensus messages on their local, bare metal memory. An analogy is threads receiving other threads' data via bare metal memory, a fast and scalable computation pattern.

We present APUS,[1] a new RDMA-based PAXOS protocol and its runtime system. In APUS, all replicas directly write to destination replicas' memory and poll messages from local memory to receive messages. Our runtime system handles other technical challenges such as atomic delivery of messages (§IV-A), efficient input logging (§VI-A), and failure recovery (§VI-B).

Similar to recent SMR systems [35], [27], APUS supports general, unmodified server programs. Within APUS, a program runs as is. APUS automatically deploys this program on replicas, intercepts inputs from the program's inbound socket calls (e.g., `recv()`), and invokes PAXOS to enforce same inputs across replicas.

We implemented APUS in Linux. APUS intercepts POSIX inbound socket calls (e.g., `accept()` and `recv()`) to coordinate inputs using the Infiniband RDMA architecture [1]. To help people inspect whether replicas run in sync, on top of APUS's PAXOS protocol, APUS provides an efficient network output checking protocol. To recover or add replicas, APUS leverages CRIU [26] to automatically, efficiently checkpoint a program without perturbing consensus in normal case.

We compared APUS with five popular, open source PAXOS-like implementations, including four TCP/IP-based ones (libPaxos [65], ZooKeeper [6], CRANE [27] and S-Paxos [19]), and an RDMA-based one (DARE [63]). We evaluated APUS on nine widely used or studied server programs, including 4 key-value stores (`Redis` [66], `Memcached` [54], `SSDB` [67], and `MongoDB` [57]), a SQL server `MySQL` [13], an anti-virus server `ClamAV` [24], a multimedia server `MediaTomb` [12], an LDAP server OpenLDAP [61], and a transactional database `Calvin` [68]. Evaluation shows that

[1]We name our system after apus, one of the fastest birds.

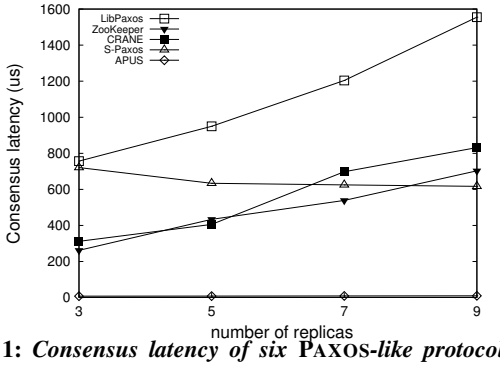

Fig. 1: ***Consensus latency of six* PAXOS*-like protocols.*** **All protocols ran with 24 concurrent proposing clients. Both X and Y axes are broken to fit in all these protocols.**

1. APUS is fast and scalable. Figure 1 shows that APUS's consensus latency outperforms four TCP/IP-based PAXOS protocols by up to 85.8x and DARE by 4.9x. APUS's consensus latency stays almost constant to the number of concurrent requests and replicas.
2. APUS achieves low overhead on diverse real-world server programs. We ran all nine server programs with seven replicas and compared to servers' own unreplicated executions at peak performance. In average, APUS incurred only 4.2% overhead on throughput and 4.3% on response time.
3. APUS is robust on replicas failures and packet losses. Its leader election latency was reasonable.

Our major contribution is the first RDMA-based PAXOS protocol that achieves low performance overhead on diverse server programs. APUS has the potential to largely improve both the scale and performance of many replication systems [44], [41], [27], [35], [18], [19]. For instance, Azure [44] deploys about seven replicas in each PAXOS group, and now it can enjoy much better performance even when serving more concurrent requests. Overall, a fast, scalable, and general SMR service, APUS can significantly promote the deployments of PAXOS and improve both the consistency and fault-tolerance of various systems within datacenters.

The remaining of this paper is organized as follows. §II introduces PAXOS and RDMA background. §III gives an overview of APUS. §IV presents APUS's consensus protocol with its runtime system. §V describes the network output checking protocol. §VI presents implementation details. §VII compares APUS protocol with DARE. §VIII presents evaluation results, §IX discusses related work, and §X concludes.

II. Background

A. Paxos

Paxos [69], [46], [45], [23], [47], [52] runs the same program and its data on a group of replicas and enforces a strongly consistent order of inputs across replicas. Because a consensus can be achieved as long as a majority of replicas agree, Paxos is well known for tolerating various faults, including minor replica failures and packet losses. If the leader replica fails, Paxos elects a new leader from the backups.

To handle replica failovers, standard Paxos must log inputs in local stable storage. When a new input comes, the Paxos leader writes this input in local stable storage. The leader then starts a new consensus round among replicas. A backup also writes the received consensus request in local storage if it agrees on this request. Since logging is done by each replica locally, it is scalable.

The consensus latency of Paxos protocols is notoriously high and unscalable [6], [33]. As datacenters incorporate faster networking hardware and more CPU cores, traditional Paxos protocols [65], [19], [27], [35], [6] are having fewer performance bottlenecks on network bandwidth and CPU resources.

However, software TCP/IP layers and OS kernels remain performance bottleneck [62]. To quantify this bottleneck, we evaluated four TCP/IP-based Paxos-like protocols on a computer with 24-cores, 40Gbps network, and we spawned 24 concurrent consensus clients. When changing the replica group size from three to nine, although network and CPUs were not saturate, the consensus latency of three protocols drastically increased by 30.3% to 156.8% (Figure 1), and 36.5% to 63.7% of this increase was in OS kernel. If only one consensus client was spawned, the latency increase on the number of replicas was more gentle (Table II).

This evaluation also shows that both the number of concurrent requests and replicas make Paxos latency increase drastically. This problem becomes worse as server programs tend to support more concurrent requests and advanced SMR systems such as Azure deploy seven to nine replicas [44] to handle replica updates.

B. RDMA

RDMA architectures (e.g., Infiniband [1] and RoCE [3]) become common in datacenters due to its ultra low latency, high throughput, and its decreasing prices. The ultra low latency of RDMA not only comes from its kernel bypassing feature, but also its dedicated network stack implemented in hardware. Therefore, RDMA is considered the fastest kernel bypassing technique [40], [56], [63]; it is several times faster than software-only kernel bypassing techniques (e.g., DPDK [2] and Arrakis [62]).

RDMA has three operation types, from fast to slow: one-sided read/write operations, two sided send/recv operations, and IPoIB (IP over Infiniband). IPoIB can run unmodified socket programs, but it is several times slower than the other two primitives. A one-sided RDMA write operation can directly write from one replica's memory to a remote replica's memory without involving the remote OS kernel or CPU. Prior work [56] shows that one-sided operations are up to 2x faster than two-sided operations, so APUS uses one-sided operations (or "WRITE" in this paper). On a WRITE succeeds, the remote NIC sends an RDMA ACK to local NIC.

A one-sided RDMA communication between a local and a remote NIC needs a Queue Pair (QP), including a send queue and a receive queue. Each QP has a Completion Queue (CQ) to store ACKs. A QP belongs to a type of "XY": X can be R (reliable) or U (unreliable), and Y can be C (connected) or U (unconnected). HERD [40] shows that WRITEs on RC and UC OPs incur almost same latency, so APUS uses RC QPs.

Normally, to ensure a WRITE resides in remote memory, the local replica normally busily polls an ACK from the CQ before it proceeds (or *signaling*). Polling ACK is time consuming as it involves synchronization between the NICs on both sides of a CQ. We looked into the ACK pollings in a fastest RDMA-based Paxos protocol DARE [63], and we found that, although DARE is highly optimized (its leader maintains one global CQ to receive all backups' ACKs in batches), polling ACKs is still time consuming: when the CQ was empty, it took 0.039$\sim$0.12 μs; when the CQ has one or more ACKs, it took 0.051$\sim$0.42 μs.

Fortunately, depending on protocol logic, one can do *selective signaling* [40]: it only checks for an ACK after pushing a number of WRITEs. Because APUS's protocol logic does not rely on RDMA ACKs, it just occasionally invokes selective signaling to clean up ACKs.

III. APUS Overview

APUS follows a typical SMR deployment scenario: it runs replicas of a server program in a datacenter. Replicas connect with each other using RDMA QPs. Client programs located in LAN or WAN. The APUS leader handles client requests and runs its RDMA-based protocol to coordinate inputs across replicas.

Figure 2 shows APUS's architecture. APUS intercepts a server program's inbound socket calls (e.g., `recv()`) using a Linux technique called LD_PRELOAD. APUS involves four key components: a Paxos consensus protocol for input coordination (in short, the *coordinator*), an output checking protocol (the *checker*), a circular in-memory consensus log (the *log*), and a guard process that handles checkpointing and recovering a server's process state and file system state (the *guard*).

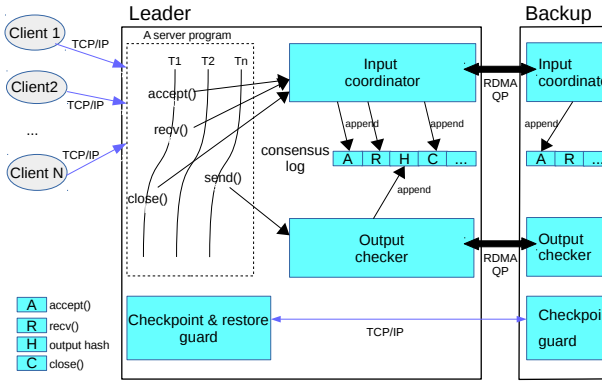

Fig. 2: APUS *Architecture (key components are in blue).*

The coordinator is invoked when a server program thread calls an inbound socket call to manage a client socket connection (e.g., `accept()` and `close()`) or to receive inputs from the connection (e.g., `recv()`). On the leader side, APUS executes the actual Libc socket call, extracts the returned value or inputs of this call, stores it in local SSD, appends a log entry to its local consensus log, and then invokes the coordinator for a new consensus request on "executing this socket call".

The coordinator runs a consensus algorithm (§IV), which WRITEs the local entry to backups' remote logs in parallel and polls the local log entry to wait quorum. When a quorum is reached, the leader thread simply finishes intercepting this call and continues with its server execution. As the leader's server threads execute more calls, APUS enforces the same consensus log and thus the same socket call sequence across replicas.

On each backup side, the coordinator uses a APUS internal thread called *follower* to poll its consensus log for new consensus requests. If the coordinator agrees the request, the follower stores the log entry in local SSD and then WRITEs a consensus reply to the remote leader's corresponding log entry. A backup does not need to intercept a server's socket calls because the follower will just follow the leader's consensus requests on executing what socket calls and then forward these calls to its local server program.

The output checker is occasionally invoked as the leader's server program executes outbound socket calls (e.g., `send()`). For every 1.5KB (MTU size) of accumulated outputs per connection, the checker unions the previous hash with current outputs and computes a new CRC64 hash. After a fixed number of hashes are generated, the checker then invokes consensus across replicas, which compares the hash at its global hash index on the leader side.

This output consensus is based on the input consensus algorithm (§IV) except that backups carry their hash at the same hash index back to the leader. For this particular output consensus, the leader first waits quorum. It then waits for a few μs in order to collect more remote hashes. It then compares remote hashes it has.

If a hash divergence is detected, the leader optionally invokes the local guard to forward a "rollback" command to the diverged replica's guard. The diverged replica's guard then rolls back and restores the server program to a latest checkpoint before the last successful output check (§V). The replica then restores and re-executes socket calls to catch up. Because output hash generations are fast and an output consensus is invoked occasionally, our evaluation didn't observe performance impact on this checker.

IV. THE RDMA-BASED PAXOS PROTOCOL

This section presents APUS's consensus protocol with its runtime system, including the RDMA-based consensus algorithm in normal case (§IV-A), handling concurrent connections (§IV-B), leader election (§IV-C), and reliability guarantees (§IV-D).

A. Normal Case Algorithm

Recall that APUS' input consensus protocol contains three roles. First, the PAXOS consensus log (§III). Second, a leader replica's server program thread (in short, a leader thread) which invokes consensus request. For efficiency, APUS lets a server program's threads directly handle consensus requests whenever they call inbound socket calls (e.g., `recv()`). Third, a backup replica's APUS internal follower thread (§III) which agrees on or rejects consensus requests.

```
struct log_entry_t {
  consensus_ack reply[MAX]; // Per replica consensus reply.
  viewstamp_t vs;
  viewstamp_t last_committed;
  int node_id;
  viewstamp_t conn_vs; // client connection ID.
  int call_type; // socket call type.
  size_t data_sz; // data size in the call.
  char data[0]; // data, with a canary value in the last byte.
} log_entry;
```

Fig. 3: APUS*'s log entry for each socket call.*

Figure 3 shows the format of a log entry in APUS's consensus log. Most fields are regular as those in a typical PAXOS protocol [52] except three ones: the `reply` array, the client connection ID `conn_vs`, and the type ID of a socket call `call_type`. The `reply` array is for backups to WRITE their consensus replies to the leader. The `conn_vs` is for identifying which connection this socket call belongs to (see IV-B). The `call_type` identifies four types of socket calls in APUS: the `accept()` type (e.g., `accept()`), the `recv()` type (e.g., `recv()` and `read()`), the `send()` type (e.g., `send()`), and the `close()` type (e.g., `close()`).

Figure 4 shows the input consensus algorithm. Suppose a leader thread invokes a consensus request when it calls a socket call with the `recv()` type. A consensus

request includes four steps. The first step (**L1**) is executing the actual Libc socket call, because APUS needs to get the actual return values or received data bytes of this call and then replicates them in remote replicas' logs.

The second step (**L2**) is local preparation, including assigning a global viewstamp to locate this entry in the consensus log, building a log entry structure for this call, and writing this entry to a local parallel logging storage on SSD (§VI-A). Then, APUS invokes consensus for each incoming request (entry) concurrently.

The third step (**L3**) is to WRITE a log entry to remote backups in parallel. Unlike a previous RDMA-based consensus algorithm [63] which has to wait for ACKs from remote NICs, our WRITE immediately returns after pushing the entry to its local QP between the leader and each backup, because PAXOS has handled the reliability issues (e.g., packet losses) for our WRITEs. In our evaluation, pushing a log entry to local QP took no more than 0.3 μs. Therefore, the WRITEs to all backups are done in parallel (see **L3** in Figure 3).

The fourth step (**L4**) is the leader thread polling on its `reply` field in its local log entry for backups' consensus replies. Once consensus is reached, the leader thread finishes intercepting this `recv()` socket call and continues with its server application logic.

On a backup side, one tricky synchronization issue is that an efficient way is needed to make the leader's RDMA WRITEs and backups' polls atomic. For instance, while a leader thread is doing a WRITE on `vs` to a remote backup, the backup's follower thread may be reading `vs` concurrently, causing a corrupted read value.

To address this issue, one existing approach [30], [40] leverages the left-to-right ordering of RDMA WRITEs and puts a special non-zero variable at the end of a fix-sized log entry because they mainly handle key-value stores with fixed value length. As long as this variable is non-zero, the RDMA WRITE ordering guarantees that the log entry WRITE is complete. However, because APUS aims to support general server programs with largely variant received data lengths, this approach cannot be applied in APUS.

Another approach is using atomic primitives provided by RDMA hardware, but a prior evaluation [70] has shown that RDMA atomic primitives are much slower than normal RDMA WRITEs and local memory reads.

APUS tackles this issue by adding a canary value after the actual `data` array. Because APUS uses a QP with the type of RC (reliable connection) (§II), the follower always first checks the canary value according to `data_size` and then starts a standard PAXOS consensus reply decision [52]. Our efficient, synchronization-free approach guarantees that the follower always reads a complete log entry.

A follower thread in a backup replica polls from the

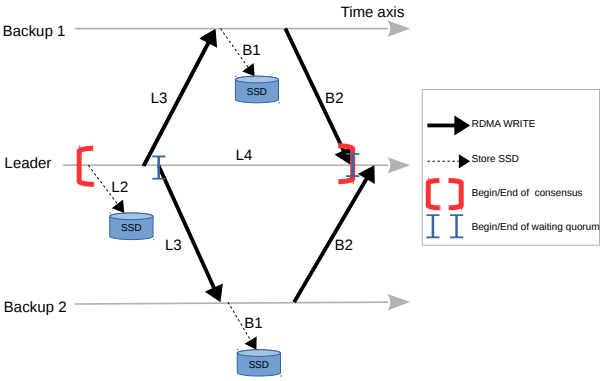

Fig. 4: APUS *consensus algorithm in normal case.*

latest un-agreed log entry and does three steps to agree on consensus requests, shown in Figure 4. First (**B1**), it does a regular PAXOS view ID checking to see whether the leader is up-to-date, it then stores the log entry in its local SSD. Second (**B2**), it does a WRITE to send back a consensus reply to the leader's `reply` array element according to its own node ID. Backups perform these two steps in parallel (see Figure 3).

Third (**B3**, not shown in Figure 4), the follower does a regular PAXOS check on `last_committed` and executes all socket calls that it has not executed before this viewstamp. It then "executes" each log entry by sending the socket calls to the local server program.

B. Handling Concurrent Connections

Unlike traditional PAXOS protocols which mainly handle single-threaded programs due to the deterministic state machine assumption in SMR, APUS aims to support both single-threaded as well as multithreaded server programs running on multi-core machines. Therefore, a strongly consistent mechanism is needed to map every concurrent client connection on the leader and to its corresponding connection on backups. A naive approach could be matching a leader connection's socket descriptor to the same one on a backup, but backups' servers may return nondeterministic descriptors due contentions on systems resources.

Fortunately, PAXOS already makes viewstamps [52] of socket calls strongly consistent across replicas. For TCP connections, APUS adds the `conn_vs` field, the viewstamp of the the first socket call in each connection (i.e., `accept()`) as the connection ID for log entries. Then, APUS maintains a hash map on each local replica to map this connection ID to local socket descriptors.

C. Leader Election

Compared to traditional PAXOS leader election protocols, RDMA-based leader election poses one main issue caused by RDMA. Because backups do not communicate frequently with each other in normal case, thus a backup does not know the remote memory locations where the

other backups are polling. Writing to a wrong remote memory location may cause the other backups to miss all leader election messages. An existing system [63] establishes an extra control QP with extra remote memory to handle leader election, posing more complexity via the extra communication channels.

APUS addresses this issue with a simple, clean approach. It runs a leader election with the same consensus log and the same QP. In normal case, the leader does WRITEs to remote logs as heartbeats with a period of T. Each consensus log maintains a control data structure called `elect[MAX]`, one element for each replica. Normal case operations and heartbeats use the other parts of the consensus log but leave this `elect` array alone. Once backups have not received heartbeats from the leader for a period of 3*T, they start to elect a new leader and let their follower threads poll from the `elect` array.

Backups start a standard PAXOS leader election algorithm [52] with three steps. Each replica writes to its own `elect` element at remote replicas. First, backups propose a new view with a standard two-round PAXOS consensus [45] by including both the view and the index of the latest log entry. The other backups also propose their views and poll on this array in order to follow other proposals or confirm itself as the winner. The backup whose log is more up-to-date will win. A log is more up-to-date if its latest entry has either a higher view or the same view but a higher index.

Second, the winner proposes itself as a leader candidate using this array, another two-round PAXOS consensus. Third, after the second step reaches a quorum, the new leader notifies remote replicas itself as the new leader and it starts to WRITE periodic heartbeats.

D. Reliability Guarantee

To minimize protocol-level bugs, APUS's protocol derives from viewstamp-based protocol [52]. We made this design choice because PAXOS is notoriously difficult to understand [59], [45], [46], [69], implement [23], [52], or verify [72], [34]. Deriving from a viewstamp-based protocol [52] helps us incorporate these readily mature understanding, engineering experience, and the theoretically verified safety rules into our protocol.

Although APUS's PAXOS protocol works on a RDMA network, the reliability of APUS does not rely on a lossless RDMA. APUS still provides same fault-tolerance guarantee as the standard PAXOS model, where a stable storage exists, but the hardware (e.g., network devices) of replicas may fail, and server programs may crash.

V. OUTPUT CHECKING PROTOCOL

Most server programs are multithreaded and they may run into nondeterminism (e.g., concurrency errors [49]), which may cause replicas to diverge. APUS provides a fast output checking protocol for a practical purpose: improving APUS users' assurance on whether replicas run in sync. If diverged replicas are detected, users can restore them (§VI-B).

A main technical challenge for comparing outputs across replicas is that network outputs and their physical timings are miscellaneous. For example, when we ran `Redis` simply on pure SET workloads, we found that different replicas reply the numbers of "OK" replies for SET operations randomly: one replica may send four of them in one `send()` call, while another replica may only send one of them in each `send()` call. Therefore, comparing outputs on each `send()` call among replicas may not only yield wrong results, but may slow down server programs among replicas.

To tackle this challenge, APUS presents a bucket-based hash computation mechanism. When a server calls a `send()` call, APUS puts the sent bytes into a local, per-connection bucket with 1.5KB (MTU size). Whenever a bucket is full, APUS computes a new CRC64 hash on a union of the current hash and this bucket. Such a hash computation mechanism encodes accumulated network outputs. Then, for every T_{comp} (by default, 10K in APUS) local hash values are generated, APUS invokes the output checking protocol once to check this hash across replicas. Because this protocol is invoked rarely, it did not incur observable performance lost in our evaluation.

To compare a hash across replicas, APUS's output checking protocol runs the same as the input coordination protocol (§IV-A) except that the follower thread on each backup replica carries this hash value in the `reply` written back into the leader's corresponding log entry.

VI. IMPLEMENTATION DETAILS

A. Parallel Input Logging

To handle replica fail-overs, a standard PAXOS protocol should provide a persistent input logging storage. APUS uses the PAXOS viewstamp of each input as key and its input data as value. APUS stores this key-value pair in Berkeley DB (BDB) with a BTree access method [16], as we found this method fastest in evaluation.

However, if more inputs are inserted, the BTree height will increase, which will cause the key-value insertion latency to largely increase.

To handle this issue, we implemented a parallel logging approach [17]: instead of maintaining a single BDB store, we maintain an array of BDB stores. We use an index to indicate the current active store and insert new inputs. Once the number of insertions reach a threshold, we move the index to the next empty store in the array and recycle preceding stores. This implementation made APUS logging latency efficient: 2.8$\sim$8.7 μs (§VIII-C).

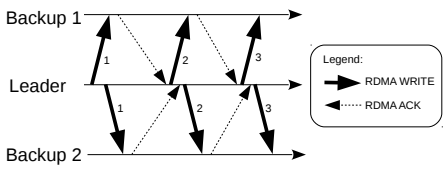

Fig. 5: ***DARE's RDMA-based protocol.*** **It is a sole-leader, two-round protocol with three steps: (a) the leader WRITEs a consensus request to all backups' consensus logs and waits for ACKs to check if they succeed; (b) for the successful backups in (a), leader does WRITEs to update tail pointer of their consensus logs; and (c) on receiving a majority of ACKs in (b), a consensus is reached, leader does WRITEs to notify backups.**

B. Checkpoint and Restore

We proactively design APUS's checkpoint mechanism to incur little performance impact in normal case. A checkpoint operation is invoked periodically in one backup replica, so the leader and other backups can still reach consensus on new inputs rapidly.

A guard process is running on each replica to checkpoint and restore the local server program. It assigns one backup replica's guard to checkpoint the local server program's process state and file system state of current working directory within a one-minute duration.

Such a checkpoint operation and its duration are not sensitive to normal case performance because the other backups can still reach quorum rapidly. Each checkpoint is associate with a last committed socket call viewstamp of the server program. After each checkpoint, the backup dispatches the checkpoint zip file to the other replicas.

Specifically, APUS leverages CRIU [26], a popular, open source tool, to checkpoint a server program's process state (e.g., CPU registers and memory). Since CRIU does not support checkpointing RDMA connections, APUS's guard first sends a "close RDMA QP" request to an APUS internal thread, lets this thread closes all remote RDMA QPs, and then invokes CRIU.

VII. COMPARING APUS WITH DARE

DARE [63] (Figure 5) is one of the fastest PAXOS protocols. It is RDMA-based and most relevant to APUS. DARE is designed for both a small number of concurrent requests and replicas. DARE follows a sole-leader manner with two-rounds: first, leader does RDMA writes consensus requests on each replica; second, leader does RDMA writes on each replica to update a global variable that points to the latest request (tail of consensus log) in each backup. Both rounds are essential in DARE to incase a backup becomes a new leader.

DARE is not designed to work with large concurrent requests or replicas for two reasons. First, its second round needs to update a global variable for each replica, which *serializes* concurrent consensus requests, a essential feature for PAXOS performance [52]. For instance, two ongoing DARE consensus requests may interleave and cause the variable to point to an earlier request. Therefore, the consensus of DARE's new requests can not start until the consensus of prior requests finish, confirmed in both DARE's and our evaluation (§VIII-B). Second, a sole-leader protocol can not incorporate a stable storage or checkpoint design. Therefore, DARE lacks durability (§II), another essential PAXOS feature.

Overall, APUS differs from DARE in three aspects. First, APUS's protocol has only one RDMA round (Figure 4), and DARE has two rounds. Second, APUS scales well on concurrent client connections and replicas (§VIII-B), and DARE [63] mentioned that their design choices do not include scalability. Third, although APUS is a durable protocol and DARE is a volatile one, APUS is faster than DARE by up to 4.9x. §VIII-B compares APUS and DARE performance in detail.

VIII. EVALUATION

Our evaluation machines include nine RDMA-enabled, Dell R430 servers as PAXOS replicas. Each server has Linux 3.16.0, 2.6 GHz Intel Xeon CPU with 24 hyper-threading cores, 64GB memory, and 1TB SSD. All NICs are Mellanox ConnectX-3 Pro 40Gbps connected with Infiniband [1]. The `ping` latency between every two replicas is 84 μs (the IPoIB round-trip latency).

Our evaluation machines also include one Dell R320 server for client programs. It has Linux 3.16.0, 2.2GHz Intel Xeon 12 hyper-threading cores, 32GB memory, and 160GB SSD. To mitigate latency of client requests, this client machine is located at the same LAN as the RDMA replicas with a 1Gbps NIC. The average `ping` latency between this machine and a RDMA replica is 250 μs. Note that which machines to hold clients do not affect any PAXOS protocol's consensus latency (it is only affected by the RDMA network among replicas).

We compared APUS with five popular, open source PAXOS-compatible implementations, including four TCP/IP-based ones (libPaxos [65], ZooKeeper [6], CRANE [27] and S-Paxos [19]) and an RDMA-based one (DARE [63]). S-Paxos is designed to achieve scalable throughput when more replicas are added.

We evaluated APUS on nine widely used or studied server programs, including 4 key-value stores `Redis`, `Memcached`, `SSDB`, `MongoDB`; `MySQL`, a SQL server; `ClamAV`, an anti-virus server that scans files and delete malicious ones; `MediaTomb`, a multimedia storage server that stores and transcodes video and audio files; OpenLDAP, an LDAP server; `Calvin`, a widely studied transactional database system. All these programs are multithreaded except `Redis` (but it can serve concurrent requests via Libevent). These servers all update or store important data and files, thus the strong PAXOS fault-tolerance is especially attractive to these programs.

Table I introduces the benchmarks and workloads we used. We used the protocol or program developers' own performance benchmarks or popular third-party benchmarks. For benchmark workload settings, we used the benchmarks' default workloads whenever available. To perform a stress testing on APUS's input consensus protocol, we chose workloads with significant portions of writes, because write operations often contain more input bytes than reads (e.g., a key-value SET operation contains more bytes than a GET).

Program	Benchmark	Workload/input description
`ClamAV`	clamscan [8]	Files in `/lib` from a replica
`MediaTomb`	ApacheBench [11]	Transcoding videos
`Memcached`	mcperf [7]	50% set, 50% get operations
`MongoDB`	YCSB [10]	Insert operations
`MySQL`	Sysbench [9]	SQL transactions
OpenLDAP	Self	LDAP queries
`Redis`	Self	50% set, 50% get operations
`SSDB`	Self	Eleven operation types
`Calvin`	Self	SQL transactions

TABLE I: *Benchmarks and workloads.* "Self" in the Benchmark column means we used a program's own performance benchmark program. Workloads are all concurrent.

The rest of this section focuses on these questions:

§VIII-A: How does APUS performance compare to TCP/IP-based PAXOS protocols?

§VIII-B: How does APUS performance compare to DARE?

§VIII-C: What is the performance overhead of running APUS with server programs? How does it scale with the number of concurrent requests?

§VIII-D: How fast is APUS on handling checkpoints and electing a new leader?

A. Comparing with TCP/IP-based PAXOS

A common practice in PAXOS evaluation [63], [48], when comparing APUS with other PAXOS protocols, we ran APUS with a popular key value store `Redis`. To stress APUS on our 24-core machines, we spawned 24 concurrent requests for all six protocols, a common high concurrent value in prior evaluation [6], [27], [35]. Our evaluation also showed that most server programs reached peak throughput before 16 requests (§VIII-C).

All four TCP/IP-based protocols were run on IPoIB (§II-B). Figure 1 shows that the consensus latency of three traditional protocols increased almost linearly to the number of replicas (except S-Paxos). S-Paxos batches requests from replicas and invokes consensus when the batch is full. More replicas can take shorter time to form a batch, so S-Paxos incurred a slightly better consensus latency with more replicas. Nevertheless, its latency was always over 600 μs. APUS's consensus latency outperforms these four protocols by 32.3x to 85.8x.

To understand the scalability bottleneck in these four protocols, we spawned only one client and inspected the micro events in their protocols (Table II). From three to nine replicas, the consensus latency (the "Latency" column) of these protocols increased more gently than that on 24 concurrent clients. For instance, when the number of replicas increased from three to nine, ZooKeeper latency increased by 30.3% with one client; this latency increased by 168.3% with 24 clients (Figure 1). This indicates that concurrent consensus requests are the major scalability bottleneck for these protocols.

Specifically, three protocols had scalable latency on the arrival of their first consensus reply (the "First" column), which implies that network is not saturate. libPaxos is an exception because its two-round protocol consumed much bandwidth. However, there is a big gap between the arrival of the first consensus reply and the "majority" reply (the "Major" column). Given that the replies' CPU processing time was small (the "Process" column), we can see that various systems layers, including OS kernels, network libraries, and language runtimes (e.g., JVM), are another major scalable bottleneck (the "Sys" column). This indicates that RDMA is useful on bypassing these systems layers.

Note that on three replicas, libPaxos and CRANE's proposing leader and acceptors are in different threads, so they two had different "First" and "Major" arrival times. CRANE and S-Paxos's proposing leader itself is just an acceptor, so they two had same "First" and "Major" arrival times (i.e., their "Sys" times were 0).

Proto-#Rep	Latency	First	Major	Process	Sys
libPaxos-3	81.6	74.0	81.6	2.5	5.1
libPaxos-9	208.3	145.0	208.3	12.0	51.3
ZooKeeper-3	99.0	67.0	99.0	0.84	31.2
ZooKeeper-9	129.0	76.0	128.0	3.6	49.4
CRANE-3	78.0	69.0	69.0	13.0	0
CRANE-9	148.0	83.0	142.0	30.0	35.0
S-Paxos-3	865.1	846.0	846.0	20.0	0
S-Paxos-9	739.1	545.0	731.0	35.0	159.1

TABLE II: *Performance breakdown of TCP/IP-based* PAXOS *protocols with only one client.* The "Proto-#Rep" column means the protocol name and replica group size; "Latency" means the consensus latency; "First" means the latency of its first consensus reply; "Major" means the latency of its the majority reply; "Process" means time spent in processing all replies; and "Sys" means time spent in systems (OS kernel, network libraries, and JVM) between the "First" and the "Major" reply. All times are in μs.

B. Comparing with DARE

We compared APUS and DARE [63] on key-value servers with same requests. APUS ran a widely used one, `Redis`; DARE supported a 335-line, RDMA-based key-value server written by their authors. To thoroughly analyze their latency with scalability, we ran up to seven replicas and 24 clients.

Figure 6 shows the consensus latency of APUS and DARE on seven replicas with randomly arriving, update-heavy (50% SETs and 50% GETs) and read-heavy (10% SETs and 90% GETs) workloads. DARE performance on

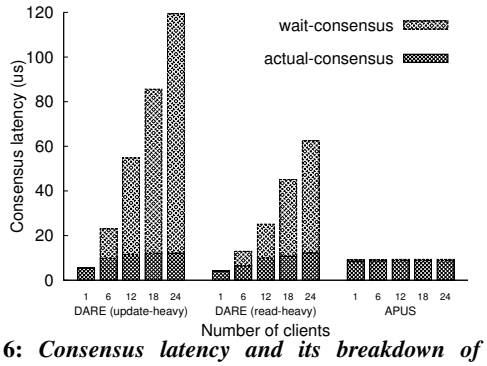

Fig. 6: ***Consensus latency and its breakdown of* APUS *and DARE.*** **The number of replicas is seven. Consensus latency contains two parts: "Wait-time" means the duration between the time a request being received by a server program and the time a consensus for this request starts. "Consensus-time" means the actual duration for consensus.**

these two workloads were different because it handles GETs with only one consensus round [63]. APUS handles all requests with the same protocol. When there was only one client, APUS was slightly slower than DARE because DARE does not store inputs persistently. On 6 to 24 requests, APUS was 87.9% to 763.4% faster than DARE due to two reasons.

First, APUS is a one-round protocol and DARE is a two-round protocol (for SETs), so DARE's actual consensus time was 53.2% higher than APUS. Even comparing DARE's read-heavy workloads (one-round for GETs) with APUS on more concurrent requests, APUS's actual consensus time was still slightly faster than DARE's because APUS's protocol avoids expensive ACK pollings (§II-B).

Second, DARE's second consensus round updates a global variable in remote backups, which serializes ongoing consensus requests (§VII). Although DARE compensates this limitation by batching same SET or GET types, the randomly arrival of requests often make batches small, causing a large wait duration (a new batch can not start consensus until prior batches reach consensus). DARE's evaluation [63] confirmed a high wait duration: with three replicas and nine concurrent clients, DARE's throughput on real-world inspired workloads (50% SET and 50% GET arriving randomly) was 43.5% lower than that on 100% SET workloads. DARE's evaluation also showed that its throughput dropped by 30.1% when the number of replicas increased from three to seven.

Overall, these results suggest that DARE is better on smaller number of concurrent requests and replicas (e.g., leader election [21], [6]), and APUS is better on larger number of concurrent requests or replicas (e.g., replicating server programs [35], [27]).

C. Performance Overhead

To stress APUS, we used a large replica group size of 9 to run all server programs. We spawned up to 32 concurrent connections, and then we measured both response time and throughput. We also measured APUS's bare consensus latency. Each performance data point was taken from a mean value of 10 executions.

APUS ran with nine evaluated programs without modifying them except `Calvin`. `Calvin` integrates its client program and server program within the same process and uses local memory to let these two programs talk. To make `Calvin`'s client and server communicate with POSIX sockets so that APUS can intercept the server's inputs, we wrote a 23-line patch for `Calvin`.

We turned on and off the output checking (§V) and didn't observe difference in APUS performance. Only three programs (`MediaTomb`, `MySQL`, and OpenLDAP) have different output hashes cause by physical times.

Figure 7 shows APUS's throughput. We varied the number of concurrent client connections for each server program by from one to 32 threads. For `Calvin`, we only collected the 8-thread result because `Calvin` uses this constant thread count in their code to serve client requests.

Overall, compared to these server programs' unreplicated executions, APUS merely incurred a mean throughput overhead of 4.2% (note that in Figure 7, the Y-axises of most programs start from a large number). As the number of threads increases, all programs' unreplicated executions got a performance improvement except `Memcached`. A prior evaluation [35] also observed a similar `Memcached` low scalability. APUS scaled almost as well as the unreplicated executions.

APUS achieves such a low overhead in both throughput and response time mainly because of two reasons. First, for each `recv()` call in a server, APUS's input coordination protocol only contains two one-sided RDMA writes and two efficient local SSD writes (§VI-A) for the leader and each backup.

Program	# Calls	Input	SSD time	Quorum time
`ClamAV`	30,000	37.0	7.9 μs	10.9 μs
`MediaTomb`	30,000	140.0	5.0 μs	17.4 μs
`Memcached`	10,016	38.0	4.9 μs	7.0 μs
`MongoDB`	10,376	490.6	7.8 μs	9.2 μs
`MySQL`	10,009	28.8	5.1 μs	7.8 μs
OpenLDAP	10,016	27.3	5.5 μs	6.4 μs
`Redis`	10,016	40.5	2.8 μs	6.3 μs
`SSDB`	10,016	47.0	3.0 μs	6.2 μs
`Calvin`	10,002	128.0	8.7 μs	10.8 μs

TABLE III: ***Leader's input consensus events per 10K requests, 8 threads.*** **The "# Calls" column means the number of socket calls that went through APUS input consensus; "Input" means average bytes of a server's inputs received in these calls; "SSD time" means the average time spent on storing these calls to stable storage; and "Quorum time" means the average time spent on waiting quorum.**

To understand APUS's performance overhead, we collected the number of socket call events and consensus durations on the leader side. Table III shows these statistics per 10K requests, 8 or max (if less than 8) threads. According to the consensus algorithm steps in

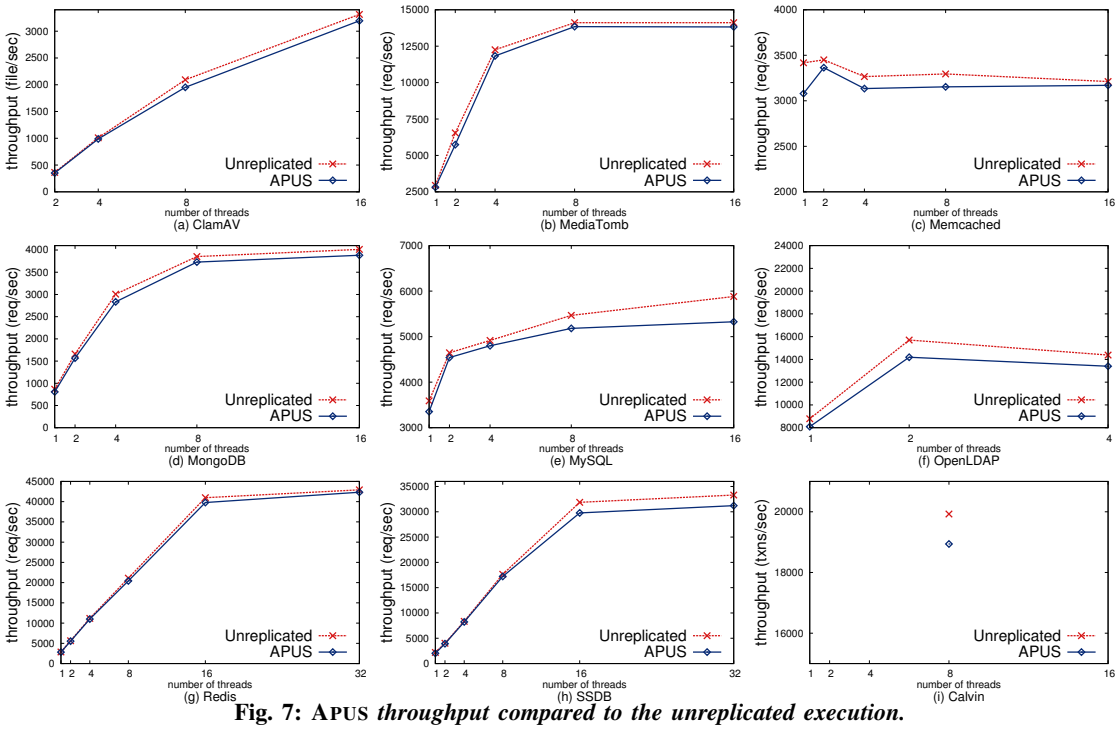

Fig. 7: APUS *throughput compared to the unreplicated execution.*

Figure 4, for each socket call, APUS's leader does an "L2": SSD write (the "SSD time" column in Table III) and an "L4": quorum waiting phase (the "quorum time" column). L4 implies backups' performance because each backup stores the proposed socket call in local SSD and then WRITEs a consensus reply to the leader.

By adding the last two columns in Table III, a APUS input consensus took only 9.1 μs (`Redis`) to 22.4 μs (`MediaTomb`). APUS's small consensus latency makes it achieve reasonable throughputs in Figure 7. Overall, Figure 6 and Table III indicate that APUS has low overhead on server programs' response time. APUS's mean overhead on response time was 4.3%. Due to space limit, the response time overhead figure is put here [14].

D. Checkpoint and Recovery

We ran the same performance benchmark as in §VIII-C and measured programs' checkpoint timecost. Each APUS periodic checkpoint operation (§VI-B) cost 0.12s to 11.6s on the evaluated server programs, depending on the amount of modified memory and files in the server programs since their own last checkpoint. `ClamAV` incurred the largest checkpoint time (11.6s) because it loaded and scanned files in a `/lib` directory.

Checkpoint operations did not affect APUS's performance in normal case because they were done on only one backup. The leader and other backups still formed majority and reached consensus rapidly.

To evaluate APUS's PAXOS recovery feature, we ran APUS with `Redis` and manually killed one backup, and we did not observe a performance change in the benchmark runs. We then manually killed the APUS leader and measured the latency of our RDMA-based leader election with three rounds (§IV-C). Figure IV shows APUS's election latency from three to eleven replicas. Because PAXOS leader election is rarely invoked in practice, although APUS's election latency was slightly higher than its normal case consensus latency, we considered it reasonable.

# Replicas	3	5	7	9
Election latency (μs)	10.7	12.0	12.8	13.5

TABLE IV: APUS*'s latency on on leader election.*

IX. RELATED WORK

Software-based consensus. There are a rich set of PAXOS algorithms [52], [46], [45], [69], [58] and implementations [23], [52], [21], [27]. PAXOS is notoriously difficult to be fast and scalable [55], [41], [33]. Since consensus protocols play a core role in datacenters [73], [36], [5] and worldwide distributed systems [25], [50], a variety of study have been conducted to improve specific aspects of consensus, including order commutativity [58], [51], understandability [59], [46], and verifiable reliability [72], [34]. Recent systems [20], [53], [15] extend PAXOS to tolerate byzantine faults [22], [43].

Three SMR systems, Eve [42], Rex [35], and CRANE [27], use TCP/IP-based PAXOS protocols to improve the availability of server programs. Evaluation in these systems shows that SMR services incur modest overhead on server programs' throughput compared to unreplicated executions. None of these three systems evaluate their response time overhead on key-value stores which are sensitive on latency. APUS is the first SMR

system that achieves low overhead on both response time and throughput on real-world key-value stores.

Hardware- or Network- assisted consensus. Recent systems [38], [29], [37], [64], [48] leverage augmented network hardware or topology to improve PAXOS consensus latency. Three systems [38], [29], [37] implement consensus protocols in network devices (e.g., switches). "Consensus in a Box" [38] implemented ZooKeeper's protocol in FPGA. These systems are suitable on maintaining compact metadata. However, as mentioned in prior work [48], these systems' hardware may not be sufficient to store large amount of replicated states (e.g., server programs' continuously arriving inputs).

Speculative Paxos [64] and NOPaxos [48] leverage the synchrony feature of datacenter topology to order requests, so they can eliminate consensus rounds if packets are not reordered or lost. If packets are lost or reordered, they invoke consensus to rescue. These two systems are not designed for scalability because when the number of concurrent requests or replicas increase, the probability of reordered or lost packets will increase. Moreover, these two systems' consensus modules go through TCP/IP layers and incur high consensus latency, and APUS can help them.

RDMA-based systems. RDMA techniques have been implemented in various architectures, including Infiniband [1], RoCE [3], and iWRAP [4]. RDMA have been leveraged in many systems to improve application-specific latency and throughput, including high performance computing [32], key-value stores [56], [40], [30], [39], transactional processing systems [70], [31], and file systems [71]. For instance, FaRM [30] leverages RDMA to build a fast DHT. FaRM uses a data replication approach [60], which works in a primary-backup manner [28]. In general, PAXOS provides better consistency and availability than primary-backup. These RDMA-based systems use RDMA to improve performance in different aspects, so they are complementary to APUS.

X. CONCLUSION

We have presented APUS, a new RDMA-based PAXOS protocol and its runtime system. Evaluation on 5 PAXOS protocols and 9 widely used programs shows that APUS is fast, scalable, and robust. It has the potential to greatly improve fault-tolerance of real-world programs. APUS is deployable: all source code, benchmarks, and raw evaluation results are available at http://github.com/icdcs17-p256/apus.

REFERENCES

[1] An Introduction to the InfiniBand Architecture. http://buyya.com/superstorage/chap42.pdf.

[2] Data Plane Development Kit (DPDK). http://dpdk.org/.

[3] Mellanox Products: RDMA over Converged Ethernet (RoCE). http://www.mellanox.com/page/products_dyn?product_family=79.

[4] RDMA iWARP. http://www.chelsio.com/nic/rdma-iwarp/.

[5] Why the data center needs an operating system. http://radar.oreilly.com/2014/12/why-the-data-center-needs-an-operating-system.html.

[6] ZooKeeper. https://zookeeper.apache.org/.

[7] A tool for measuring memcached server performance. https://github.com/twitter/twemperf, 2004.

[8] clamscan - scan files and directories for viruses. http://linux.die.net/man/1/clamscan, 2004.

[9] SysBench: a system performance benchmark. http://sysbench.sourceforge.net, 2004.

[10] Yahoo! Cloud Serving Benchmark. https://github.com/brianfrankcooper/YCSB, 2004.

[11] ab - Apache HTTP server benchmarking tool. http://httpd.apache.org/docs/2.2/programs/ab.html, 2014.

[12] MediaTomb - Free UPnP MediaServer. http://mediatomb.cc/, 2014.

[13] MySQL Database. http://www.mysql.com/, 2014.

[14] Apus reponse time overhead on nine server programs. http://github.com/icdcs17-p256/extra-figures/latency-overhead.pdf, 2016.

[15] B. Balasubramanian and V. K. Garg. Fault tolerance in distributed systems using fused state machines. *Distrib. Comput.*, 2014.

[16] http://www.sleepycat.com.

[17] A. Bessani, M. Santos, J. a. Felix, N. Neves, and M. Correia. On the efficiency of durable state machine replication. In *Proceedings of the USENIX Annual Technical Conference (USENIX '13)*, 2013.

[18] C. E. Bezerra, F. Pedone, and R. V. Renesse. Scalable state-machine replication. In *Proceedings of the 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, DSN '14, 2014.

[19] M. Biely, Z. Milosevic, N. Santos, and A. Schiper. S-paxos: Offloading the leader for high throughput state machine replication. In *Proceedings of the 2012 IEEE 31st Symposium on Reliable Distributed Systems*, SRDS '12, 2012.

[20] Y. Brun, G. Edwards, J. Y. Bang, and N. Medvidovic. Smart redundancy for distributed computation. In *Proceedings of the 2011 31st International Conference on Distributed Computing Systems*, ICDCS '11, 2011.

[21] M. Burrows. The chubby lock service for loosely-coupled distributed systems. In *Proceedings of the Seventh Symposium on Operating Systems Design and Implementation (OSDI '06)*, pages 335–350, 2006.

[22] M. Castro and B. Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99)*, Oct. 1999.

[23] T. D. Chandra, R. Griesemer, and J. Redstone. Paxos made live: An engineering perspective. In *Proceedings of the Twenty-sixth Annual ACM Symposium on Principles of Distributed Computing (PODC '07)*, Aug. 2007.

[24] http://www.clamav.net/.

[25] J. C. Corbett, J. Dean, M. Epstein, A. Fikes, C. Frost, J. J. Furman, S. Ghemawat, A. Gubarev, C. Heiser, P. Hochschild, W. Hsieh, S. Kanthak, E. Kogan, H. Li, A. Lloyd, S. Melnik, D. Mwaura, D. Nagle, S. Quinlan, R. Rao, L. Rolig, Y. Saito, M. Szymaniak, C. Taylor, R. Wang, and D. Woodford. Spanner: Google's globally-distributed database. In *Proceedings of the 12th Symposium on Operating Systems Design and Implementation (OSDI '16)*, Oct. 2012.

[26] Criu. http://criu.org, 2015.

[27] H. Cui, R. Gu, C. Liu, and J. Yang. Paxos made transparent. In *Proceedings of the 25th ACM Symposium on Operating Systems Principles (SOSP '15)*, Oct. 2015.

[28] B. Cully, G. Lefebvre, D. Meyer, M. Feeley, N. Hutchinson, and A. Warfield. Remus: High availability via asynchronous virtual machine replication. In *Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation*, pages 161–174. San Francisco, 2008.

[29] H. T. Dang, D. Sciascia, M. Canini, F. Pedone, and R. Soulé. Netpaxos: Consensus at network speed. In *Proceedings of the*

1st ACM SIGCOMM Symposium on Software Defined Networking Research, SOSR '15, 2015.

[30] A. Dragojević, D. Narayanan, O. Hodson, and M. Castro. Farm: Fast remote memory. In *Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation*, NSDI'14, 2014.

[31] A. Dragojević, D. Narayanan, E. B. Nightingale, M. Renzelmann, A. Shamis, A. Badam, and M. Castro. No compromises: Distributed transactions with consistency, availability, and performance. In *Proceedings of the 25th ACM Symposium on Operating Systems Principles (SOSP '15)*, Oct. 2015.

[32] M. P. I. Forum. Open mpi: Open source high performance computing, Sept. 2009.

[33] L. Glendenning, I. Beschastnikh, A. Krishnamurthy, and T. Anderson. Scalable consistency in scatter. In *Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP '11)*, Oct. 2011.

[34] H. Guo, M. Wu, L. Zhou, G. Hu, J. Yang, and L. Zhang. Practical software model checking via dynamic interface reduction. In *Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP '11)*, pages 265–278, Oct. 2011.

[35] Z. Guo, C. Hong, M. Yang, D. Zhou, L. Zhou, and L. Zhuang. Rex: Replication at the speed of multi-core. In *Proceedings of the 2014 ACM European Conference on Computer Systems (EUROSYS '14)*, page 11. ACM, 2014.

[36] B. Hindman, A. Konwinski, M. Zaharia, A. Ghodsi, A. D. Joseph, R. Katz, S. Shenker, and I. Stoica. Mesos: A platform for fine-grained resource sharing in the data center. In *Proceedings of the 8th USENIX conference on Networked Systems Design and Implementation*, NSDI'11, Berkeley, CA, USA, 2011. USENIX Association.

[37] D. Huynh Tu, B. Pietro, W. Han, L. Ki Shu, W. Hakim, C. Marco, P. Fernando, and S. Robert. Network hardware-accelerated consensus. Technical report, USI Technical Report Series in Informatics, 2016.

[38] Z. István, D. Sidler, G. Alonso, and M. Vukolic. Consensus in a box: Inexpensive coordination in hardware. In *Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation*, NSDI'16, 2016.

[39] J. Jose, H. Subramoni, K. Kandalla, M. Wasi-ur Rahman, H. Wang, S. Narravula, and D. K. Panda. Scalable memcached design for infiniband clusters using hybrid transports. In *Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (Ccgrid 2012)*, CCGRID '12, 2012.

[40] A. Kalia, M. Kaminsky, and D. G. Andersen. Using rdma efficiently for key-value services. Aug. 2014.

[41] M. Kapritsos and F. P. Junqueira. Scalable agreement: Toward ordering as a service. In *Proceedings of the Sixth International Conference on Hot Topics in System Dependability*, HotDep'10, 2010.

[42] M. Kapritsos, Y. Wang, V. Quema, A. Clement, L. Alvisi, M. Dahlin, et al. All about eve: Execute-verify replication for multi-core servers. In *Proceedings of the Tenth Symposium on Operating Systems Design and Implementation (OSDI '12)*, volume 12, pages 237–250, 2012.

[43] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong. Zyzzyva: Speculative byzantine fault tolerance. In *Proceedings of the 21st ACM Symposium on Operating Systems Principles (SOSP '07)*, Oct. 2007.

[44] S. Krishnan. *Programming Windows Azure: Programming the Microsoft Cloud*. May 2010.

[45] L. Lamport. Paxos made simple. http://research.microsoft.com/en-us/um/people/lamport/pubs/paxos-simple.pdf.

[46] L. Lamport. The part-time parliament. *ACM Trans. Comput. Syst.*, 16(2):133–169, 1998.

[47] L. Lamport. Fast paxos. Fast Paxos, Aug. 2006.

[48] J. Li, E. Michael, N. K. Sharma, A. Szekeres, and D. R. K. Ports. Fast replication with nopaxos: Replacing consensus with network ordering. In *Proceedings of the 12th Symposium on Operating Systems Design and Implementation (OSDI '16)*, Nov. 2016.

[49] S. Lu, S. Park, E. Seo, and Y. Zhou. Learning from mistakes: a comprehensive study on real world concurrency bug characteristics. In *Thirteenth International Conference on Architecture Support for Programming Languages and Operating Systems (ASPLOS '08)*, pages 329–339, Mar. 2008.

[50] Y. Mao, F. P. Junqueira, and K. Marzullo. Mencius: building efficient replicated state machines for wans. In *Proceedings of the 8th USENIX conference on Operating systems design and implementation*, volume 8, pages 369–384, 2008.

[51] P. J. Marandi, C. E. Bezerra, and F. Pedone. Rethinking state-machine replication for parallelism. In *Proceedings of the 2014 IEEE 34th International Conference on Distributed Computing Systems*, ICDCS '14, 2014.

[52] D. Mazieres. Paxos made practical. Technical report, Technical report, 2007. http://www. scs. stanford. edu/dm/home/papers, 2007.

[53] H. Meling, K. Marzullo, and A. Mei. When you don't trust clients: Byzantine proposer fast paxos. In *Proceedings of the 2012 IEEE 32Nd International Conference on Distributed Computing Systems*, ICDCS '12, 2012.

[54] https://memcached.org/.

[55] E. Michael. *Scaling Leader-Based Protocols for State Machine Replication*. PhD thesis, University of Texas at Austin, 2015.

[56] C. Mitchell, Y. Geng, and J. Li. Using one-sided rdma reads to build a fast, cpu-efficient key-value store. In *Proceedings of the USENIX Annual Technical Conference (USENIX '14)*, June 2013.

[57] Mongodb. http://www.mongodb.org, 2012.

[58] I. Moraru, D. G. Andersen, and M. Kaminsky. There is more consensus in egalitarian parliaments. In *Proceedings of the 13th ACM Symposium on Operating Systems Principles (SOSP '91)*, Nov. 2013.

[59] D. Ongaro and J. Ousterhout. In search of an understandable consensus algorithm. In *Proceedings of the USENIX Annual Technical Conference (USENIX '14)*, June 2014.

[60] D. Ongaro, S. M. Rumble, R. Stutsman, J. Ousterhout, and M. Rosenblum. Fast crash recovery in ramcloud. In *Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP '11)*, Oct. 2011.

[61] http://www.openldap.org/.

[62] S. Peter, J. Li, I. Zhang, D. R. K. Ports, D. Woos, A. Krishnamurthy, T. Anderson, and T. Roscoe. Arrakis: The operating system is the control plane. In *Proceedings of the Eleventh Symposium on Operating Systems Design and Implementation (OSDI '14)*, Oct. 2014.

[63] M. Poke and T. Hoefler. Dare: High-performance state machine replication on rdma networks. In *Proceedings of the 24th International Symposium on High-Performance Parallel and Distributed Computing*, HPDC '15, 2015.

[64] D. R. K. Ports, J. Li, V. Liu, N. K. Sharma, and A. Krishnamurthy. Designing distributed systems using approximate synchrony in data center networks. In *Proceedings of the 12th USENIX Conference on Networked Systems Design and Implementation*, NSDI'15, 2015.

[65] M. Primi. LibPaxos. http://libpaxos.sourceforge.net/.

[66] http://redis.io/.

[67] ssdb.io/.

[68] A. Thomson, T. Diamond, S.-C. Weng, K. Ren, P. Shao, and D. J. Abadi. Fast distributed transactions and strongly consistent replication for oltp database systems. May 2014.

[69] R. Van Renesse and D. Altinbuken. Paxos made moderately complex. *ACM Computing Surveys (CSUR)*, 47(3):42:1–42:36, 2015.

[70] X. Wei, J. Shi, Y. Chen, R. Chen, and H. Chen. Fast in-memory transaction processing using rdma and htm. In *Proceedings of the 25th ACM Symposium on Operating Systems Principles (SOSP '15)*, SOSP '15, Oct. 2015.

[71] G. G. Wittawat Tantisiriroj. Network file system (nfs) in high performance networks. Technical Report CMU-PDLSVD08-02, Carnegie Mellon University, Jan. 2008.

[72] J. Yang, T. Chen, M. Wu, Z. Xu, X. Liu, H. Lin, M. Yang, F. Long, L. Zhang, and L. Zhou. MODIST: Transparent model checking of unmodified distributed systems. In *Proceedings of the Sixth Symposium on Networked Systems Design and Implementation (NSDI '09)*, pages 213–228, Apr. 2009.

[73] M. Zaharia, B. Hindman, A. Konwinski, A. Ghodsi, A. D. Joesph, R. Katz, S. Shenker, and I. Stoica. The datacenter needs an operating system. In *Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing*, 2011.