Architecture of a Distributed Space Traffic Coordination System

Christopher Kebschull
OKAPI:Orbits GmbH, Rebenring 33, 38106 Braunschweig, Germany – christopher@okapiorbits.com
Adam Stradomski
OKAPI:Orbits GmbH, Rebenring 33, 38106 Braunschweig, Germany – adam@okapiorbits.com
Daniel Lubián-Arenillas
OKAPI:Orbits GmbH, Rebenring 33, 38106 Braunschweig, Germany – daniel.lubian@okapiorbits.com

ABSTRACT

The rapid increase in active satellites, particularly in low Earth orbit, has led to a surge in conjunction events between operational spacecraft. This paper explores the emerging concept of Space Traffic Coordination (STC) platforms and proposes a vision for a distributed network of interoperable STC systems. Different existing and upcoming platforms are introduced, as well as features that are incorporated in some of them, like in-platform chat, automatic assignment of actions based on industry practices and coordination with non-members of the STC platform, all available in OKAPI:Astrolabe.

This last point introduces the complexities of handling coordination with spacecraft operators that are not part of a given system, as well as how to ensure that information is secure, confidential and coming from the appropriate conjunction partner. Therefore, challenges arising from this are discussed, based on the idea of identity verification for spacecraft operators, and various governance models for such a network are presented, ranging from centralized to decentralized approaches.

The paper examines the pros and cons of different identity verification methods, including platform-specific verification, external identity providers, and decentralized "friend of a friend" models. It also considers the implications of various network governance structures, such as consensus-based approval and champion-based systems.

Drawing parallels with existing technologies like blockchain and decentralized social media protocols, the authors suggest potential technical solutions for implementing a distributed STC network. The paper aims to initiate a dialogue among stakeholders in the space traffic management community to develop a common vision for coordinated space traffic operations.

The authors conclude by emphasizing the benefits of a distributed network in preserving autonomy, fostering innovation, and maintaining transparent data-sharing practices. They call for further research and community engagement to refine these concepts and work towards a prototype implementation based on existing STC platforms.

1. INTRODUCTION

Since the 1950s, artificial objects around Earth have been increasing their numbers steadily. However, since the early 2010's, the growth rate has been significantly greater due to the rapid commercialization of space. This has been the focus of multiple studies that have tried to capture different future scenarios of the debris environment around Earth, concluding that over-excessive traffic in frequently used orbits will render spaceflight to become close-to-impossible over the coming decades ([1]; [2]). Most of these studies were done considering a lower launch rate than the observed in the last years, so their results might be conservative with respect to reality. To mitigate the possibility of rendering used orbits unusable, different applicable laws and industry standards have been developed, setting in place requirements to operators of satellites (i.e. [3]) under the jurisdiction of a law or applicable standard (i.e. [4]) and to enable safe and sustainable use of space. Common to all operational requirements, is the mitigation of collision risk and thus the ability to perform collision avoidance (COLA).

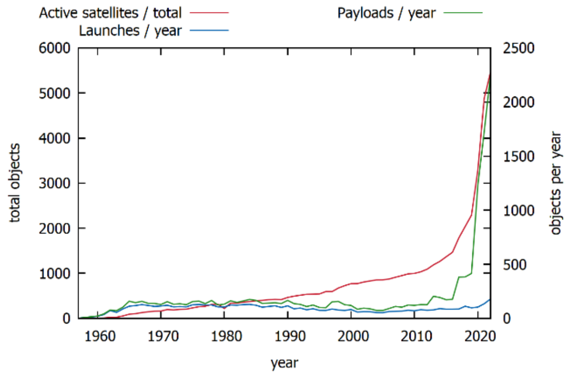

Figure 1. Overview of the evolution of active objects over time (red), as well as the number of launches and launched payloads per year. Data from space-track.org [5].

In the past, most conjunction events were against space debris (inactive objects). However, with the latest trends, close approaches between active satellites are becoming the new norm in the congested low Earth orbits (LEO), particularly between altitudes of 500 km to 550 km (see Figure 1). While for space debris it is possible, under the consideration of more or less known uncertainties, to propagate the determined trajectory using only physical models, active satellites might perform maneuvers, which depending on the orbit, mission constraints and satellite capabilities, might be quite frequent. As such, propagation of orbits based only on past observations for active satellites will lead to less trustworthy data and collision warnings. Only the spacecraft operators can know what the upcoming trajectory might be due to their insider perspective.

Therefore, to build more transparency, it is becoming more and more standard practice to share operational data more actively between satellite operators, including maneuvers as foreseen by the operations schedule. This improves the accuracy of the predicted trajectory of the satellites, leading to a more accurate detection and risk assessment of conjunctions. In geostationary orbits (GEO), this has been coordinated by the Space Data Association for almost 15 years, covering about 50% of the satellites operated in GEO but also including satellites in LEO. In LEO itself, it is getting more common to share the operator's own ephemeris via space-track or other public sources, but this is mostly done by operators of large constellations. Consequently, in this paper, transparency (i.e. data sharing of ephemerides and maneuvers) is considered one of the cornerstones to increase the safety of operators' assets as it allows us to make more accurate collision risk assessments. Nevertheless, in case operators are facing a critical conjunction, it becomes paramount that both operators coordinate the close approach event among each other to avoid (a) the loss of their assets and (b) the generation of space debris. Hereby, coordination is understood as who must act in what ways to mitigate the risk of a potentially critical conjunction. Therefore, coordination is considered as the second cornerstone which is built on top of data sharing as a necessary baseline.

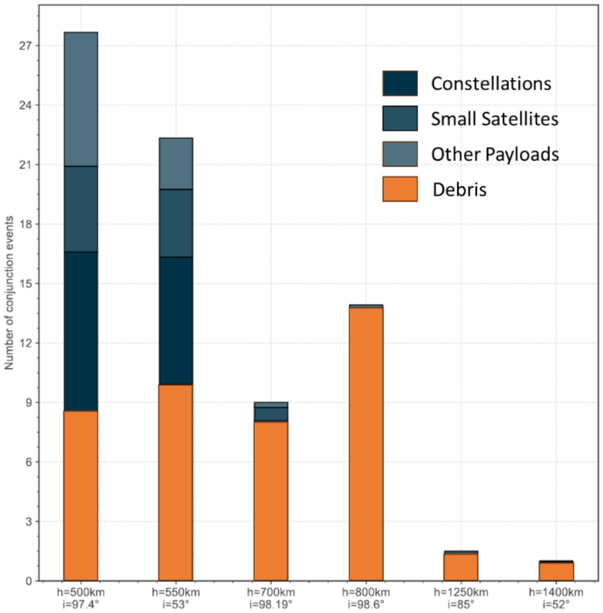

Figure 2. Conjunction events classified by secondary object for representative targets over 2022. Adapted from [7].

To the current date, no generally agreed-upon rules or guidelines for such a coordination exist, which is why there are currently two basic coordination procedures that are used in operations:

- Case-by-case: If a close approach is detected, satellite operators reach out to each other and decide case-by-case, who must act and how. Some tools exist to support these activities, but generally, every combination of satellite operators might lead to different results.
- Assumed responsibility: A special case is Starlink, which assumes general responsibility for themselves for all conjunctions that are detected for their satellites [5]. For most cases, this assumption is implicit; between NASA and Starlink though, a specific agreement exists through which Starlink takes the responsibility to undertake all required collision risk mitigation measures for close approaches involving Starlink and NASA spacecraft [7]. Other operators might have similar agreements in place but have not been released to the public.

There have been proposals describing possible parameters that could define these guidelines for who should be assigned the responsibility to act, e.g., perform a collision avoidance maneuver (CAM). From the academic world [8][19] some studies have been done considering parameters like owner's type of entity (institutional, defense, commercial, scientific), or age of the spacecraft. Frandsen [8], for example, points at the advantages of following this approach.

On the commercial side, the Space Safety Coalition [9], an industrial conglomerate, has proposed simple set of rules based on maneuverability levels: non-maneuverable, minimally maneuverable, maneuverable, automatic COLA, crewed (see Table 1). These basic rulesets have been suggested as best practices for sustainable space operations.

Table 1. Rules of the road proposed by the Space Safety coalition [9].

	Non-Maneuverable	Minimally Maneuverable	Maneuverable	Automated Cola	Crewed
Non-Maneuverable	N/A	Minimally moves	Maneuverable moves	Automated COLA moves	Crewed moves
Minimally Maneuverable		Satellite moving into orbit yields satellites in their mission orbit. Otherwise, bilateral.	Maneuverable moves	Automated COLA moves	Crewed moves

Maneuverable			Satellite moving into orbit yields satellites in their mission orbit. Otherwise, bilateral.	Automated COLA moves	Crewed moves
Automated Cola				Pre-coordinated agreement	Crewed moves
Crewed					Bi-lateral agreement

In any case, generally applicable “rules of the road” also come with one big disadvantage: there is no international body that is in the position to make these generally applicable, neither *de jure* nor *de facto*; even more so, there are no means available to go even further and enforce the adherence to such rule or even consider sanctions in the case of disregard. In other words, none of these proposed guidelines or suggested “rules of the road” have been translated to legal means, and therefore, are not enforceable in any way.

On top of that, not all cases can be covered using basic rule sets. Still, there is a high intrinsic motivation for satellite operators to reduce their on-orbit collision risk while keeping the associated transaction cost minimal. The example of Starlink additionally shows that the cost of performing avoidance measures in modern satellite operations might be lower compared to the cost associated with an uncertain process to handle risks.

But before the assignment of who maneuvers, operators need to reach out to their conjunction partner to create a channel of communications. This first step is easy to avoid when both operators are registered in a space traffic coordination (SCP) platform that eases this process, since such a platform would perform some sort of verification on the operator on the other end of the communications channel. But what happens when the operator is not available on the platform? What happens when there are multiple SCP platforms?

With this paper, the authors want to bring this issue to the attention of different stakeholders and create a discussion on how this issue could be resolved. It starts with an overview of what the authors understand as a space traffic coordination platform and some current examples are presented in Section 2. Secondly, the topic of identify verification, focused on spacecraft operators is introduced. In Section 4, a comparison of different distributed architectures for a network of space traffic coordination platforms is collected. Finally, possible next steps and final words conclude the paper.

2. SPACE TRAFFIC COORDINATION (STC) PLATFORMS

With the purpose of supporting both aforementioned cornerstones —data sharing and coordination—, special space traffic management software platforms have been introduced by either institutional or commercial actors to satellite operators. These will be referred to as Space Traffic Coordination (STC) platforms. Their main offering usually comprises:

- The owner/operator (O/O) gets an overview of upcoming conjunction events, so they can be considered in their operational planning.
- Up-to-date information of the conjunction event is compiled in a single location when published, possibly from different sources.
- Both satellite operators get a common understanding of the situation by using a single origin of truth based on an external provider, that provides both secure storage and verified dynamical models.
- Onboard operators have been pre-screened and verified by the service provider.
- Contact details of the onboarded operators have been compiled and made available for other operators.
- Optionally, a more direct and more responsive communication channel is available on the platform.
- Optionally, a support team is available for inquiries by both operations teams.

Therefore, space traffic coordination would cover the activities from the realm of information harmonizing, data sharing and collaborative planning of space activities.

One of the key aspects to consider here is that these platforms are more relevant the more operators have registered. Otherwise, operators would need to revert to traditional ways to coordinate, in the best case. In the worst case, they would not coordinate and act without considering their conjunction partner actions. Thus, one of these platforms is more attractive the more operators of one's operator vicinity can be contacted. In information technology, this is called the "network effect": a user-based platform is as valuable as its user-base [11].

However, not only satellite operators would benefit from being part of such a system. There are more interested parties apart from the entities commanding spacecraft in the orbital environment. For example, launch providers, as organizations that put spacecraft in orbit, have similar needs of coordination with other maneuvering objects in space. Regulators, governmental and other institutional organizations, like space agencies, would also be part of the platform as observers, in case they do not operate spacecraft. Finally, SSA data providers (commercial or not) could use the data shared in the STCP to better monitor the space object population.

Traditionally, government and institutional have taken the lead in providing SSA information while moving to the STM domain. Space-Track [12], currently managed by 18th Space Defense Squadron (SDS) of the USA, has been the go-to source of TLEs and more precise ephemerides due to their large sensor network, composed mainly by radar and optical sensors.

At the same time, a new effort has been put due to the transfer of responsibilities from the DoD to the DoC (through the Office of Space Commerce, OSC) to provide basic SSA services to space operators for spaceflight safety, by blending government and commercial data. This new system has received the name of *Traffic Coordination System for Space* (TraCSS) [13]. The vision for this system is not to be the unique reference, but a national hub that could interact within a coordinated system of SSA providers.

In this regard, the European Union has been pursuing their own system for SSA based on the interests of the different member states, EUSST [14]. It has its own SST sensor network and wants to achieve high autonomy with respect to the US counterpart. In their roadmap, they want to "enable higher coordination among space operators".

Both EUSST and the OSC have made an exercise recently [15] to see what the benefits would be of exchanging data and fusing it on a regular basis. The first results of the experiment conclude that both databases have proven to be more accurate and robust than the individual datasets, at least for the selected satellites involved in the campaign.

In a similar fashion, but with a different focus, the Space Data Association [16] has also been doing some exploratory work on coordination by aggregating operator ephemerides to try to find a common "truth" of the space environment. These activities have been done with 15 GEO operators that have submitted their operational ephemerides and their maneuver plans. One of the main conclusions is that the accuracy and precision varies a lot between operators, as well as the capabilities to generate them for SSA purposes, since most ephemerides were missing covariance information. This highlights the need to have a system in the middle that can fuse the different sources to get the most accurate and timely representation of the space object population.

On the commercial side, one of these platforms is OKAPI:Astrolabe, developed by OKAPI:Orbits as part of the ESA-funded CASCADE project and whose initial version was released in January 2024 [17][18]. OKAPI:Astrolabe has put its focus on satellite operators and their needs during conjunction events, allowing them to directly communicate with each other to coordinate the conjunction event and thus avoid a critical close encounter. For this purpose, various features have been implemented, such as chat functionality, actions ticketing system, timeline overviews and a collision avoidance process. Furthermore, it allows uploading both tentative and operational ephemerides, including maneuver plans, so all parties have the same understanding of the situation.

With the goal of bringing automation to space traffic coordination, OKAPI:Astrolabe includes a rule engine that can assign the action (if needed) to one of the satellite operators involved in the conjunction based on pre-established agreements. These agreements, or *coordination assignment protocols* are based on the introduced concept of *rules of the road* [19]. OKAPI:Astrolabe considers three kinds of protocols:

- Baseline protocols: generally applicable and based on industry standards and guidelines. Currently, SSC suggested ones have been included (see Table 2).

- Global protocols: user-defined and suggested action plans on the side of one operator with all their vicinity. An example of this is Starlink, that has stated that will always maneuver, should the conjunction parameters reach their actionability thresholds. They can be understood as multilateral agreements.
- Bilateral protocols: user-defined and designed to translate formal and informal agreements between two operators that have recurrent conjunctions between their fleets.

With a set of hierarchy management of these rules and subsequent evaluations, the rule engine that evaluates the different protocols available in OKAPI:Astrolabe allows automatic handling and coordination of recurrent conjunction events, which is particularly interesting for fleet operators who must assess several thousands of conjunction warnings per day. Operators can declare adherence to baseline and globally published protocols, while being able to define their own from scratch.

Table 2. Translation of the Space Safety Coalition suggested Rules of the Road [9] into OKAPI:Astrolabe coordination assignment protocols.

Trigger Conditions	Assignment
Sat1 and Sat 2 maneuverability not equal.	Satellite with highest maneuverability is assigned.
Sat1 and Sat2 maneuverability are the same, and one is not in its nominal orbit.	Satellite not in the nominal orbit is assigned.

Already several platforms are available to perform space traffic coordination, but these platforms are walled gardens. They do not allow communications outside of them, and therefore operators need to be registered in several to be able to communicate with each userbase. At the same time, each platform needs to verify that the operator being registered is who it claims to be, adding a burden on both the operator (who needs to verify in each platform) and the platform.

Moving forward, STC platforms would need to find a way to interoperate with each other, in a way that makes sense and reduces the burden of identity verification, data sharing and communication gaps. This is aligned with the vision expressed for TraCSS by the US Office of Space Commerce [20].

3. IDENTITY VERIFICATION

Before knowing which operator involved in the close approach would be the one that needs to maneuver, the operators need to establish a communications channel with each other. For this, space traffic coordination platforms might provide contact details that have already been compiled and made available from proactive satellite operators that have submitted their own information. But these contact details need to be verified in two senses: that the contact details are the appropriate ones, and that they have been submitted by the real organization. A second step would be that the entities provide reliable and actionable data, be it ephemerides, maneuver plans or results of orbit determination from sensor measurements.

Identity verification or proofing is the process of confirming that the entities involved in the transaction are who they claim to be [21]. This is crucial to ensure the integrity, security, and trustworthiness of the data being exchanged. Identity verification helps prevent fraud, unauthorized access, and data breaches by ensuring that only legitimate parties can access or transmit sensitive information.

A typical identity verification process is legal entity verification before signing a contract. This involves checking the organization's legal name, registration number, address and other identifying information against governmental or commercial business registers. It also involves personal identity verification with government issued ID or cross-referencing official records for parties that act in behave of the organization entity.

Commercial STC platform providers will perform identity verification for their customers for signing the contract. This process is slow and expensive. Organizations either need to have dedicated legal departments or pay external companies to perform legal verification for them. As part of the contract negotiation and signing, this process might not be significant compared the whole, but when coming to conjunction coordination event there is no time or resources available for it to be a viable option.

Additional challenges come when your business partners are outside of your region, language or culture zone. Verification becomes ever more complex due to language barriers, cultural differences or local regulations and politics. For example, coordination between operators from Brazil and China will have problems with contact discoverability and language communication. It might be easier between operators, for example, that have headquarters in the US and the UK.

In a world where multiple STC platforms coexist, part of the operators might have been already verified by a STC provider, and they will not go via same the complex process with a different STC platform where the conjunction partner operator is registered.

Going forward, faster and cheaper verification processes, eliminating redundant verification, are needed. Though verification should be time limited, forced to be renewed like contracts.

One option would be to re-use trust established by STC platform and its customer, by creating trusts between STC platforms. This allows operators to register with one STC platform to coordinate cases with any operators registered within STC network. It lifts off the burden of operators having to be verified with each platform. This forces STC platforms to create automated interfaces that verify and trust data coming for the STC network for coordination cases. A diagram displaying this concept is showing in Figure 3.

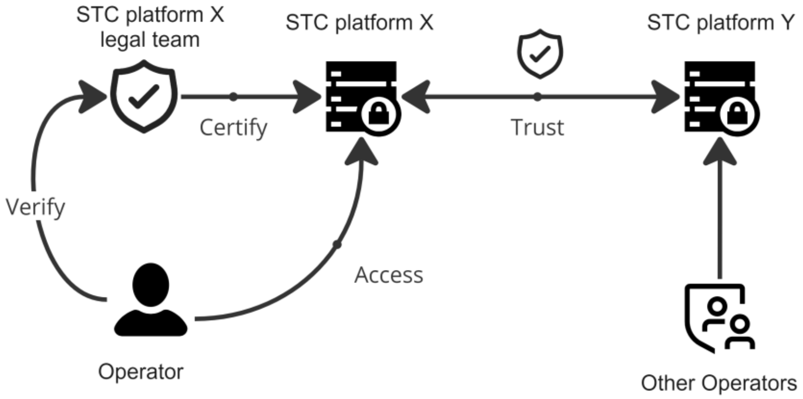

Figure 3. Diagram portraying how trust between different STC platforms could be established.

Pros:

- Reusing existing verification procedures established by STC platforms for contract signing
- Operators needs to go through identity verification process only once
- Any registered operators will be able immediately to coordinate cases with any registered operator in the network

Cons:

- Operators must have a contract with an STC platform
- STC platforms would need to create secure communication channels for data exchange
- STC platforms would need to verify each other
- Still may create siloes STC networks in different world regions / political areas

Another option is to de-couple identity verification from STC platforms. An external identity provider (IdP) or providers could perform verification of the operator and then the STC platforms would trust any identities provided by the IdP(s), as shown in Figure 4. This system is what is being followed when safely browsing the internet. Trust is created between user web browsers and web servers to create secure communications and verify the parties involved. The verification is performed by third parties called Certificate Authorities (CA) that verify and approve the certificates for web servers. Web browsers keep the list of trusted CAs and trust all certificates created by them.

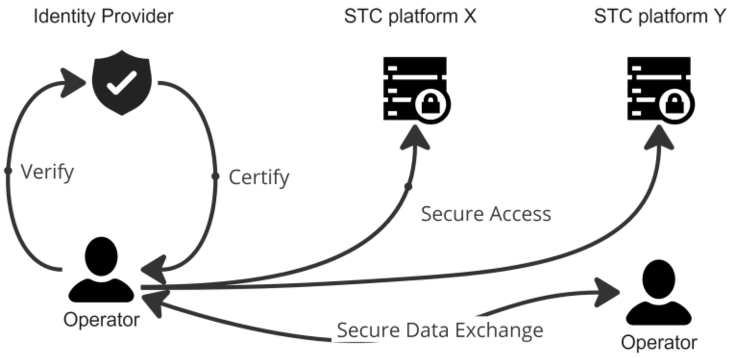

Figure 4. Diagram showing externalization of operator identity verification in a STC network.

Pros:

- Having trusted IdP would allow operators to login and share data with any STC platforms that trusts this IdP
- This even allows directly to exchange data between operators in a secure way with or without STC platforms in the middle
- This model is proven and already implemented

Cons:

- Additional organizations need to exist, or an existing organization needs to take these responsibilities
- Additional costs will need to be assumed to maintain the Identity Provider

Both internal and external verification need someone performing a process to assess that the information provided is coming from the right operator. At the same time, a process to verify that the data the candidate to enter the network would upload would need to be assessed, to prevent polluted data. Adherence to common standards, practices and quality levels could be added to this process. In the end, IdPs could act as gatekeepers to the STC network.

4. GOVERNANCE MODELS FOR A DISTRIBUTED NETWORK OF STC PLATFORMS

In a world where a diverse set of STC platforms coexist, with different kinds of owners and purposes, a network of interoperable STC platforms might surge. In this section, we propose different governance models for a distributed network of STC platforms.

A distributed network of STC platforms might contain different actors in it, each of them with different interests and with their own platform that might have a different set of features, the main feature being to be able to put in contact spacecraft operators during conjunction events, as a minimum.

As mentioned before, other platforms might include ways to automatize the assignment of cases, based on rules of the road, like OKAPI:Astrolabe, while others might focus on compiling and generating precise ephemerides to find these close approaches, like Space-Track or EUSST. Others might focus on keeping track of spacecraft status, ownership and contact details for everyone else to use.

Each SCP platform might be owned by different entities: commercial companies, non-profit organizations, civil institutions, a large constellation operator, space agencies, etc. At the same time, each platform might be based in different countries or economic areas, and therefore might need to comply with different regulations. Therefore, each SCP platform might opt for different approaches in how it is internally managed, what is their external offering and which spacecraft operators they target, which will also determine the underlying technical solution and their value proposition.

As introduced in the previous section, there are two main approaches for identity verification (IdV), which is the first step when joining a STC platform: it can either be delegated into an external Certification Authority (or group of them), or each STC platform can perform their own IdV. There are approaches that lie in between these two options.

A Centralized Identity Provider is an idealistic vision of one organization responsible for validation, registration, and approval of spacecraft operators while connecting to a network. Such an approach is easy to implement with established technologies for Identity and Access Management (like Microsoft Entra ID, Okta Auth0). Unfortunately, for cross-border industries, it is very hard to agree for everyone to have one central organization recognized by every party. If challenged by at least one big partner, then it breaks apart into a silo approach. Moreover, centralized organizations tend to be slow with big bureaucratic overhead, which makes it unusable during conjunction coordination event with no time to spare. Either certification is done ahead of time, or a “leap of faith” is done going over this official process. It is difficult to imagine an entity non-dependent of the United Nations performing this role.

On the other end, there is a completely decentralized model where each operator verifies the identity of other operators on their own. For example, SpaceX has started offering an API where neighboring operators can submit their own ephemerides for conjunction screening against the Starlink constellation [22]. These operators need to generate their own certificate that verifies their identity to SpaceX and would only be valid for this system. While the idea is to be more transparent and open with the space operators community, if many operators follow this path, it would become difficult to integrate each offering into each flight dynamics operational center.

A midway solution would be to have several entities providing this identity verification. These entities could be external authorities (e.g., International Telecommunications Union), the state where the spacecraft is registered (Germany, Nigeria, India, etc.), the local space agency (ESA, NASA, ROSCOSMOS), a STC platform administrator, or another member of network. This concept is already implemented in public key infrastructure [23] by certification authorities (CA) in the Internet. CA is an entity that stores, signs, and issues digital certificates. Popular web browsers like Google Chrome, Mozilla Firefox or Microsoft Edge come with a list of supported CA that they trust.

When these are external entities, we fall under the case of External Identity Providers. This concept is easy to implement with established technologies for Identity and Access Management. Each STC platform can define its own list of supported Identity Providers. IdP organizations that are closer to local markets can efficiently onboard local companies to the market. Fragmentation of trust is still possible if some organizations do not recognize all IdPs as valid.

The last case is known as "朋友的朋友" or "Freundesfreund", which stands for "friends of a friend". This is a decentralized identity provider concept where a distributed network of trusted spacecraft operators or data providers self-approve new operators or data providers based on previously agreed set of rules. Any entity in the network can onboard a new entity to the network (see Figure 5). The new entity will be automatically recognized as trusted by all members of the network. In this concept, or governance model, every member has the same weight or power of decision in onboarding new members into the network.

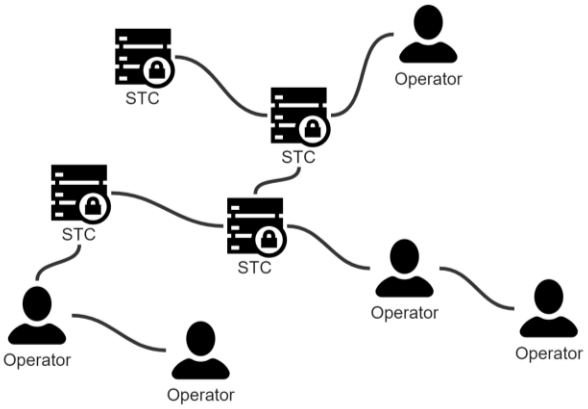

Figure 5. STC network showing the concept of "Friend of a friend".

If this weight is not equal, and thus not every member of the network can perform the onboarding, but only some can do it, the concept of a champion-based governance model arises. The entities that can onboard, or that have a higher weight in the network, are called *champions*. Champion organizations could be selected based on different criteria: membership age, number of satellites, data sharing transparency, ownership (civil vs commercial), etc.

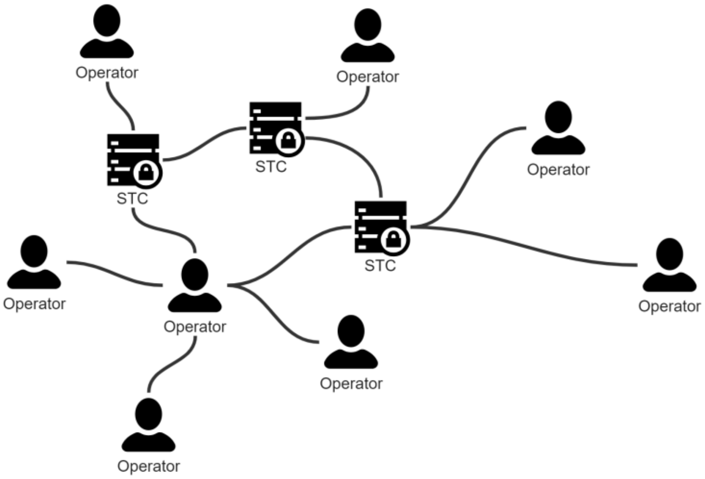

Figure 6. STC network diagram based on champion-based governance model.

An operator willing to be part the STC network ("candidate") might need the approval of these champions. There are different strategies to offload the task of identity verification to the network. There is the option that only a single champion approval is need get access to network. This is the concept of "friend of a friend" if any operator can act as a champion.

But there are different possibilities here one we request that a quota is met to be part of the network. This is consensus-based approval. One option is that a certain number of approvals from different champions is needed. If each operator (or champion if only some entities can do it) gets a reputation level, then the access is got once an operator gets the support of entities adding up to a certain reputation threshold. This reputation could be based on data sharing practices, antiquity, or constellation size, for example.

A final topic arises when one considers that access to the network would probably need to be renewed. Certain maintenance and reviewing practices would need to be kept in place, to ensure access is still given to the appropriate entities. In the end, moderation is one of the areas where more work needs to be put to ensure a community keeps being useful to all its members.

Finally, this is not a technological problem. There are existing technologies that could be explored for almost every described scenario. Blockchain has been proposed as part of SpaceDAO [24][25] and is also the backbone of cryptocurrencies like Ethereum [26], with its smart contract functionality that allows to run code within the network. In the domain of social media and social networks, the Word Wide Web Consortium (W3C) hosts a standard called ActivityPub [27], that serves as a protocol to exchange social network actions between agents in a decentralized manner, and that has been implemented by, for example, Mastodon (a microblogging platform) [28], Peertube (a social video hosting provider) [29] or Pixelfed (a social image sharing platform) [30]. All these interconnected platforms, each of them defined in their own way, can interact with each other and constitute the "Fediverse" [31][32].

5. NEXT STEPS & FINAL WORDS

In this paper, different propositions of how a decentralized network of space traffic coordination platforms might look like have been explored. The purpose of the paper is to bring attention of how a future in which a diverse set of STC platforms might look like, since there is already a multitude set of these. Even if the number is currently small, interoperation will most probably be required, and it is currently the vision of some of the bigger STC proponents of today, like the US Office of Space Commerce [20].

After an overview of what the authors understand of Space Traffic Coordination, and what the main requirements of a platform dedicated to it might be, the problem of identity verification of spacecraft operators for space traffic coordination is introduced. The idea is then developed into governance models of a space traffic coordination network, since the entities verifying the identity would probably also control the access to the network. Depending on how centralized or decentralized this verification is done, there are different possible models and concepts to follow, and that have also been put in place in other domains, like the Internet. Some ideas on how this could look like have been shown, bringing some benefits and disadvantages of each governance model.

Distributed networks are beneficial when several entities want to remain in control of the information that pertains to them. It also allows for new entities to offer a different set of options without having to rely on the infrastructure set up by other entities. A different "client" to the network could be developed, allowing commercial entities like STM providers to compete with established, bringing innovation, providing new analysis methods, and pushing the boundaries of automation, while preserving transparent and open data sharing practices, which are the backbones required for space traffic coordination.

Next steps include further developing the high-level concept here presented, as well as starting to investigate the technological solutions already mentioned that could enable these concepts.

Finally, with this paper, the authors want to start a conversion amongst the community involved in space traffic management and coordination: satellite operators, SSA providers, SST sensor operators, researchers and analysts, space agencies and governmental bodies, from different geographical backgrounds and sizes, so a common vision can be achieved. Therefore, the authors would appreciate any feedback or ideas from the community to steer these efforts. At OKAPI:Orbits, the plan is to develop a technical prototype based on OKAPI:Astrolabe to demonstrate this vision in partnership with like-minded entities.

6. REFERENCES

[1] B. Bastida Virgili, J.C. Dolado, H.G. Lewis, J. Radtke, H. Krag, B. Revelin, C. Cazaux, C. Colombo, R. Crowther, M. Metz, Risk to space sustainability from large constellations of satellites, Acta Astronautica, Volume 126, 2016, Pages 154-162, ISSN 0094-5765, https://doi.org/10.1016/j.actaastro.2016.03.034.

[2] D'Ambrosio, Andrea & Servadio, Simone & Siew, Peng Mun & Jang, Daniel & Lifson, Miles & Linares, Richard. Analysis of the LEO orbital capacity via probabilistic evolutionary model, AAS/AIAA Astrodynamics Specialist Conference, California, 2022.

[3] French Space Operations Act n°2008-518 of 3rd June 2008 and Decree on Technical Regulation issued pursuant to Act n°2008-518 of 3rd June 2008, 31.

[4] Space systems — Space debris mitigation requirements, ISO 24113:2019, 2019.

[5] Data retrieved from Space-Track Tempo on 27.01.2023. www.space-track.org

[6] SpaceX Orbital Debris Meeting Ex Parte (8-10-21).pdf, last accessed 27.01.2023.

[7] ESA Space Debris Office, ESA's Annual Space Environment Report, GEN-DB-LOG-00288-OPS-SD, 12. June 2023.

[8] Hjalte Osborn Frandsen, Looking for the Rules-of-the-Road of Outer Space: A search for basic traffic rules in treaties, guidelines and standards, Journal of Space Safety Engineering, Volume 9, Issue 2, 2022, Pages 231-238, ISSN 2468-8967, https://doi.org/10.1016/j.jsse.2022.02.002.

[9] Best Practices for the Sustainability of Space Operations, Space Safety Coalition, Version 2.34, , https://spacesafety.org/best-practices/, 2023.

[10] Nonreimbursable Space Act Agreement Between The National Aeronautics and Space Administration And Space Exploration Technologies Corp For Flight Safety Coordination With NASA Assets. January 2021. Accessible via: nasa-spacex_starlink_agreement_final.pdf, last accessed 27.01.2023.

[11] Shapiro, Carl, and Hal R. Varian. Information Rules: A Strategic Guide to the Network Economy. Harvard Business School Press, 1999.

[12] Space-Track, https://www.space-track.org/, accesed 22 August 2024.

[13] Office of Space Commerce, Traffic Coordination System for Space (TraCSS), https://www.space.commerce.gov/traffic-coordination-system-for-space-tracss/, accesed 22 August 2024.

[14] EUSPA, EUSST, https://www.eusst.eu/, accesed 22 August 2024.
[15] Hoots, Felix, et al. ‘US-EUSST Data Exchange for Improved Orbital Safety’. AMOS Conference (2022).
[16] Oltrogge, Daniel, et al. ‘Deep Operator and SSA Collaboration for Space Sustainability’. Journal of Space Safety Engineering, vol. 11, no. 2, June 2024, pp. 342–61. ScienceDirect, https://doi.org/10.1016/j.jsse.2024.03.007.
[17] Esfandiar Farahashi et al, Towars Automated, Clear and Efficient Rule-based Conjunction Coordination for Constellations, IAC-23-B6,5,9,x78082, 74th International Astronautical Congress, Baku, Azerbaijan, 2023.
[18] Adrian Diez et al. Hands-on Demonstration of a Space Traffic Coordination Platform. 10th Annual Space Traffic Management Conference, Austin, Texas, USA, 2024
[19] Simon Burgis, Enabling Efficient Satellite Mission Design with Rule-Based Collision Avoidance, IAC-23,A6,7,3,x78296, 74th International Astronautical Congress, Baku, Azerbaijan, 2023.
[20] US Office of Space Commerce. Global Space Situational Awareness Coordination. April, 2024. https://www.space.commerce.gov/global-ssa-coordination-vision/
[21] Paul A. Grassi Michael, E. Garcia James, L. Fenton [SP 800-63-3] Digital Identity Guidelines https://doi.org/10.6028/NIST.SP.800-63-3
[22] SpaceX. Starlink Space Traffic Coordination APIs Documentation. https://docs.space-safety.starlink.com/docs/, accesed August 2024.
[23] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile https://datatracker.ietf.org/doc/html/rfc5280
[24] Red Boumghar, Annalisa Ricardi, Cesar Guzman and Shahzad Ameen. Orbit Decentralized Autonomous Organization Using Blockchain-Based Consensus Mechanisms. 10th Annual Space Traffic Management Conference, Austin, Texas, USA, 2024
[25] Red Boumghar et al. Decentralized and Neutral Consensus Mechanisms in Space Conjunctions Assessment and Mitigation: Space DAO STM. 10th Annual Space Traffic Management Conference, Austin, Texas, USA, 2024
[26] Ethereum.org. https://ethereum.org/en/
[27] W3C. ActivityPub: W3C Recommendation 23 January 2018. https://www.w3.org/TR/activitypub/. Accessed August 2024.
[28] Mastodon - Decentralized social media (joinmastodon.org)
[29] What is PeerTube? | JoinPeerTube. https://joinpeertube.org/
[30] Pixelfed - Decentralized social media. https://pixelfed.org/
[31] La Cava, L., Greco, S. & Tagarelli, A. Understanding the growth of the Fediverse through the lens of Mastodon. *Appl Netw Sci* **6**, 64 (2021). https://doi.org/10.1007/s41109-021-00392-5
[32] Mahadeva, Nikhil, Everyone Everywhere All at Once: The Fediverse Problem (January 15, 2024). http://dx.doi.org/10.2139/ssrn.4716427