PROFITAP

WHITEPAPER

TIMESTAMP ANALYSIS AND THREE EFFICIENT WAYS TO RUN IT WITH IOTA

VISIT **WWW.PROFITAP.COM**

How accurate timestamping makes a difference in OT network analysis

As industrial networks have grown larger and more complex than ever before, network monitoring tools are quickly becoming a necessity. Network access control solutions can help with managing industrial devices and OT networks. The acronym OT refers to Operational Technology, i.e., that set of technologies, software, and hardware, directly connected with the production, transportation, and transformation of assets. It refers to everything that concerns the monitoring and control systems of the production system that are also specified with other acronyms as ICS (Industrial Control Systems), SCADA (Supervisory Control and Data Acquisition), or PLC (programmable logic controller or programmable controller).

Whether it is a company with one plant or hundreds of factories worldwide, efficiency and excellence in the network infrastructures are key to maximizing operational efforts and avoiding latency, bottlenecks & downtime, which adds costs. And in ICS, like the manufacturing industry, time equals money. In any OT network when a device, data center, or server on the network does not operate correctly, accurate and fast troubleshooting is crucial. Every minute of downtime impacts business production, and so profit.
To be able to counter (and even prevent) network downtime, virtual attacks, breaches, or system errors, access, and visibility to the networks is crucial: in other words, monitoring, capturing, and correlating packets for a chance to detect and prevent threats early.

A crucial aspect of running and maintaining a network is achieving optimal performance. In the context of network monitoring, performance can be linked to the concept of latency, referring to the speed of the network or the Remote Response time. Apart from the processing time needed for any network application service to process a request, there is a delay involved for the request to reach the service. While referring to latency, it's that delay we are talking about.

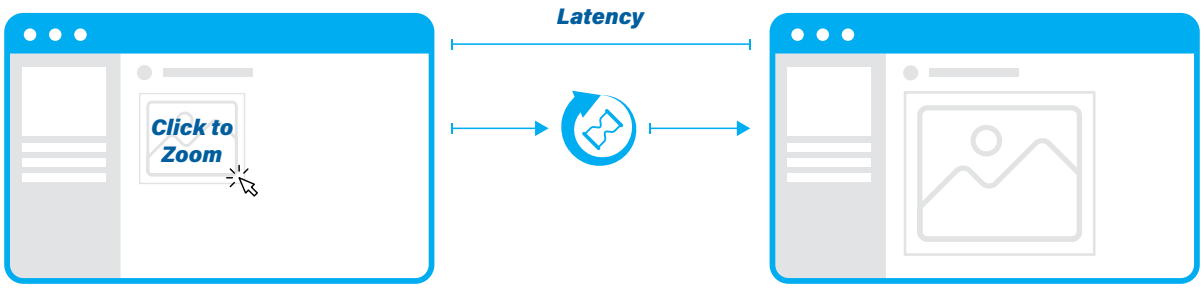

Fig 1. *In network monitoring, performance can be linked to the concept of latency, referring to the speed of the network or the Remote Response time.*

This becomes a big issue for industrial control systems (ICS) with remote locations. Imagine a manufacturing center in the US accessing a data center in Europe. If ignored, latency can trigger the service level agreements (SLAs) violation. In other words: losing access to data and cloud-based applications for even a few minutes at a time can cost company productivity, lost revenue opportunities, and brand damage.

Even though it can be pretty difficult to improve latency, it's important to precisely measure it with purpose-built solutions. The ability to timestamp packets with high accuracy when monitoring is essential for understanding what is going on in the network at a packet level. Accurate time information is important for legal and criminal investigation, and the same applies to accurate forensic analysis and performance testing to measure crucial indicators like latency.

A timestamp is a sequence of characters that can help you identify when a certain event occurred, by giving you the actual date and time of day, sometimes accurate to a small fraction of a second. Timestamps are added as information to the header of each packet, which in turn can be interpreted by an analyzer such as IOTA or Wireshark. In a nutshell, a timestamp is a record of the time at which a packet was received and processed through your network access device.

When analyzing packets, an important requirement is knowing the exact date and time they were captured with the highest possible accuracy and resolution. This can be especially important in many applications and situations where different time zones are involved, such as compliance, troubleshooting, capacity planning, intrusion detection and prevention of cyberattacks, and so on. This ensures packets contain the actual time of their occurrence over the network.

A timestamp is a sequence of characters that can help you identify when a certain event occurred, by giving you the actual date and time of day, sometimes accurate to a small fraction of a second.

Three methods to run a timestamp analysis with IOTA plus

As mentioned before, timestamping is an important tool when analyzing network traffic. But what equipment can you use for this type of analysis? Here we'll discuss the IOTA series, which offers several timestamping options. All IOTA models are able to timestamp ingress frames using a hardware time counter. The time counter has a resolution of <10 ns, the resolution depends on the device and feature: 8 ns for the 1G and 1G+, 6.4 ns for the 10G, and 5 ns for the 10G+.

We will go through 3 methods to synchronize 2 IOTA devices: with one GPS signal, with 2 GPS signals, and without GPS signals.

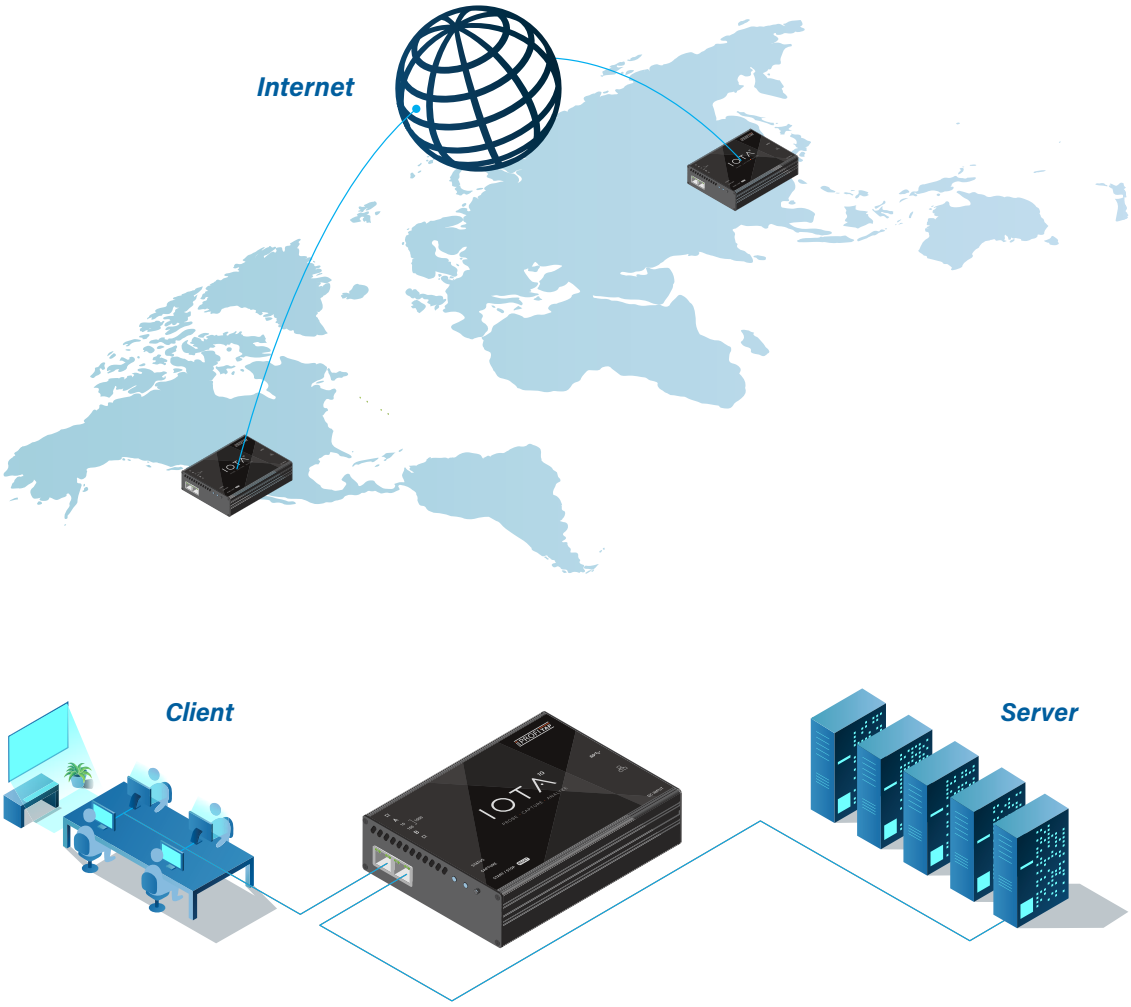

Fig 2. *On premise monitoring or remotely in different timezones with IOTA*

Method 1: relying on 1 GPS signal

Let's get started with two key definitions: Time initialization means taking a timestamp from a source. It happens once during IOTA boot time. Counter disciplining means synchronizing the counter speed to an external source. This happens every second during the IOTA operation.

IOTA 1's time is initialized from the GPS signal, and the timestamp counter is disciplined from the GPS. In this case, IOTA 1 is the "main" device, disciplining IOTA 2.

IOTA 2 uses its own system time (set either via NTP or manually), while the timestamp counter is disciplined from external PPS (from IOTA 1).

For this method, it is important that IOTA 2's system time be within 0.5 s of UTC global time.

If IOTA 2's system time has an offset greater than 0.5 s, this may induce a constant time offset between IOTA 1 and IOTA 2 (aligned to whole seconds, like 1 s, 2 s, etc).

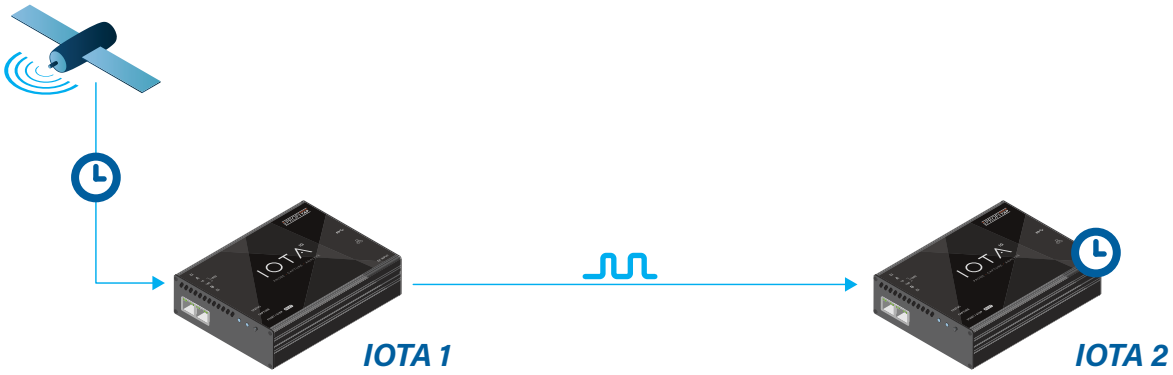

Fig 3. *Method 1: relying on 1 GPS signal.*

Benefits of this method:

- It measures delay between packets within IOTA1 and the same packets within IOTA2 (as clocks are synchronized).
- It makes possible to run timestamp analysis also when there is no possibility to use GPS on IOTA2 (or no/weak signal).

Method 2: relying on 2 GPS signals

Times are initialized from GPS and timestamp counters are disciplined from GPS.
In this case, both IOTAs rely on GPS signals in both taking timestamps and disciplining. Therefore, both IOTAs will have valid absolute **UTC-aligned** timestamps.

Fig 4. *Method 2: relying on 2 GPS signals.*

Benefits of this method:

- It measures precise packet delays between IOTAs.
- In case of geographically separated capture point locations (different cities/countries), there is no distance limit.

Method 3: no GPS signal

To synchronize two IOTAs together (not to UTC) without GPS signal, both IOTAs use their own system time for timestamping (the generic "0.5 seconds difference" rule also applies here). IOTA 1 generates a PPS signal and forwards it to IOTA 2 through a PPS cable.

Alternatively, an external PPS source provides PPS to both IOTAs.

Fig 5. *Method 3: No GPS signal.*

Benefits of this method:

- Relative (not UTC-aligned) delay measurements between and within IOTAs.
- An effective way to run a timestamp analysis If there is no possibility to use GPS.

PROFITAP

Profitap develops and manufactures hardware and software solutions that help you get complete access and visibility into your network. These network visibility solutions are designed with the security, forensics, deep packet capture and network & application performance monitoring sectors in mind.

Profitap network solutions help eliminate network downtime, add security to existing and new networks all over the world, assist in lawful interception applications and reduce network complexity. All of Profitap's network monitoring tools are highly performant, secure and user-friendly, and provide complete visibility and access to your network, 24/7.

As we are experts in our field, we have developed our products to set new standards in an industry where the definition of excellence is constantly being challenged.

With more than 1,000 clients from 55 countries, Profitap has become a must-have solution or many important businesses, many of which are among Fortune 500 companies.

PROFITAP HQ B.V.
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN
THE NETHERLANDS

sales@Profitap.com
www.Profitap.com

Profitap

@Profitap

Profitap-international