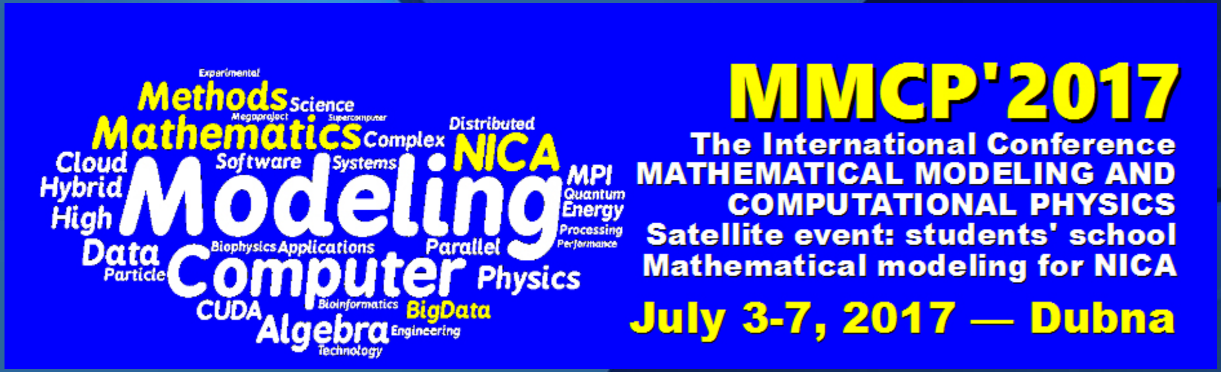
Computer Modeling of a Dispersed Storage System for Private Data on Public Resources

S.Polyakov, A.Kryukov[1], A.Demichev
SINP MSU, Moscow



MMCP'2017
The International Conference
MATHEMATICAL MODELING AND
COMPUTATIONAL PHYSICS
Satellite event: students' school
Mathematical modeling for NICA
July 3-7, 2017 — Dubna

[1] kryukov@theory.sinp.msu.ru

Outlook

- Introduction
  - Problem
  - Current status
  - Existing analogs
- Requirements to such systems
- Proposal methods
- Conclusions

Problem (1/3)

- Currently the flow of data from diverse sources including various sensors, WWW, mobile devices, large scientific experiments, etc., is growing with enormous speed.
  - A large number of data are of a private nature
- Changes in science and business led to the understanding that it is necessary to develop new architecture and operating principles of information systems to cope with this vast stream of data and private data in particular.

Problems (2/3)

- In the existing centralized solutions, including clouds, the data centers collect and store data from the peripheral nodes.
- In this centralized model, much depends on the stability of the data centers, on the trust of users to providers of the storage services and on the bandwidth of the channels through which information is exchanged between the cloud and the periphery.
- The proposed alternative method based on a distributed dispersed storage system (DSS) for data volumes of several tens or hundreds of terabytes per user or user group on the free public storage resources of Internet users
  - This solution may be significantly more favorable both from economic and technical points of view.

Problem (3/3)

- P2P data storage are evenly distributed among all peers in the network, which provides
  - natural load balancing,
  - the absence of bottlenecks and points-of-failure
  - special mechanisms of encoding, fragmentation and distribution of information which provides privacy and reliability of the data
- The novelty of the proposed project is the adaptation, optimization and integration of information dispersal algorithms into a P2P network to create a safety, reliability, performance and usability storage systems of private information on public resources

Current status (1/2)

- In the recent years, peer-to-peer system research has grown significantly
- P2P networks offer the following benefits:
  - do not require any special administration or financial arrangements.
  - self-organized and adaptive. Peers may come and go freely. P2P systems handlethese events automatically.
  - gather and harness the tremendous computation and storage resources on computers across the Internet.
  - distributed and decentralized. Therefore, they are potentially fault-tolerant and load-balanced.

Current status (2/2)

- One of the example of implementation of information dispersal algorithm (IDA) is a file system dsgfs, created by Cleversafe in 2006.
  - Its important distinction is the use of a fixed set of dedicated storage resources, whereas our proposed use of P2P networks implies significant rate of joining and leaving the network by individual users (churn).
- The fragmentations of stored files is used by BitTorrent protocol, allowing to transfer files from several nodes simultaneously.
  - It is only using simple non-optimized replication. Also, BitTorrent networks use centralized registries of file locations (trackers) that are the potential points of failure.

Analogs

- A cloud data storage network Storj allows users to lease their hard drive space.
  - IDA is used to provide the security and privacy of the data.
- Project Sia, where users can set their own price for leased storage space.
  - However, it is left to data owner to store the information on location of their data and manage (or at least keep track of) its transfer between the nodes.
  - The monitoring of the data can be entrusted to a third party server, but this creates problems of possible breach of trust and creates a centralized data management node which contradicts the peer-to-peer paradigm.

Requirements

- There are some specific requirements for storage of private information on the Internet public resources. It should provide the following conditions:
  - reliability
  - accessibility
  - privacy

Reliability and Accessibility

- The reliability means a possible to restore data if some part of data was lost.
  - The simplest solution of the problem, that is storing multiple copies of data on different media.
    - It is the most costly in terms of storage and data transfer, and excessive in reliability.
  - The good solution is using IDA for disperse storage of data over Internet. It is similar RAID technique but on the network.
- Accessibility. The accessibility means a permanent access to the data if some part of data is unavailable over the network.
  - The simplest solution is make distributed storage instead of centered solution. The P2P is most suitable candidate

Privacy (1/2)

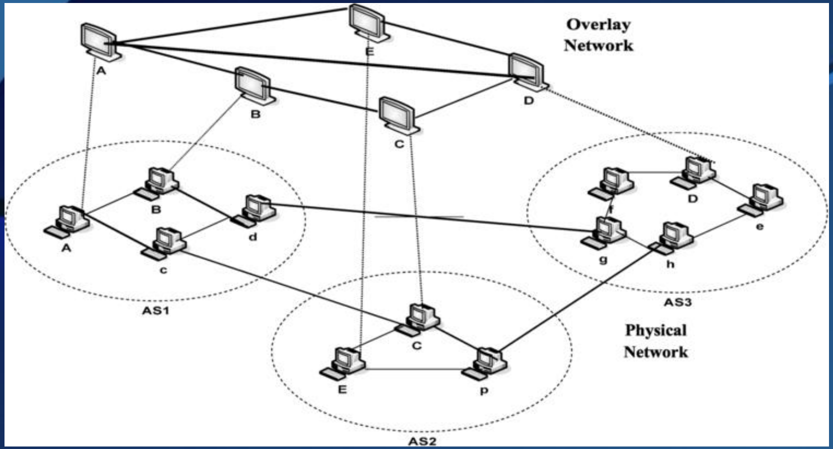
- The privacy means to protect data from unauthorized access.
- The privacy has two features:
  - Authentication and authorization
  - Encryption both channels and storage
- The authentication and authorization problem are well know and we will not discuss. See for example X509 certificate.
- We did not also discuss the encryption channels. See for example TLS.

Privacy (2/2)

- Privacy on the storage node.
- How to protect data from illegal access of storage administrator?
- There are two solution.
  - Encryption data
  - Disperse data over network
  - It is possible use both approaches.
- Encryption data. The problem of key management.
  - Key store on the storage - not a really solution.
  - Keys store on the client side — the problem of multiple data transfer.

Proposal solutions

- The general approach to the analysis of the overlay topology and data search algorithms is the theory of complex networks which describe a wide range of different systems.
- The optimization will be carried out assuming varying rates and types of nodes disappearing (churn, failure, crash), and also joining of the new nodes to the network.
- For large dynamic networks, which are expected to be dispersed P2P storage network, cases of failure of part of the nodes of the interconnection network are almost inevitable because of the physical faults, overload, or simply due to quiting the network by a peer.
- We intend to create a computer model of DSS behavior under the condition of high volatility of the P2P network, and use it to estimate functionality, performance, scalability, and reliability of the DSS.



Proposal solution

- We will use multicriteria optimization to find the optimal parameters of the DSS:
  - the choice of P2P network type (purely decentralized or hybrid, where some peers serve the search request of other regular peers);
  - the choice of topology of overlay P2P network (structured or unstructured, hierarchical or non-hierarchical);
  - the choice of corresponding search and data routing algorithms;
  - the choice of techniques for checking retrievability of undistorted data and timely restoration of lost fragments;
  - the parameters of the IDAs (number of fragments n that files are split into, and number of fragments k < n necessary to restore it);

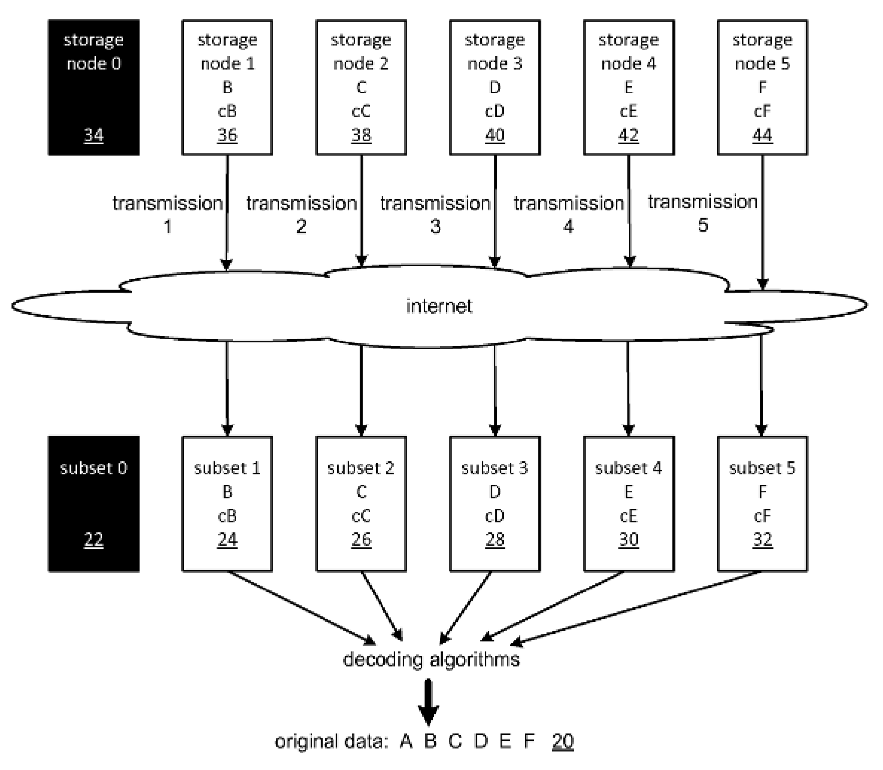


FIG. 3

Planed results

- The main results of the work performed will be:
  - topology of the P2P network most suitable for the implementation of IDA in a dynamically changing network;
  - developed search and data routing algorithms for the selected P2P networks, optimal for use with IDA;
  - an algorithm for recovering the lost pieces of information in a dynamically changing P2P network based on the principles of self-organization;
  - developed method for checking retrievability of undistorted data (data chunks), stored on a particular node of the network.

Conclusions

- The proposal aproaches to the DSS allow to organize the storing of private data on the public Internet resources.
- The computer modeling of P2P DSS network let us optimize the essential properties of the DSS
  - The redundancy of IDA
  - The discovery algorithm
  - The “small world” properties of overlay network.
- The results of modeling will be put on the future programming realization of DSS

Thank you!

Questions?