EphemeriShield – Defence Against Cyber Anti-Satellite Weapons

Rafal Graczyk, Marcus Voelp
University of Luxembourg, Interdisciplinary Centre for Security Reliability and Trust
6, avenue de la Fonte, L-4364 Esch-sur-Alzette
LUXEMBOURG

rafal.graczyk@uni.lu

marcus.voelp@uni.lu

ABSTRACT

Mitigating the risks associated with space system operations, especially in Low Earth Orbit, requires a holistic approach, which addresses, in particular, cybersecurity challenges, in addition to meeting the data acquisition requirements the mission needs. Space traffic management systems form no exception to this rule but are further constrained by backward compatibility requirements that sometimes are based on decades old foundations. As a result, some space situational awareness systems continue to operate with object catalogues and data dissemination architectures that are prone to failures, not to mention adversarial actions. Proof-of-concept papers, demonstrating this vulnerability in example attacks on space object ephemerides distribution channels have already been published and show the urgency in rethinking the way we build such high-critical infrastructure. Leveraging recent developments of distributed systems theory and concepts from multi-party consensus in limited-trust environments and in the presence of malicious actors, we designed a more secure system for orbital object ephemerides distribution, ultimately targeting at increasing the safety of satellite operations. This paper presents EphemeriShield, *a distributed ephemerides storage and distribution system, aiming at maintaining safety and security guarantees in presence of active attacker or unfortunate fault. Using our* EphemeriShield *prototype setup, we were able to prove its ability to mask attacks and local faults that otherwise would lead to unnecessary manoeuvres. Wide adoption of* EphemeriShield *may help satellite system operations to become safer and less vulnerable to intentionally adversarial activities, which improves the overall sustainability of space.*

KEYWORDS

Cybersecurity; Small satellites; Space surveillance and tracking; Specialists' meeting, Space traffic management

1.0 INTRODUCTION

Satellites are both crucial and, despite common belief, fragile parts of our civilian and military critical infrastructure. While, many efforts focus on securing the ground and space segments, especially when national security or business interests are affected, this is unfortunately not yet the case for small-sat operations and the NewSpace revolution. Both aim at democratising access to and exploitation of near-earth orbits. New players keep arriving on the market, typically in the form of small and medium-sized companies, offering new and more affordable services. Despite the necessity and inevitability of this process, it also opens new venues for targeted attacks against space-related infrastructures. Small organisations, with less established revenue models, have a natural incentive to cut-corners in search for lower cost and faster time-to-market solutions [1]. While there are many classical Anti-SATellite (ASAT) weapons using various kinds of effectors (kinetic, RF, laser, etc.), we recently observed a proof of concept, demonstrating a further attack of this kind [2], following

a more cybernetic approach to attack the information sphere, rather than causing a direct energy transfer in orbit.

Satellite operators know their own space assets very well, where they are located and with what orbital parameters they are flying (e.g., from GNSS receivers on board of their spacecrafts or from their own tracking and ranging facilities). What these operators typically cannot derive by just relying on their own means of observation are the locations and orbital parameters of other objects, such as active and inactive satellites, but more importantly, fields of space debris on a potential collision course [3] [4]. Instead, they obtain information about such objects by querying Two-Line Element (TLE) debris files provided by Celestrack or Space-Track or a few other sources. The devastating consequences of triggering Keppler's syndrome in orbital collisions are well known to this audience [5], leaving it without saying that we need to avoid them. For that reason, orbital conjunction assessment aims at foreseeing possible close encounters, threatening the well-being of satellites, monitoring changes of the orbital situation, and engaging in collision avoidance manoeuvres, to the degree that propulsion or attitude manipulation allow [6]. However, if misused, this avoidance poses another threat: Cyber-ASAT [2] describes a method for altering TLE debris to orchestrate fake alarms and unnecessary collision avoidance manoeuvres, targeting satellites to exhaust their fuel or to disrupt their availability during collision avoidance. The spectrum of TLE attack possibilities (altering or spoofing) is wide:

- Malicious Space Surveillance and Tracking (SST) system operators could intentionally alter the TLE;
- External groups could intentionally alter the TLE provided to satellite operators (e.g., by hacking into their SST user front-end or by performing a man-in-the-middle attack);
- TLE altering could also happen unintentionally, as a result of an error.

The consequences of TLE spoofing attacks are diverse and may include fake collision avoidance alarms, spanning from seemingly low critical, but unnecessary manoeuvres to the waste of propellant, but they may also include potentially orchestrated activity, launching organised attack campaigns on some third party, by tricking several space-asset operators into undertaking actions that increase the collision likelihood with that party's space assets. It is not that unlikely, since, despite the vastness of space, not all orbits are equally useful, and space assets keep being placed only in a few crowded regions, as presented in Figure 1 and Figure 2.

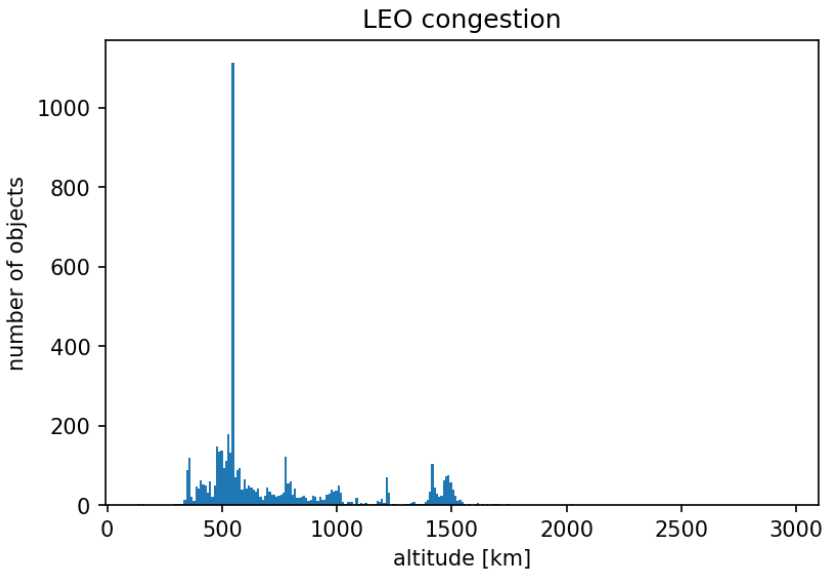

Figure 1: Distribution of objects in LEO at various altitudes

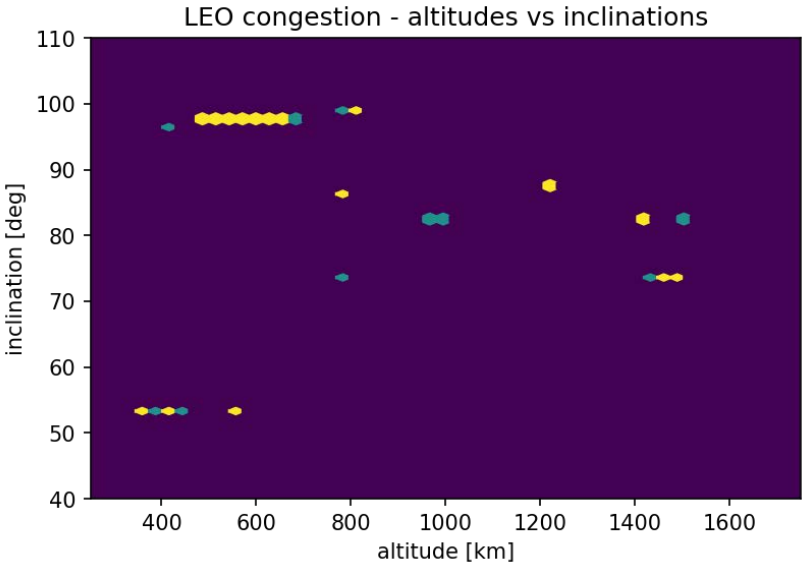

Figure 2: Distribution of objects in LEO at various altitudes and inclinations

2.0 BACKGROUND INFORMATION

Safety and security of space operations is ensured by Space Situational Awareness (SSA) or, if one deals with movement or kinetic interference between objects, by Space Surveillance and Tracking (SST) and Space Traffic Management (STM) systems. The SSA, dealing mainly with the surveillance and tracking of anthropogenic objects, in addition, often includes near-Earth natural object detection and space weather monitoring [7]. SSA processes are about building knowledge about where man-made space objects are in order to forecast their trajectories, especially for the purpose of avoiding potential collisions. Subjects of interest for SSA are active and defunct payloads, but also upper stages of launchers that did not deorbit and a significant number of pieces of debris. Space Traffic Management [8] comprises the set of technical and regulatory provisions for promoting safe access to outer space, safe operations in outer space and safe return from outer space to Earth, free from physical or radio-frequency interference. It extends SSA. STM attempts to harmonize space operations, with the goal of reaching safety (non-interference) by orchestrating data collection (from civil and military sensors), data processing (cataloguing objects and their orbital information), data product (warning dissemination), coordination (of operations, standards, guidelines) and data distribution (linking data sources with data users) [1].

Data collection is a process of conducting optical, laser and radar observations for the purpose of detecting objects in space and estimating their orbits. Sensing has been traditionally conducted by military, governmental or international organisations (such as the US Air Force Space Fence, the European Space Agency SSA programme), and advanced Russian and Chinese SSA infrastructure, with many other countries quickly catching up [1]. In recent years, commercial sources became available as well, like LeoLabs radar sensing or Sybilla Technologies and Officina Stellare's autonomous, optical observation networks. Obviously, different types of sensors exhibit different properties and performance. Sensor networks for SSA have been extensively analysed in the literature [9]. In particular, it has been established that increasing the number of lower performing sensors will not contribute to a further decrease of detection uncertainties [10]. However, increasing the number of sensors, their diversity and spatial distribution would contribute positively to the availability and, if processed correctly, resilience of orbital parameters [11], [12], [13].

Data processing is, by its very nature, intertwined with data product generation and closely coupled to data distribution infrastructures. Distribution mechanisms, especially in recent years have gained significant

interest. Several developments have been conducted in classical IT architectures, microservice-based platform architectures for dissemination of SSA data sharing and experimentation [14]. Chen et al. [15] augmented the SSA data distribution system with task planning, distribution and supervision for constellation management. MacLeod presented an SSA data distribution and processing system, at NASA, including advanced analytics information fusion and multi-entity integration systems [16]. NASA, in addition, is conducting an agency-level program for conjunction assessment data products, which includes all assets under their investigation and which provides advisory services for the manoeuvre planning of satellite system operators [17]. Comparable services have been established by the European Space Agency for managing European space assets [18]. Academic organisations develop similar capabilities for space event information data acquisition, modelling, simulation for scientific and educational purposes and research on active debris removal [19]. SOCRATES [3], provides service to the satellite operator community, distributing the conjunction reports and collision alerts, using TLE data that is made available by military operators. Similar services of conjunction assessment have been exercised by commercial entities, LeoLabs together with Planet, where radar measurements from LeoLabs were validated against the "true" orbits, provided by the International Laser Ranging Service (ILRS), and against measurements from Planet's on-board GPS instrumentation. The radar data was further used to form the basis of a conjunction assessment [6].

Generation of data products from acquired orbital ephemerides, namely conjunction assessments and collision warnings, in the presence of (unavoidable) uncertainty has also drawn some attention in the academic community. Delande et al. [20] propose algorithms for enhancing tracking performance, and for embracing uncertainties by fusing human-based data sources with physics-based data sources. Ma et al. [21] elaborate on the reliability of collision probability assessments, including those resulting from false or missed alarms. They further provide a manoeuvring cost estimation framework to support decision making processes. In a similar fashion, false confidence in the conjunction assessment validity, stemming from probability dilution phenomena, where quality data appear to reduce the risk of collision, has been analysed by Balch et al. [22]. Cai and Jah [23] proposed a sensor fusion method for space object tracking, which overcomes the limitations of typically used averaging consensus algorithms. They include relative accuracy of local inputs in weighted approximation and ensure better robustness by adaptively determining fusion weights based on information gained from local estimates.

Organisations like the Consultative Committee for Space Data Systems (CCSDS) are responsible for creating and evolving standards, which take cybersecurity good practices as a solid foundation for building the protocols, data formats and systems, ensuring confidentiality, integrity and, where possible, availability. While extremely useful, those approaches can only make it harder for malicious actors to breach cybersecurity, however, when the system is already compromised, good security practice cannot help much to tolerate and operate safely through the attack. Fault and Intrusion Tolerance, advocated by many, comes with a promise of providing selected safety and security guarantees, even while the system is under attack and even if such attacks are partially successful.

In this context, distribution of SSA data is a crucial part of Space Traffic Management architectures. In recent years, awareness grew that SSA distribution is a typical example of a critical infrastructure that may be subject to threats from malicious actors, attacking the integrity and authenticity of distributed data, as pointed out in the introduction. Fault and Intrusion Tolerance principles, as a high, state-of-the-art, form of cybersecurity and cyber-safety, have already been evaluated as a remedy that could quickly increase the resilience of SSA systems. Reed proposed a distributed blockchain as an alternative to the single owner/operator information sharing model. The proposed system is augmented with automatic discovery of behavioural anomalies, captured and recorded as evidenced by Reed et al. [24]. Others went even further, proposing to combine ground SSA distribution systems with space segment manoeuvre control, in one, blockchain based system [25]. The latter concept, however, would require implementing trusted components that would need to be able to take over the control of space assets, which currently is not very practical. With the quick growth of mega-constellations, this need for manoeuvring automation might become unavoidable. More feasible near-term solutions include developing a distributed ledger for data acquisition and distribution decentralisation (using

e.g., the Hyperledger framework) where no single entity is responsible for holding and processing the SSA data, while the system presents itself to users as a single entity. Such systems allow reducing the trust between parties by relying on computer protocols for data manipulation and storage [26]. Permissioned blockchains suggest themselves as participants need not be anonymous, which allows parties to be held accountable for injecting unreliable data. On the other end of spectrum, Surdi [27] proposed to use a fully anonymous, public blockchain, like Ethereum, to provide very similar functionality. This concept also evaluated the possibility of utilising the space segment for automated manoeuvring.

There is no doubt that nowadays we are experiencing a huge shift in the way near space is used, by whom and for what purpose. Widespread proliferation of small satellite technologies and an exponential growth in the number of deployed payloads also requires profound changes in the ways we manage and use space and how we approach cooperating with other stakeholders. It is also the right moment to accept the fact that resilience of space situational awareness architectures, and their derivatives, is more critical than ever and will become subject of more and more advanced threats [28]. Perhaps, it is the moment, due to proliferation of sensing capabilities, where SSA or SST data shall not be treated as a trade or national security matter but as a commodity enabling safe and secure access and the utilisation of space for all actors [1], [29] [30].

3.0 EPHEMERISHIELD CONCEPT

In this work, we propose a solution to the presented problem in the form of a distributed system that will have no central authority responsible for storing and disseminating catalogues of objects orbiting Earth together with information about their orbital parameters. Instead, each peer that participates in the system will have full access to all records stored in the system. Peers distribute data in a consensual manner, ensuring information replication at each peer's node. This way, single point of failure syndromes of classic systems are removed, which currently exist in the traditional direct ephemerids distribution mechanisms. Our proposed solution is to build data dissemination systems using permissioned, private ledgers where peers have strong and verifiable identities, which further allows for redundancy in SST data sourcing. Each partner that provides object localisation data can be held responsible for low quality information, identified as doing so and excluded in the future.

In our proposed solution, object data (unique identifier and ephemerids) is stored in a blockchain. The chaincode runs in the system and defines an asset (in this case, orbital elements of objects under tracking) and transactions. Chaincode comprises the operations that are associated with a designated blockchain systems. Transactions are the instructions for how to modify an asset and embed algorithmic criteria to decide whether to update an object's orbital elements, request for conjunction analysis and whether to distribute warnings.

Our EphemeriShield architecture is based on Hyperledger Fabric, which is a distributed database extended with a data-processing engine and with the means to exhibit Byzantine fault-tolerance [31]. That is, the database can tolerate up to a configurable number of its components to behave arbitrarily, even in an intentionally malicious way. Operations in the Hyperledger Fabric, and therefore also in EphemeriShield, follow the transaction processing flow shown in Figure 3.

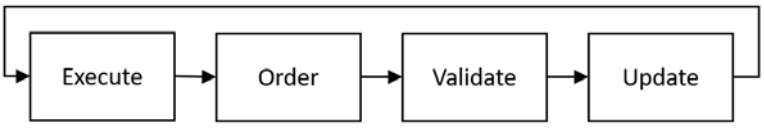

Figure 3: Hyperledger Fabric transaction processing flow

A peer in the network, which intends to provide new orbital parameter information submits such a request to the system, thereby becoming a client node. The client's request and its content are distributed among the peers implementing EphemeriShield. Each of these peers executes the request, performs predefined and updateable processing steps by executing the chaincode (which could further be extended to sanitise submitted data and to perform plausibility checks) and records and distributes the results. At the same time, the peer endorses what other correct peers have prepared and marks incorrect results that it detects. Following this, a separate, system level service produces a total order within the transaction set to assist validation. In the third step, transactions are validated with respect to the system's policies and a sufficient number of endorsements are collected from the peer pool that guarantees that the behaviour of faulty peers got masked. If all the requirements are met the transitions, in the defined order, update the ledger, storing ephemerides, along with their metadata or auxiliary information.

Clearly, based on what we wrote so far, at least three type of peer nodes can be identified in our system:

- SST data providers, contributing to updating the database with new orbital elements as soon as they are detected by physical measurements.
- SST data users, who are interested in obtaining up-to-date orbital elements information on objects they control; and,
- a third type, which commonly could be the same as the second, looking for conjunction analysis results, which will raise alerts on future proximity events.

This third type requires significant data-processing capabilities, as conjunction candidate objects need to be selected (whose number could be substantial, especially on Low Earth Orbit (LEO)). The orbits of such candidates need to be propagated for some time into the future (depending on the quality of used models, usually no longer than a few days ahead) to check for possible close proximity passes. However, with today's high data-processing capabilities, this should not pose any organisational or technical problems to a large majority of ground segment facilities.

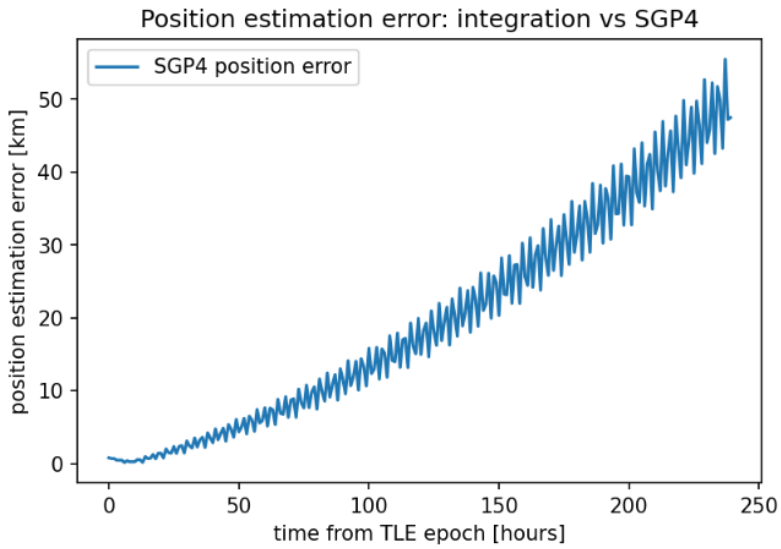

Figure 4: Position estimation error using SGP4 analytical solution w.r.t numerical integration baseline (Cowell method with J2 perturbation model)

In order to keep the blockchain size reasonable, only recent system snapshots (i.e., the state of all objects in the catalogue) and transactions relating to them need to be kept. This is possible due to fact that ephemerides

older than few days become useless for predicting the current position and velocity of an object on orbit, as numerical propagators, but especially popular SGP4, used with TLEs, cannot take into account all the perturbations that affect the orbital movement of bodies. In LEO, these perturbations can be significant. The resulting propagation errors would be too large (refer to Figure 4). On the other hand, keeping the catalogue with historical data is valuable for scientific purposes and, perhaps, could also serve as an evidence base for keeping stakeholders accountable to their actions in the event of having to settle disputes over consequences of kinetic or RF interference that could happen between space assets in the future.

As all the operations on the surveyed objects catalogue are immutable and traceable (thanks to the permissioned, ledger-based, blockchain) it is possible to assign financial value to the use of the system, as incentive for participants to provide correct and high-quality data. Eventually, such an additional mechanism would lead to a quite desirable outcome: SST data providers and analysers could have their costs covered (at least to some extent) by the users of their data. Incentives embedded in the proposed mechanisms, along with the independence from a central authority, and redundancy in data sources and data processing may further lead to a democratisation of access to SST information, which contributes to the stability of the system, providing trust without the need of central enforcement.

All information injected into the system has to pass sanity checks, validating the feasibility envelope of provided parameters by numerical propagation with respect to the last inputs or with respect to other ephemerids provided by other SST data sources. A basic algorithm for orbital elements validation before adding them to ledger is outlined in Figure 5. Each entry in the orbital data ledger consists of an object identification number (there are few regimes in which objects can be identified, which are relevant, so this field will have several subfields, each for a different ID number), epoch (moment in time) for which the ephemerides have been collected, and the ephemerides data itself, which typically are the orbital elements required for an unambiguous definition of an object's orbit. Classically, these are the semi-major axis, eccentricity, inclination, right ascension of ascending nodes, argument of perigee, and the true anomaly. When the new ephemerides are available for the object (i.e., it has just been tracked by sensing facility in the network), before they are stored on the ledger, they need to pass the sanity check. The sanity check takes the last ephemerides set for a given object and numerically propagates the objects position forward to the epoch of the new, proposed, ephemerides. If the propagated and newly proposed position are within an acceptable error range (i.e., error ellipsoid) for a given sensor and numerical propagator, the new orbital elements set can then automatically be appended to the ledger. After all values are checked, sanitised, and accepted by the chaincode, which governs data entry, a transaction is added to the blockchain and made visible to all participants in the system, which update the ephemerids catalogue. In case of discrepancy or detection of non-feasible SST data entries, a warning is raised for manual intervention. This way, discrepancies reveal measurement errors, attempts of intentional information modification or significant orbital manoeuvres without prior information.

```
1  on new ephemerides entry (object_i, epoch_new, OE_new):
2    (OE_old, epoch_old) := retrive_last_ephemeris(object_i)
3    OE_prop := propagate(OE_old, epoch_old, epoch_new)
4    if |OE_new − OE_prop| < ϵ:
5      append_ephemerides(object_i, epoch_new, OE_new)
6    else:
7      raise_warning(object_i, epoch_new, OE_new)
```

Figure 5: Orbital Elements entry check algorithm

Whenever a new orbital element is submitted to the database, previous information existing in the database has to be used to verify the correctness of the new entry. Since all assets operating in space are subject to the same, known, laws of physics, their future behaviour can be predicted, with some accuracy. In case of

scheduled orbital manoeuvres, their influence on orbits, if conducted correctly is also, to large extent, deterministic. The process presented here (Figure 6) is not that much about sensor data fusion or decreasing of uncertainty, but more about detecting anomalous behaviour, non-compliance to regulations, non-compliance to declared manoeuvre plans or detecting manoeuvring without prior notice. This process detects both, the physical behaviour of space assets recorded by a non-faulty sensor or made-up behaviour provided by faulty or compromised sensor facilities or networks.

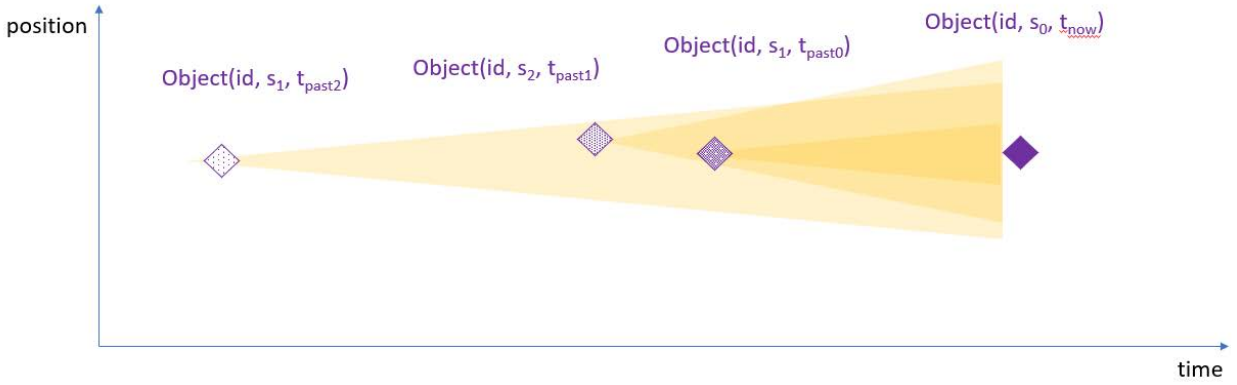

Figure 6: The Orbital Elements entry sanitisation concept

4.0 CONCLUSION

Proliferation of miniaturised technologies has led to an exponential growth in the number of objects that occupy very similar and therefore also very crowded orbits. Along with the expansion of commercial activities into near space, societal dependence on service providers also increase through these means. Space assets, become a vital part of our societies' critical infrastructure, and their safety and security of operation is often overlooked.

In this paper, we have presented EphemeriShield, an orbital elements distribution system, as an answer to some of the challenges imposed by the very fast evolution of how we use space. The method presented here allows for quick checks of whether a space asset's orbital parameter information, provided by sensing facilities or STM organisations, meet minimum plausibility criteria or are suspected of being the result of faults or security incidents and must therefore not be trusted.

It is worth noticing that the system design approach we propose is not at all aimed at replacing existing cybersecurity measures. Instead, it builds on top of them, contributing another layer of protection against malicious behaviour, by utilising various, and most important, independent sources of SSA information. With growing awareness in the space community that ground infrastructure is critical and that STM is one of them, the numbers of organisations that deploy SSA facilities will increase and EphemeriShield will from a stronger last line of defence against faults and intrusions.

Our EphemeriShield prototype is currently at TRL 2-3, at the stage of concept formulation along with first experimental validations, including orbital elements sanitisation and malicious orbital elements set modifications. Discussions on obtaining several, continuous, independent, streams of satellite tracking data to be fed into our prototype and to further evaluate our system, are ongoing and we would be happy to collaborate in a partnership to further develop and validate EphemeriShield in the production-like environment of satellite system operators.

7.0 REFERENCES

[1] Lal, B., Balakrishnan, A., Caldwell, B.M., Buenconsejo, R.S. and Carioscia, S.A. (2018). Global Trends in Space Situational Awareness (SSA) and Space Traffic Management (STM). The Institute of Defence Analysis, Washington DC.

[2] Pavur, J., and Martinovic, I. (2019). The Cyber-ASAT: On the impact of cyber weapons in outer space. In: 2019 11th International Conference on Cyber Conflict, May 2019, pp. 1-18.

[3] Kelso, T.S. and Alfano, S. (2006). Satellite orbital conjunction reports assessing threatening encounters in space (SOCRATES). In: Proceedings of SPIE – The International Society for Optical Engineering, Volume 6221, id. 622101.

[4] 18th Space Control Squadron (2019). Spaceflight Safety Handbook for Satellite Operators, Joint Force Space Component Command.

[5] Kessler, D., Johnson, N., Liou, J.C., and Matney, M. (2010). The Kessler Syndrome: Implications to future space operations. Advances in the Astronautical Sciences, 137.

[6] Nicolls, M., Vittaldev, V., Ceperley, D., Creus-Costa, J., Foster, C., Griffith, N., et al. (2017), Conjunction assessment for commercial satellite constellations using commercial radar data sources. In: Advanced Maui Optical and Space Surveillance (AMOS) Technologies Conference, Jan 2017, p. 18.

[7] Wikipedia.org. Space situational awareness programme. https://en.wikipedia.org/wiki/Space_Situational_Awareness_Programme (accessed 18 Feb 2022).

[8] Wikipedia.org. Space traffic management. https://en.wikipedia.org/wiki/Space_traffic_management (accessed 18 Feb 2022).

[9] Choi, E.J., Cho, S., Jo, J.H., and Park, J.H. (2017). Performance analysis of sensor systems for space situational awareness, J. Astron. Space Sci. 34(4), pp. 303-313. https://doi.org/10.5140/JASS.2017.34.4.303

[10] Vallado, D., Virgili, B., and Flohrer, T. (2013). Improved SSA through orbit determination of two-line element sets. 10.13140/2.1.4644.2241.

[11] Blake, T., Gustin, C., Luu, K., Robertson III, L., Smokelin, J.S., and Zollinger, G. (2012). Ibex: A space situational awareness data fusion program. In: Proceedings of the Advanced Maui Optical and Space Surveillance Technologies Conference, 2012.

[12] Hussein I.I., DeMars K.J., Früh C., Erwin R.S. and Jah M.K. (2012). An AEGIS-FISST integrated detection and tracking approach to space situational awareness. In: 2012 15th International Conference on Information Fusion (FUSION), pp. 2065-2072.

[13] Bellows, C.T. (2015). Leveraging External Sensor Data for Enhanced Space Situational Awareness. PhD Thesis, Air Force Institute of Technology. Theses and Dissertations, https://scholar.afit.edu/etd/1926.

[14] Lu, W., Xu, Q., Lan, C., Lyu, L., Zhou, Y., Shi, Q. et al. (2020). Microservice-based platform for space situational awareness data analytics. International Journal of Aerospace Engineering. 2020. Doi: 10.1155/2020/8149034.

[15] Chen, Y., Tian, G., Guo, J., and Huang, J. (2021). Task planning for multiple-satellite space-situational-awareness systems. *Aerospace* 8(3)3, 73. https://doi.org/10.3390/aerospace8030073

[16] MacLeod, T., Gagliano, L., Mason, S., and Percy, T. (2015). Integrated space asset management database and modeling. In: Proceedings of the Advanced Maui Optical and Space Surveillance Technologies Conference 2015.

[17] NASA. Satellite Safety: CARA conjunction assessment risk analysis. https://satellitesafety.gsfc.nasa.gov/CARA.html (accessed 18 Feb 2022).

[18] Merz, K., Virgili, B.B., and Braun, V. (2017). Current collision avoidance service by ESA's space debris office. In: Proc. 7th European Conference on Space Debris.

[19] Horstmann, A., Kebschull, C., Müller, S., Gamper, E., Hesselbach, S., Soggeberg, K. et al. (2018). Survey of the current activities in the field of modeling the space debris environment at TU Braunschweig. Aerospace – Special Issue "Space Debris: Impact and Remediation." ISSN 2226-4310. 5. 10.3390/aerospace5020037.

[20] Delande, E., Houssineau, J., and Jah, M. (2018). Physics and human-based information fusion for improved resident space object tracking. Advances in Space Research, https://doi.org/10.1016/j.asr.2018.06.033.

[21] Ma, C., and Bai, X. (2014). Analysis of false alarm and missing alarm in conjunction assessment of space objects. Proceedings of the 27th Conference of Spacecraft TT&C Technology in China.

[22] Balch, M.S., Martin, R., and Ferson, S. (2019). Satellite conjunction analysis and the false confidence theorem. In: Proceedings of the Royal Society Series A, 475, 20180565.

[23] Cai, H., and Jah, M. (2021). Consensus credibility particle filter for space object tracking. Proc. 8th European Conference on Space Debris (virtual), Darmstadt, Germany.

[24] Reed, H.G., Dailey, N., Carden, R., and Bryson, D. (2020). Blockchain Enabled Space Traffic Awareness (BESTA): Automated comparison of SSA to agreed behavior for discovery of anomalous behavior, Advanced Maui Optical and Space Surveillance Technologies Conference.

[25] Xu, R., Chen, Y., Blasch, E., and Che, G. (2019). Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness. Opt. Eng. 58(4) 041609. https://doi.org/10.1117/1.OE.58.4.041609

[26] Popp, M., Rogojin, V., Boysan, M.C., and Wallum, M. (2021). SST data trust as a service – Towards secure de-centralised management and exchange of space surveillance and tracking data. In: Proc. 8th European Conference on Space Debris, 2021.

[27] Surdi, S. (2020). Space situational awareness through blockchain technology. Journal of Space Safety Engineering, 7(3), pp. 295-301, ISSN 2468-8967, https://doi.org/10.1016/j.jsse.2020.08.004.

[28] European Space Policy Institute (Jan 2020). ESPI Report 71 – Toward a European approach to space traffic management – Full report. https://espi.or.at/publications/espi-public-reports/send/2-public-espi-reports/494-espi-report-71-stm

[29] Peldszus, R. (2018). Foresight methods for multilateral collaboration in space situational awareness (SSA) policy and operations. The Journal of Space Safety Engineering, https://doi.org/10.1016/j.jsse.2018.07.001

[30] Rovetto, R.J., and Kelso, T.S. (2016). Preliminaries of a space situational awareness ontology. In: Proceedings of AAS/AIAA Spaceflight Mechanics Meeting, in Advances in the Astronautical Sciences. Univelt Inc., pp. 4177-4192.

[31] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., de Caro, A., et al. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. EuroSys '18: Proceedings of the Thirteenth EuroSys Conference, doi: 10.1145/3190508.3190538.