GEO-Trust: Geo-aware security protocol for enabling cross-border trustable operations and data exchange in a global digital economy

Dr. Antonio J. Jara, *IEEE member*
University of Applied Sciences Western Switzerland (HES-SO)
jara@ieee.org

Yann Bocchi
University of Applied Sciences Western Switzerland
yann.bocchi@hevs.ch

***Abstract*— Security and trustability in Internet is a baseline problem that continues arising as far as digitalization and data economy are taking place. It is well-known the value of data in the current digital age and social media economy. Consequences of this has produced a digitally-enabled data capture for different business domains and research. Nowadays, there is a lack of trustability for sharing data. In addition, legal regulations about data protection such as Swiss Data Protection Act (DPA), which is being updated and influenced by GDPR's European Union principles are defining a more restrictive regulation about data usage, data geo-location and data sharing which are crucial to enable a data economy. Therefore, key challenges need to be addressed for guarantying a safe and regulations compliance flow of data (cross-borders). GEO-TRUST is developing techniques and algorithms that promote regulation of data exchange, trustability, consent management, reputation and security as contribution for the emerging Data Economy Ecosystem. In details, GEO-TRUST project proposes an innovative protocol called Proof of Offset (POO) to enable a higher control and limit data access by geo-location, accountability, data exposition minimization, data semantic annotation that guarantee cross-domain data re-use and higher awareness about data protection. This work presents the key concepts and initial results behind this technology being developed under the support of Hasler Foundation in Switzerland.**

Keywords—Internet of Things, Smart Cities, Security, Data Economy, 5G, SDN, Edge Computing, FIRE.

I. Introduction

GEO-TRUST is attending the legal requirements about data usage geo-location, which are crucial to enable a data economy. In Europe there is a major challenge in enabling the new legal framework and regulations defined by EU General Data Protection Regulation (GDPR). GDPR places an increased number of requirements to demonstrate data protection compliance and a higher empowerment to users about their data, it means that we need to provide innovative protocols for data usage and monitoring and with a special focus on data geo-location due to the constraints for data portability and data access.

Next generation Internet data-driven services require an intelligent nerve that facilitates the data trading, data exchange and data management that facilitates the business development, at the same time that satisfies the regulation *Personal Data:* Global Data Privacy Regulation (GDPR) and *Non-personal data and machines data: as a complement to GDPR,* as part of the actions to enable a digital single market and a data economy, another non-personal data emerging regulation are being defined, where data management for machines and devices is being addressed [1].

EU and Switzerland are working for protecting data flows across borders and sectors and disciplines. This data should be accessible and reusable by most stakeholders in an optimal way. However, key challenges are being found for enabling a free flow of data (cross-borders), i.e., removing data localization restrictions. Additionally, Trust is a key precondition for the development of the data economy as a whole. The proposed regulation for the European Data Economy seeks to provide reassurance to regulators and businesses and promote the reuse of public and publicly funded data. In particular, for Smart Cites, Connected Cars, and any IoT solution where the data is generated by a non-personal machine, it needs to be tradable to allow innovative business models to flourish, new market entrants to propose new ideas and start-ups to have a fair chance to compete. In addition, we must take into account the different regulative and legislative domains beyond European and Swiss borders. For example, Swiss companies and any other European company may not want to move critical data to the USA because of the patriot act [2] that allows United States governmental institutions to access all electronic data. Therefore, even when companies are headquartered in European continent, their data can be geo-located beyond Europe borders and finalize in infrastructure providers which offer data centres in USA with totally different regulations.

For that reason, a Data Economy Ecosystem that offers lawfully by default is required to bootstrap and enable this ecosystem. It means innovative techniques to limit data access by geo-location, accountability, data exposition minimization, data semantic annotation that offer cross-domain data re-use and higher data protection awareness.

Distance metrics and geo-location have been a studied problem in the Internet. First, it has been motivated for scalability due to attend problems such as server selection, since majority of Internet services are provided by multiple server, and we can find how nowadays majority of cloud computing services such as Amazon Elastic Compute Cloud (EC2) or Microsoft Azure have available a wide map of data centres to cover all the globe in order to optimize access to offered services over their cloud computing platforms.

Cloud Computing and distributed resources allocation has extended this approach by providing more flexibility in the placement, movement, and interconnection of digital resources. However, several use-cases and following the

978-1-7281-3967-8/19/$31.00 ©2019 IEEE

legal framework described require the data to be located under a certain jurisdiction.

Current approaches for geolocation are based on building a database to keep the mapping between IP blocks and a geographic location. Several databases are available and are frequently used by many services, web sites and public databases such as IP2Location [3]. This IP geolocation solution are highly limited since it is not able to verify if the target IP-address relays the packets to the desired destination (i.e., making use of tunnels, Virtual Private Networks (VPNs) or proxies to expose a different IP address location), the lack of a detailed database in a global scale [4], and cloud operators might move the virtual resource to another data centre and relaying all packets to and from the original IP-address. To overcome this shortcoming, a relevant work from University of Luxembourg and Fraunhofer AISEC [5] proposed a geolocation approach based on Virtual-network Coordinate Systems (VCS). Through Round-Trip Time (RTT) measurements between different locations in the Internet with known coordinates and the location of the nodes. There are three solutions based on this VCS concept, namely Vivaldi [6], Pharos [7] and Phoenix [8]. However, these methods for geolocating using general latency delays [9-10] are prone to error over 1000km [11].

GEO-TRUST presents a mechanism for verifying the location of target nodes that want to consume data without the need of trusting the cloud operator. Based on dedicated hosts, which serve as landmarks and monitors, with known locations using the standard defined in Global Network Positioning (GNP) [12] maps nodes.

This infrastructure of well-known locations is based on existing infrastructure such as Future Internet Research Experimentation (FIRE) testbeds, as we can find PlanetLab Europe / Fed4FIRE and Barcelona Supercomputing Centre (BSC). GEO-TRUST proposes a new algorithm called Proof of Offset (POO), which is based on RTTs and carry out a hierarchical approach based on two phases, an initial general phase for identification of the country using a general number of monitors at a global scale. and a second fine-gran phase for the verification of the country via a fine-grain number of monitors located at the same country.

The precision of these geo-location classification system is usually expressed by the prediction error, which defines the difference between the calculated and real distance. GEO-TRUST considers not only the prediction error in terms of real distance, else the proper country classification, since the major challenge is to define legal jurisdiction which is defined at a country level.

Finally, other key advanced from GEO-TRUST via POO is the identification of relay nodes such as proxies that could try to manipulate the system or violate the solution. To my knowledge, none of these systems have been tested in a more complex network environment with relay nodes (proxies) forwarding traffic to the actual recipient, which is assumed here. Thus, POO analyses the effectivities of the inclusion of puzzles to verify real node location, making not feasible for intermediary nodes to run this kind of computational challenges.

This work applications can satisfy key needs from Internet of Things and data economy to guarantee the proper data usage; at the same time that we will leverage emerging trends and innovative network architectures (some of them internet agnostic networks such as blockchain) in order to integrate the protocol on top of it. In details, this project objectives are:

1- To **develop and deliver innovative protocols and networking methods for enabling secure data exchange** that attends existing gaps such as **data consumption geo-location and data access control**.

2- To set up an **empirical validation in a large scale geo-distributed distributed and interconnected testbed** such as offered by Fed4FIRE [20-21] and Barcelona Supercomputing Centre (BSC), in order to demonstrate how it works over Internet and also over Internet Agnostic Networks such as emerging blockchain and distributed networks.

3- To **create significant evidence of the benefits of the proposed protocols** as part of an emerging data economy for the safety data reuse, accountability and trustability via new models that guarantees the **satisfaction of rules, contracts and agreements** in terms of quantity (accountability), geo-location (legal constraints beyond European Union and Swiss borders), and **data usage** (data minimization and rights to revoke permissions) that **enable and promote new collaboration models** driven by users acceptance, compliance with new regulation frameworks.

GEO-TRUST aims moves to solutions that enable a major trust in the opportunities of the data economy, at the same time that protect to users. .

II. Use-cases and relevance

GEO-TRUST is motivated by the emerging regulations about data economy and data protection. GEO-TRUST has proposed the core algorithms as Internet agnostic, in order to assure its integration over the emerging networks and architectures. In details, there is three major challenges with three technology approach. First, communication capacity where 5G is leading the research focused on virtualization of networks making use of Software Defined Networks (SDN) and Network Functions Virtualization (NFV) in order to make network more programmable and scalable. Second, computational capacity which includes offloading techniques such as edge computing, cloudlets and other approaches focused on moving intelligence from the centralized infrastructures to distributed infrastructures, which offer resources closer to the user, as part of this paradigm shift from centralized parties to distributed and self-organizing (autonomous) architectures, a trust challenge has raised which has promoted the creation of new techniques such as Distributed Ledger Technology (DLT), i.e., blockchain, to democratize reputation and trustability. In addition, cost effectiveness and sustainability challenges in terms of resources such as energy, for this case the clearest reference are the massive networks as promoted by connected devices (IoT/M2M) are the clearest reference scenario to reach a trade-off between cost and performance.

Virtualized network infrastructures (SDN/NFV) and 5G

Virtualization technologies as SDN/NFV offer different architectural options to address the needs of 5G networks [13-15]. SDN/NFV is a new paradigm that permits decoupling of control and data planes of traditional Internet networks, in order to provide a higher programmability and flexibility, allowing the network to dynamically adapt to change traffic patterns and user demands. SDN/NFV implementations are being integrated with other paradigms such as edge computing, in order to allocate the resources. Relevant European Initiatives such as 5G-PPP European Programme (https://5g-ppp.eu), ETSI standardization activates around SDN and NFV are leading at the software level the market with relevant initiatives such as ETSI Open Source MANO (OSM) [16], OSM is providing the control plane is still suffering from scalability and performance concerns for a very large network

At the same time, this virtualization is enabling a new approach based on microservices, where data management (data collection, data processing and data storage) are being ready to be deployed via a scalable and distributed architecture that enhance availability, flexibility but at the same time also to reduce the network distance from the data collection point to the data storage and consequently offer a better control of potential vulnerable points for privacy and security.

GEO-TRUST is carrying out the evaluation and validation of the SDN/NFV capabilities for deploying a common network for the deployment of microservices in a distributed scenario. In particular, the federated testbeds from Fed4FIRE are ready for SDN/NFV. This technology is focused on the flexible applications deployment using microservices (agile technology). This initial objective is extended with the validation over distributed infrastructure. Distribution of the microservices in multiple allocations simulating the current needs to offer hybrid deployments between edge/fog and cloud computing environments. This Objective is crucial for the scalability of solutions based on 5G for massive deployments.

Distributed Ledger Technologies (DLT) and blockchain

Following the trend from virtualization technologies, and the potential from agile deployments based on microservices, enable to move from centralized infrastructure to move decentralized ones. However, it implies key challenges in terms of trustability. The key contribution of blockchain is that it provides a way to carry out transactions with another person or entity without having to rely on third-parties. Blockchain technologies are able to track, coordinate, carry out transactions and store information from a large number of devices, enabling the creation of applications that require no centralized cloud. Some companies like IBM go further and talk about blockchain as a technology for democratizing trust [17].

Blockchain works thanks to many decentralized miners (i.e., accountants) that scrutinize and validate every transaction. This contribution allowed the blockchain to provide a solution to the Byzantine Generals' Problem [18]. A blockchain, as its name implies, is a chain of timestamped blocks that are linked by cryptographic hashes.Every node of the network receives two keys: a public key, which is used by the other users for encrypting the messages sent to a node, and a private key, which allows a node to read such messages based on asymmetric cryptography. The fact of signing the transaction in a unique way (using the private key) enables authenticating it (only the user with a specific private key can sign it) and guarantees integrity (if there is an error during the transmission of the data, it will not be decrypted). As the peers of the node that broadcast the transaction receive the signed transaction, they verify that it is valid, thus, contributing to its spread through the network. The transactions disseminated in this way and that are considered valid by the network are ordered and packed into a timestamped block by special nodes called miners. The election of data included into the block depend on a consensus algorithm. One of the major challenges from blockchain is that accumulation of power by centralized entities such as exchanges, countries or large corporations. For that reason, consensus algorithms are a key component in the future of blockchain infrastructure sustainability.

GEO-TRUST is able to validate the value of POO algorithm to verify geographical distribution of consensus, as also replication and geographical dispersion.

Massive connected devices sustainability and IoT

IoT is paving the way for a world where many of our daily objects to interact with their environment in order to collect information and automate certain tasks. Such a vision requires, among other things, seamless authentication, data privacy, security, robustness against attacks, easy deployment and self-maintenance. The current challenges are focused on the data economy, which is the core focus from GEO-TRUST. Therefore, POO algorithm is a key component to attend the end-to-end data sharing and data exchange in the network. Currently, most IoT solutions rely on the centralized server-client paradigm, connecting to cloud servers through the Internet such as Context Brokers (MQTT, Orion Context Broker in FIWARE etc.). Although this solution may work properly nowadays, the expected growth suggests that new paradigms have to be proposed, i.e., offer an IoT as suggested in the past to create large end-to-end network, where connected devices are able to attend directly data request and supply to their customer, i.e., offering a higher level of autonomy and distribution. For that reason, since data sources will move back to the IoT infrastructure, it is required by IoT nodes to make use of POO to validate that target nodes are genuine and satisfy contracts / policies. Therefore, a lightweight version of POO and a performance optimization from POO is deeply analysed in this work to guarantee the results from GEO-TRUST are also feasible for IoT/M2M infrastructures.

III. Proof of Offset (POO) Concept and Algorithm

Proof of Offset is an innovative algorithm that allows to validate and determinate the geo-location for a Node N based on a collaborative and distributed approach. In details, the localization process itself requires a set of n collaborative monitors, which we can refer as landmarks or monitors $M = \{M_1, M_2, \ldots, M_n\}$ at a well-known distributed geo-location $L = \{l_1, l_2, \ldots, l_n\}$. The monitors act as reference points necessary to create meaningful coordinate systems. As a general approach for GEO-TRUST, since the main motivation are country-level regulations and law, a location is equivalent to a country, which usually defines the boundary of a jurisdiction.

This algorithm uses the Round-Trip Time (RTT) and the baseline metric. As basis of evaluation, we are making use of FIRE research infrastructure via Fed4FIRE project [21], which offers an open and free access for experimentation[1]. Fed4FIRE offers a network infrastructure with known node locations and measured RTTs between. Fed4FIRE testbeds include the PlanetLab Europe, which consists of 343 nodes at 205 sites [24] and it extends to PlanetLab for a global scale validation [25]. Figure 1 presents an overview of available testbeds sites.

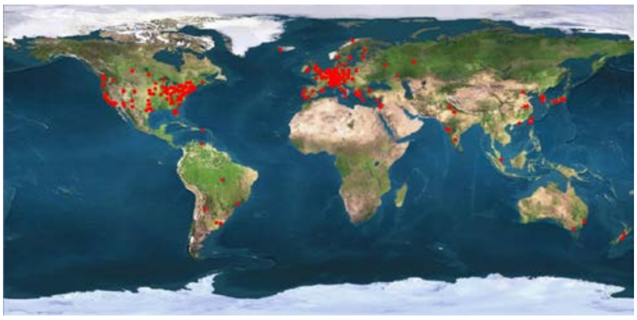

Figure 1. Planet-Lab Nodes deployment location based on Planet-Lab Visualizer[2].

Concerning the number of monitors, they are initially deployed using the described testbed. Figure 2. presents an example of a Node to be evaluated located at Ukraine, as a country which is out of the European Union but sharing borders with Russia and Europe, therefore making it as a clear example where Proof of Offset algorithm makes a difference in a fine grain, where the Node N is geo-located.

Proof of Offset algorithm is performed in two phases. First, a General phase where the node location is verified in a global level to verify / identify, which is the candidate country to validate. Second, a Fine-grain phase to validate that the Node is located at the identified country.

For the initial General phase where a number of g nodes is selected randomly out of the n available monitors. Therefore, a subset $G = \{G_1, G_2, \ldots, G_g\}$ is selected from the $M = \{M_1, M_2, \ldots, M_n\}$ monitors, where $G \subseteq M$, i.e, G is a subset of M and $g \leq n$. The subset G has a well-known distributed geo-location $GL = \{gl_1, gl_2, \ldots, gl_g\}$, where $GL \subseteq L$. Figure 2 shows the visualization of RTT tests from the G monitors to N.

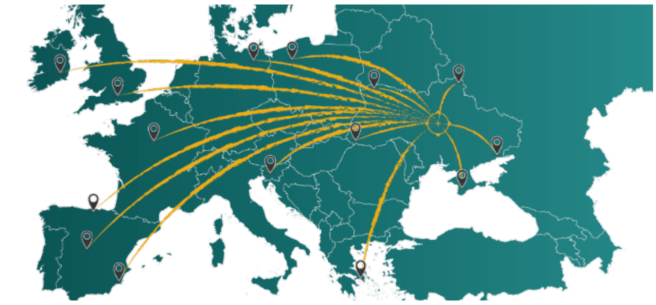

Figure 2. Proof of Offset Algorithm – Phase 1: General RTT_{array} calculation.

Once the performance has been carried out, an initial RTT_{array} obtains with the RTTs from each G_i node with N. At this stage, we determinate the Monitor M', which has the minimal RTTs, i.e. minimal latency from the obtained values in the RTT_{array} in order to determinate the candidate country for the Node N. Therefore, $M' = \min_{\forall\, m \in Gj} RTT_{array}(m)$.

Since, we know the geo-location $gl_{m'}$ from M'. Then, we know the country C that M' belongs to, which is part of the data that we have obtained from Fed4FIRE testbed, as part of their information and description.

The second phase of the algorithm selects the subset $F = \{F_1, F_2, \ldots, F_f\}$ from the $M = \{M_1, M_2, \ldots, M_n\}$ monitors, where $F \subseteq M$, $f \leq n$, and the geo-location $FL = \{fl_1, fl_2, \ldots, fl_f\}, where\ FL \subseteq L$ and $\forall fl_i$ are from the Country C.

At this moment, it is when Proof of Offset analyses deeply the minimal offsets and variations of RTT with respect to the Monitors F located at the same country that the target node N. Then, Proof of Offset algorithm carries out a cross-validation among all the F nodes as presented in Figure 3.

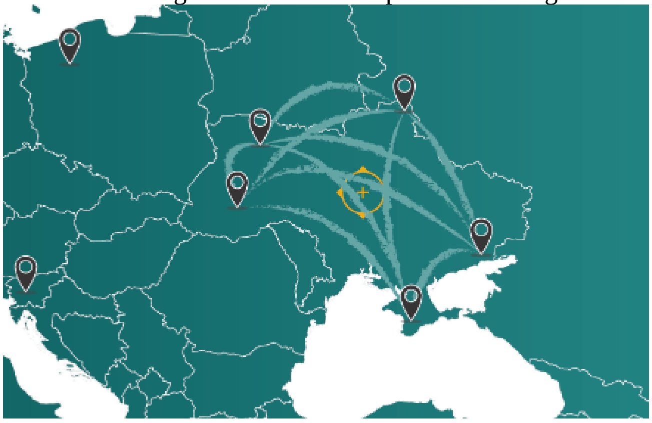

Figure 3. Proof of Offset Algorithm – Phase 2: Fine-grain POO_{matrix} calculation.

Therefore, we obtain a new RTT_{array} with all the RTT values from the F Monitors with respect to the Node N, which could be a subset of the previously obtained RTT_{array} in case that the F monitors were already selected as part of G. Then, we obtain the POO_{matrix} that includes all the RTT values from all the F monitors.

Presuming that the Euclidean distance between nodes in a map is related to the RTT real network distance on average and taking into account the offsets among all the nodes in the cross-validation among the f monitors, then we define a classification algorithm to identify the probability that N being mapped to a particular location at the same country C taking into account the reference monitors F. Additionally, the classification algorithms consider the available M monitors that are not contained in F, the historical values of POO_{matrix} in the $POOHistorical\_dataset$, and $ThirdParty\_datasets$ such as the King Data Set [26] or Caida DNS root/gTLD RTT dataset [27], since these datasets reflect how is the current status of the network and how the nodes could be

[1] FED4FIRE experimentation is available: https://www.fed4fire.eu/run-your-experiment/

[2] Planet-Lab Visualizer: http://plvisualizer.sourceforge.net

influenced by several factors, including remote server loading, congestion within Internet routes, route changes, and local effects such as link or equipment failures.

The classification of N's location is then done by the use of a supervised classification algorithm such as Box-Jenkins has been considered, i.e., an Autoregressive Moving Average model (ARMA) for the analysis of the time series provided by the $dataset$ along the time. Thereby, it allows to identify via the Autoregressive part the values of the variable on its own lagged (i.e., past) values in the dataset for the POO_{matrix} from previous F nodes among them ($POOHistorical\_dataset$) and the moving average for modelling the error term as a linear combination of error terms occurring contemporaneously and at various times in the past, where it can be also considered the current status and congestion of the network that could introduce some variability and error term ($ThirdParty\_datasets$) . Additionally, other algorithms such as instance-based learning (IB1), supported vector machine algorithm (SVM) and data mining classification techniques are also being considered.

IV. Opportunities for Proof of Offset algorithm

It is remarkable that even when it has presented with a high level of simplicity, GEO-TRUST work address all the following challenges around POO algorithm:

- Detecting when a client is connected via a Proxy or a rely node, for this purpose, the introduction of Proof of Work approach can be considered to validate actual node location and detect minimal variations (offsets) that allow to identify this case of abnormal situations.
- Network distance problems such as triangle inequality [18]. For that purpose, POO needs to define the proper trade-off among number of monitors to be considered at the General (G) and Fine-grain (F) phases, in order to make it optimal in performance without impacting negatively in the classification rates.
- European nodes are clustered closely together, which makes geolocating more focused on indicting and detecting if a node located within Europe and not moved to another continent for instance, however it would imply some challenges to identify if a node is geo-located in Switzerland or a surrounding country. For this kind of problems, POO identification of minimal variations / offsets will allow to identify these differences with respect to the state of the art approaches.
- Third party datasets depend on the availability of publicly available datasets, which may get outdated over time. Thus, POO has defined its historical dataset that will be constructed by the help of collaborative users with the same interest in policy compliance, in order to gradually remove any usage of third party datasets. Finally, POO will be available for any other technology such as blockchain nodes willing to provide the geographic location of a node and willing to perform basic RTT measurements are in a position to create a fully distributed up-to-date knowledge base.
- Byzantine attacks or coordinate inflation, deflation and oscillation attacks can be also considered for distributed networks such as blockchain, since as much as network is evolving toward distributed approaches much more vulnerable it is to Byzantine attack [28]..

V. Conclusions and Future Works

GEO-TRUST is exploring how to valorize POO algorithm over different Internet emerging networks and architectures such as Virtualized infrastructure based on SDN/NFV for 5G, Distributed Ledger Technologies such as blockchain and IoT. GEO-TRUST will address for each one of the three architectures addressed.

Opportunities over Virtualized infrastructure (SDN/NFV) for 5G

- **Evaluation of the SDN/NFV implications in terms of geo-location and end-to-end reliability.** It is remarkable that SDN are featured by enabling a common MAC / link layer, making transparent the geo-graphical distribution. Therefore, POO extensions focused on detecting proxies and rely nodes will be also leveraged for detecting the use of virtual infrastructures and when traffic are tunnelled.
- **Geographical allocation optimization**. Virtualization offers hybrid deployments between edge/fog and cloud computing environments bring benefits from flexible applications deployment in terms of agile capacity to extend services/resource and the network, at the same time that also provide an enhance security/privacy based on the allocation of the data. GEO-TRUST will explore the potentials use of POO for defining where to allocate services and applications taking benefit of network programmability.

Research challenges and opportunities for Proof of Offset algorithm over DLTs such as blockchain

- **Consensus algorithms enhancements based on geo-graphical dispersion validation**. Blockchain technology is enabling scalability and extensibility to other domains, at the same time that provides a secure consensus platform where smart contracts are basis for enforcing privacy rights. However, Consensus algorithms are vulnerable when an excessive decision power is relayed on a specific institution, which can lead to Byzantine General problem, when an entity or group of entities have more than 33% of the consensus power, they can influence the general decision. Therefore, geo-graphical dispersion validation via POO brings the value of to verify geographical dispersion of consensus. For that reason, GEO-TRUST will provide a byzantine fault tolerant geo-location system even when it is based on distributed networks.

- **Trust management via explicit consent, traceability and transparency.** On top of this network, data-driven added value services would be implemented. Blockchain's transparency gives visibility to all transactions for approved users, and this may decrease auditors' work with sampling and validating transactions [29]. Therefore, POO will empower with a responsible use of data, establishing trust through transparency and accountability demonstrating where data is being used geographically as an added value to data owners as part of the compliance with GDPR and DPA regulations.

Research challenges and opportunities for Proof of Offset algorithm over IoT and M2M networks

- **Performance optimization and lightweight implementation.** A key challenge is to define the optimal number of monitors to get a high level of trust, i.e, generate the correct geo-location estimation, at the same time that we provide an adequate scalability and performance. At the same way that exploring how to re-use historical data and third-party data sources would impact in the POO performance.
- **Support of Lossy and Low Power Networks.** IoT networks statistically lose messages, therefore we need to manage some inconsistent state when all the messages are not received from the all monitors.

ACKNOWLEDGMENT

This work has been sponsored by Hasler Foundation (http://www.haslerstiftung.ch/en/)

REFERENCES

[1] European Commission, European Data Economy and Non-personal Data Regulation, European Commission, https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy 2017

[2] Fraser, D. (2007). The canadian response to the USA Patriot Act. IEEE Security & Privacy, 5(5).

[3] Shavitt, Y., & Zilberman, N. (2011). A geolocation databases study. IEEE Journal on Selected Areas in Communications, 29(10), 2044-2056.

[4] Poese, I., Uhlig, S., Kaafar, M. A., Donnet, B., & Gueye, B. (2011). IP geolocation databases: Unreliable?. ACM SIGCOMM Computer Communication Review, 41(2), 53-56. http://www.ip2location.com

[5] Ries, T., Fusenig, V., Vilbois, C., Engel, T. (2011, December). Verification of data location in cloud networking. Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on (pp. 439-444).

[6] Dabek, F., Cox, R., Kaashoek, F., Morris, R. (2004, August). Vivaldi: A decentralized network coordinate system. In ACM SIGCOMM Computer Communication Review (Vol. 34, No. 4, pp. 15-26).

[7] Chen, Y., Xiong, Y., Shi, X., Deng, B., Li, X. (2007). Pharos: A decentralized and hierarchical network coordinate system for internet distance prediction. In Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE (pp. 421-426).

[8] Chen, Y., Wang, X., Song, X., Lua, E. K., Shi, C., Zhao, X., Li, X. (2009). Phoenix: Towards an accurate, practical and decentralized network coordinate system. In International Conference on Research in Networking (pp. 313-325). Springer, Berlin, Heidelberg.

[9] Padmanabhan, V. N., Subramanian, L. (2001). An investigation of geographic mapping techniques for Internet hosts. In ACM SIGCOMM Computer Communication Review. Vol. 31, No. 4, pp. 173-185). ACM.

[10] Katz-Bassett, E., John, J. P., Krishnamurthy, A., Wetherall, D., Anderson, T., Chawathe, Y. (2006). Towards IP geolocation using delay and topology measurements. In Proceedings of the 6th ACM SIGCOMM conference on Internet measurement (pp. 71-84). ACM.

[11] Youn, I., Mark, B. L., Richards, D. (2009). Statistical geolocation of Internet hosts. 18th IEEE Internatonal Conference on Computer Communications and Networks, ICCCN 2009. (pp. 1-6)

[12] Ng, T. E., Zhang, H. (2002). Global network positioning: a new approach to network distance prediction. Computer Communication Review, 32(1), 73.

[13] González, S., Oliva, A., Costa‐Pérez, X., Di Giglio, A., Cavaliere, F., Deiß, T., Mourad, A. (2016). 5G‐Crosshaul: An SDN/NFV control and data plane architecture for the 5G integrated Fronthaul/Backhaul. Transactions on Emerging Telecommunications Technologies, 27(9), 1196-1205.

[14] Blanco, B., Fajardo, J. O., Giannoulakis, I., Kafetzakis, E., Peng, S., Pérez-Romero, J., Sfakianakis, E. (2017). Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN. Computer Standards & Interfaces, 54, 216-228.

[15] Aissioui, A., Ksentini, A., Gueroui, A. M.,Taleb, T. (2015). Toward Elastic Distributed SDN/NFV Controller for 5G Mobile Cloud Management Systems. IEEE Access, 3, 2055-2064.

[16] ETSI, Open Source MANO (2017), http://www.etsi.org/technologies-clusters/technologies/nfv/open-source-mano

[17] Pureswaran, V., Brody, P. (2015). Device democracy: Saving the future of the Internet of Things. IBM Corporation. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03620USEN

[18] Lamport, L., Shostak, R., Pease, M. (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3), 382-401.

[19] Vermesan, O., Friess, P. (Eds.). (2013). Internet of things: converging technologies for smart environments and integrated ecosystems. River Publishers.

[20] Gavras, A., Karila, A., Fdida, S., May, M., Potts, M. (2007). Future internet research and experimentation: the FIRE initiative. ACM SIGCOMM Computer Communication Review, 37(3), 89-92. https://www.ict-fire.eu

[21] González, G., Pérez, R., Becedas, J., Latorre, M. J., Pedrera, F. (2014, September). Measurement and modelling of PlanetLab network impairments for Fed4FIRE's geo-cloud experiment. In Teletraffic Congress (ITC), 2014 26th International (pp. 1-4). IEEE. https://www.fed4fire.eu

[22] Lux, T., Mathys, V. (2018). FINMA, FINMA publishes ICO guidelines, FINMA Oficial News, https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[23] Emtseva, S. S., Morozov, N. V. (2018). Comparative Analysis of Legal Regulation of ICO in Selected Countries. KnE Social Sciences & Humanities, 3(2), 77-84.

[24] Komosny, D., Pruzinsky, J., Ilko, P., Polasek, J., Masek, P., Kocatepe, O. (2015). On geographic coordinates of PlanetLab Europe. In Telecommunications and Signal Processing (TSP), 2015 38th International Conference on (pp. 642-646). IEEE. https://www.planet-lab.eu

[25] Komosny, D., Mrdovic, S., Ilko, P., Grejtak, M., Pospichal, O. (2017). Testing Internet applications and services using PlanetLab. Computer Standards & Interfaces, 53, 33-38. https://www.planet-lab.org

[26] Gummadi, K. P., Saroiu, S., Gribble, S. D. (2002). King: Estimating latency between arbitrary internet end hosts. In Proceedings of the 2nd ACM SIGCOMM on Internet measurment (pp. 5-18). ACM.

[27] Brownlee, N., Claffy, K. C., Nemeth, E. (2001). DNS Root/gTLD performance measurements. USENIX LISA, San Diego, CA.

[28] Kaafar, M. A., Cantin, F., Gueye, B., & Leduc, G. (2009). Detecting triangle inequality violations for internet coordinate systems. In Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on (pp. 1-6). IEEE.

[29] By Ken Tysiac (2017). Blockchain: An opportunity for accountants? Or a threat?. Journal of Accountancy. Information Management and Technology Assurance.