On the use of trusted nodes for Byzantine fault tolerant peer sampling protocols

Augusta Mukam, Joachim Bruneau-Queyreix, Laurent Réveillère
augusta.mukam@u-bordeaux.fr, joachim.bruneau-queyreix@u-bordeaux.fr,
laurent.reveillere@u-bordeaux.fr

Univ. Bordeaux, CNRS, Bordeaux INP, LaBRI, UMR5800, F-33400 Talence, France

Introduction - Problem

- Most distributed systems use gossip peer sampling protocols for information dissemination in which nodes periodically build and refresh their local views of the evolving system which is a partial knowledge of the full membership.
- But an attacker controlling some nodes may aim at partitioning the network or being over-represented in the views of correct nodes to gain impact in the upper-layer protocols of the system.
- **So, How to have Less biased views for correct nodes ?**

Known Byzantine Fault Tolerant Protocols in peer sampling

Let us consider a system of n active nodes with a fraction $f < 1$ of faulty nodes. We define some metrics to evaluate state-of-the-art protocols: **Resilience**, **Time to discovery**, **Time to view stability**.

- **Brahms** [1]
  - It is one of the most Byzantine resilient protocol,
    1. Contribution of push and pull and use of Limited pushes
    2. Attack detection and blocking
    3. History sampling

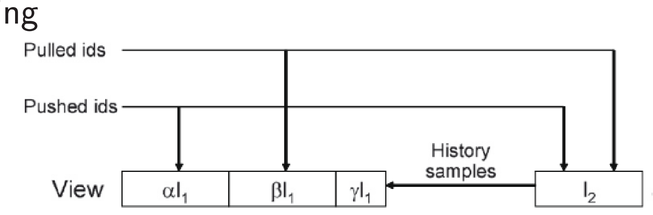

Figure 1:Brahms view update

  - **Resilience of 81% when the system is composed of $f = 18\%$.**

Now we add a proportion $t > 1$ of trusted nodes (running using TEE devices) inside the system.

- **Raptee** [2]
  - Raptee relies on different solutions on top of Brahms summarized in Fig2:
    1. Mutual authentication and Trusted communication
    2. Byzantine eviction
    3. **When $f = 10\%$, we have resilience improvment of 17% and $t = 1\%$.**

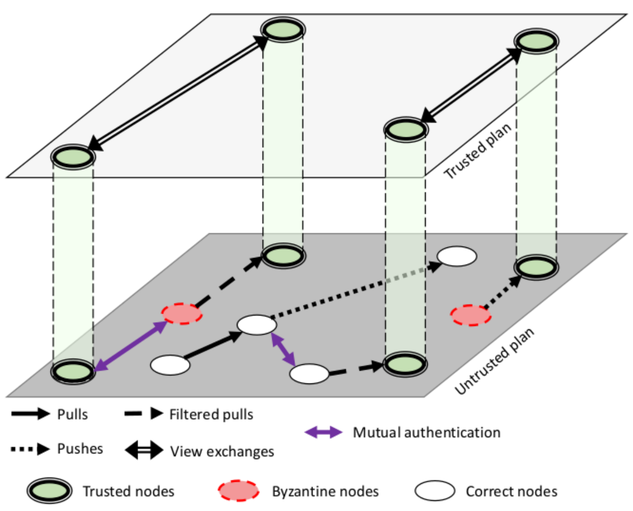

Figure 2:Overview of the RAPTEE protocol

- **Knowledge Free One pass Strategy** [3]
  1. Sampling memory, Insertion and removal probabilities
  2. Count Min Sketch: A memory constant data structure matrix built on the fly which provides an approximation of the number of times a node appeared in the stream

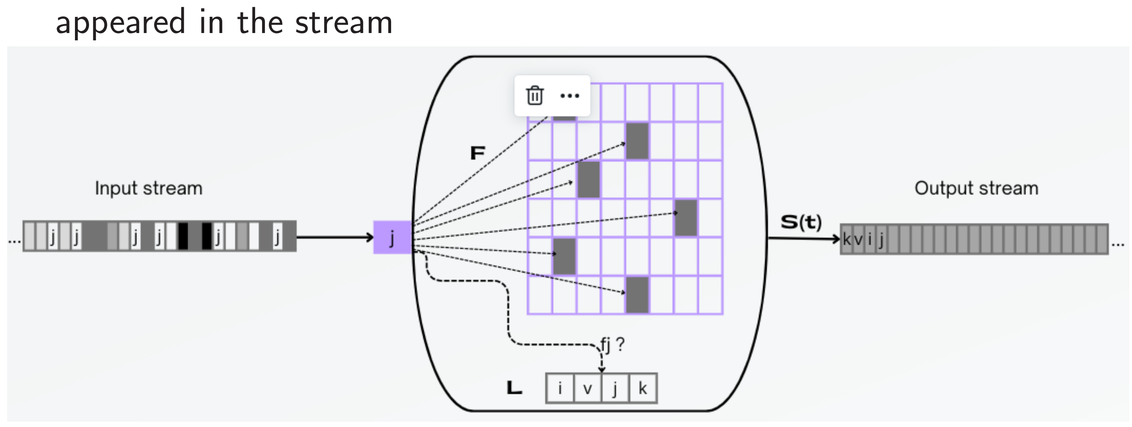

Figure 3:Sampling component of a node

Experimentation Work

- Implementation of Brahms, Raptee and Count Min Sketch
- Evalutation: Reproductibility of results

Figure 4:Resilience improvement of Raptee on Brahms

Ongoing work: Use of Count Min Sketch

- The purpose is to accelerate mutual decontamination of streams passing througth trusted nodes
- The idea is to merge the Count Min Sketch od trusted nodes during a trusted communication so that the will get more knowledge of the system

Figure 5:Use of Count Min sketch to unbias a stream

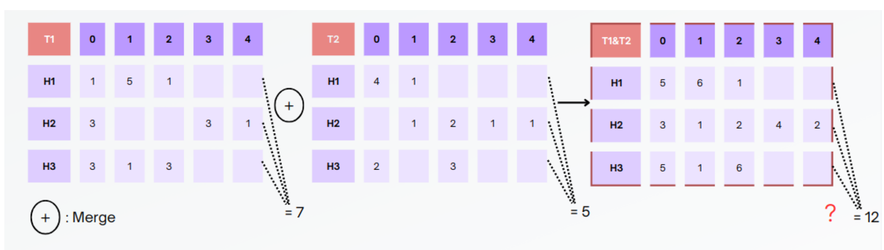

Figure 6:Merging Count Min Sketch

References

[1] E. Bortnikov et al, "Brahms: Byzantine resilient random membership sampling," Computer Networks, 2009.
[2] M. Pigaglio et al, "RAPTEE: Leveraging trusted execution environments for Byzantine-tolerant peer sampling services," IEEE 2022
[3] Emmanuelle Anceaume et al, " Uniform Node Sampling Service Robust against Collusions of Malicious Nodes. 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks DSN 2013