Establishing a Chain of Digital Forensics for Space Object Behavior Using Distributed Ledger Technology

Waqar Zaidi, Tom Kelecy, Weston Faber
L3Harris
Email: Waqar.Zaidi@L3Harris.com

Moriba Jah
University of Texas at Austin
Email: Moriba@utexas.edu

ABSTRACT

Digital forensics is defined as the process of preservation, identification, extraction, and documentation of digitally represented evidence which can be used to support or refute a claim. For a debris generating or hostile kinetic event, the perceived motion of a space object becomes increasingly uncorrelated to the breakup based on the non-conservative forces acting on it, beginning at the instant immediately following the breakup. Therefore, to infer or contest a causal relationship between a space object dynamic behavior after an event and the event itself, we must independently account for the uncertainties and effects introduced by the non-conservative forces. In this paper we examine the digital and space object forensics required to establish the body of evidence that is not only required to characterize the space object's behavior but also record the evidence digitally, needed to determine data provenance, attribution, and quality (i.e., completeness, consistency, timeliness, validity, and uniqueness). Specifically, digital forensics are addressed by organizing space object data requests onto an immutable distributed ledger such that, once consensus of the provisioned data (i.e. agreement between independent data validators) is established, each step related to its request, provision, and qualification is recorded on a transaction block. Protocols for using distributed ledger technology for space object forensics are introduced and examples of independent tracking of a space object required to obtain these forensics are explored. The value of this technology to Space Domain Awareness will be to provide more accurate quantification of event knowledge and, hence, support information trust and provide a means for prioritization of tasking to reduce event ambiguity.

1. INTRODUCTION

Space Domain Awareness (SDA) is the exploitation of intelligence to identify, locate, and track potential threats to on-orbit space systems and to manage the safety of activities in all orbit regimes [1][2]. The global SDA theater is inevitably evolving into a cadre of independent sensor networks feeding their corresponding national Space C2 and SDA operations centers. The United States and its Allies will be pushed to work together to completely characterize the space domain against known adversaries. However, while an abundance of data sharing agreements has been signed between nations, a solution for the bi-directional exchange of data does not exist [3]. On top of this, strict policy, roadblocks, and export control restrictions make it extremely difficult to share underlying observational data between any two nations. This brings us to a crossroad—is the goal of allied SDA support (1) operations agreement at the mission level (e.g., help confirm space object behavior based on the exploitation of independent and multi-sensor multi-phenomenology sensor data) or (2) sensor agreement between multiple international SDA sensors [4]. In either case, data integrity and trustworthiness must be addressed not to mention a dataset's attribution, immutability, and forensics. Additionally, one must consider the statistical orbit determination implications of simply not having enough data to completely characterize space object behavior.

Consequently, assuming two independent allied sensor networks exist that share operational knowledge, this paper offers a path for data users of those two networks to come to consensus that first, both sensor networks are properly calibrated, and second both agree a space object event is occurring (based on their own independent data exploitation). Consequently, we consider the application of digital "evidence" to infer causal space object dynamic behavior based on independently trended post-event observations. Here, space object dynamic behavior is defined as a combination of the motion induced by conservative (i.e., Newtonian, Keplerian) and non-conservative (i.e., drag, solar pressure, maneuver) forces. Perceived space object motion from an independent observer is a combination of the following:

1) Actual motion
2) Our models of the physics of actual motion
3) The measurements used to "observe" the motion
4) Our models of the sensors used to "observe" the motion
5) The inference methods we use to interpret (3) in the context of (2) and (4)

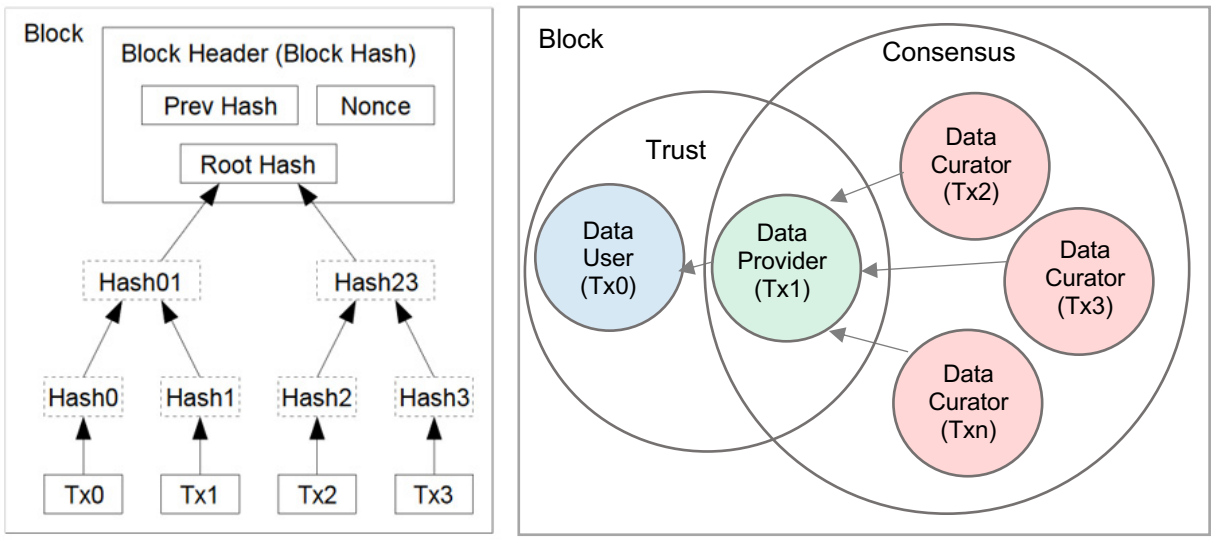
For a debris generating or hostile kinetic event, the perceived motion of a space object becomes increasingly uncorrelated to the breakup based on the non-conservative forces acting on it, beginning at the instant immediately following the breakup. Therefore, to infer or contest a causal relationship between a space object dynamic behavior after an event and the event itself, we must independently account for the uncertainties and effects introduced by the non-conservative forces. To contest or attribute a hostile breakup event, the digital and space object forensics must be preserved to establish the body of evidence that is not only required to characterize the space object's behavior but also record the evidence digitally, needed to determine data provenance, attribution, and quality (i.e., completeness, consistency, timeliness, validity, and uniqueness). We will show how we can use distributed ledger technology to obtain the chain of evidence or forensics indicating a 1-to-1 causal relationship between evidence and space object behavior prior to and after a kinetic event.

Consequently, the contents of this paper are organized as follows: first, we provide in depth details regarding distributed ledger technology and how its core features can be leveraged to establish trust into SDA applications. Next, we offer methods for and describe the importance of data curation in a proposed distributed ledger-based framework. Finally, we provide examples of using the framework and how it helps to digitally preserve the records and establish transparency and trust for a simulated breakup event observed by two independent electro-optical sensor networks.

2. DATA TRUST ESTABLISHMENT AND DISTRIBUTED LEDGER TECHNOLOGY

Distributed ledger technology is a database that exists across several locations or among multiple participants [5]. For example, Blockchain is a type of distributed ledger technology filled with entries that must be confirmed and encrypted. In fact, Blockchain uses a cryptographic signature called a hash that allows for the secure transfer of traceable and immutable bits of information between different nodes of a decentralized system. In this setup, each node processes and verifies every item, thereby generating a record of each item and creating a consensus on its veracity. There are many benefits to distributed ledger technology compared to the traditional form of centralized record keeping and verification architecture. Most importantly, since it removes the need for a central verification authority, distributed ledger technology provides increased efficiency and speed in transferring information between nodes. Distributed ledger technology is also more secure and resilient against adversarial intent because every node in the network holds complete records of the transactions removing reliance of a single node or database that could be vulnerable to cyberattacks or spoofing.

Traditionally, a block on a Blockchain contains information regarding a transaction such as the details of the purchase of coins, the transaction's time, dollar amount, and participants. An owner who creates coins can prepare new transactions that send those coins to a buyer by simply embedding the new owner's public key in the transaction and then signing the transaction with his or her private key. To make the entire transaction immutable, Blockchain uses a cryptographic term called a "Merkle Tree" which binds the elements together by creating an equation that serves as a special unforgettable signature for that specific group of elements [6]. Fig. 1 shows an example of Merkle tree where 'data blocks' contain immutable details of a transaction (e.g., data records, images, digital signatures etc.). This way of associating a group of elements makes it extremely difficult for one to forge or alter their identity, qualities, and association. More specifically, the tree works by using a mathematical algorithm known as a hashing function for the qualities of the items (such as their file name, file size, or any other special or unique properties). This enables the tree to be tamper-proof—a change in the structure of data mapped to the "root" or topmost hash changes the root hash thus signaling an unverified modification in the database. Consequently, once the authenticity of the transaction is verified (through consensus), it is given a hash that uniquely identifies it as well as links it to a previously validated block. Typically, a validation node validates a transaction, and an endorsing node simulates a smart contract (i.e., a pre-existing set of conditions) to endorse the transaction.



Transactions Hashed in a Merkle Tree

Consensus and Trust establishment on a Block

Fig. 1. Left: An example of a cryptographically hashed 'Merkle Tree' residing inside a block that contains immutable details of a transaction (e.g., digital records or files). Right: A layered consensus protocol where consensus in data curation is utilized to established trust in SDA data.

While Blockchain clearly preserves the digital forensics of a transaction, it neglects to consider the integrity of the transactional datasets themselves. "Data curation" is defined as addressing a dataset's variety, annotation, quality (or veracity), interoperability, and validation [7]. Thus, if one where to consider this technology for SDA applications, a smart contract and consensus protocols (for the curation of data obtained from an independent sensor network and agreement between two independent sensor networks) must be developed. Accordingly, returning to Fig. 1 we see a visual representation of the proposed Blockchain-based framework that includes three main types of participants on the decentralized SDA framework—data users, data providers, and data curators. SDA data requests are organized onto an immutable ledger such that, once consensus (i.e. agreement between independent data curators for the validity of the dataset provisioned in response to a request) is established, each step related to a request—its corresponding data provision(s), and their corresponding data curation(s)—are recorded on a transaction block. Then an endorsement of this transaction block would occur by a regulatory entity to determine not only if data providers and data curators have the authority to participate but are also using approved algorithms to perform the provision and curation of data.

It goes without saying data users, data providers, and data curators are expected, but not required, to be decentralized participants if independence of data provision and data curation is maintained. Thus, we have redefined traditional Blockchain consensus in the context of SDA to represent an agreement between independent data curators that a requested dataset is valid. Furthermore, we have defined the scope of an SDA data request smart contract to be the following:

<u>Scope of an SDA Data Request Smart Contract</u>

1. Data User Initiates Request for Data and Curation(s)
2. Acceptance of Data Request
3. Initiate Request for Data Curation
4. Acceptance(s) of Data Curation Request
5. Provision of Data to Curator(s) with hash
6. Completion of Data Curation
7. Completion of Data Provision to Data User

If the smart contract terms and consensus protocols are met, the SDA block at hand is chained to a previously vetted block ultimately creating a cyber secure distributed ledger with verified SDA intelligence. In fact, in the proposed

construct, digital forensics on the ledger will provide a chain of evidence that an active space object is exhibiting a certain dynamic behavior. This chain of evidence can immutably capture the entire Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) process from observation to space object behavior determination. For example, Fig. 2 shows a JSON string of a radar dataset collected on a geostationary spacecraft that includes a unique hash for that dataset making it immutable. This JSON also contains a digital signature, signing key address, and subresource integrity (SRI) of the data provider [8].


```
{
        "id": "f6e2d12c-93f5-48ac-9665-7e3e6aec867b",
        "classificationMarking": "U//PR-THOTH-OBS",
        "sri": "mxHYzCPUpLDu0rhUa/5mEHhm+HC16vnQhVziDyoicWU=",
        "signing key address": "1o1oiXfMHPXMY6kxeZfXSHsYKWp9DqtU7",
        "signature": "H5U2wXReWx40FuRBEiENB6KcUqurn5C+o4+5jrBQfOtwAAwY=",
        "obTime": "2020-11-19T03:26:38.527000Z",
        "idOnOrbit": "45465",
        "idSensor": "464",
        "satNo": 45465,
        "transactionId": "11119999",
        "azimuth": 204.739,
        "elevation": 41.897,
        "range": 37638.40245,
        "source": "Thothx",
        "dataMode": "REAL",
        "type": "RADAR"
}
```


Fig. 2. Unique Hashing Mechanism used at SDA Dataset Collection.

Additionally, this dataset is placed in an immutable database such that the dataset itself cannot be changed and its provisioning contains a unique hash as well. Accordingly, we are carefully establishing a forensics trail between the tasking of a sensor, the collection of the data from that sensor, all the way to the provisioning or dissemination of that dataset. Once that dataset is provisioned, it is now ready to be independently curated by multiple decentralized nodes such that each one of those steps contains a digital signature of the data curator and a unique hash for curation algorithms used to curate the requested data. Fig. 3 provides a hashed dataset provision.


```
{
    "modifedby": " Thothx ",
    "current State": "3",
    "TimeStamp": "11/19/2020, 9:22:18 AM CST",
    "dps": [
            {
                "qualificationRecord": [],
                "qualificationResult": "---",
                "currentState": 3,
                "dataProviderId": " Thothx ",
                "hash": "40cb367b16f492f8acfb81f95cf79cbd31bae6b",
                "url": "https://unifieddatalibrary.com/udl/radarobservation?
                obTime=%3E2020-11-19T00:00:00.000000Z&classification
                Marking=U//PR-THOTH-OBS&satNo=45465"
            }
        ]
}
```


Fig. 3. Unique Hashing Mechanism Used at SDA Dataset Provisioning.

Accordingly, to capture trust in a space object event, two types of "consensus protocols" (from here on forth known as Consensus Protocols #1 and #2) are designed for the proposed Blockchain framework—the first is to ensure an independent sensor network is adhering to proper data calibration standards and the second is to determine if two

independent sensor networks (each adhering to the first consensus protocol) are in agreement that a space object event is occurring.

3. DATA QUALITY METRICS AND CONSENSUS PROTOCOLS FOR A SPACE DOMAIN AWARENESS DISTRIBUTED LEDGER FRAMEWORK

Consensus Protocol #1 must ensure an independent sensor network is properly calibrated—this curation (or proof of calibration) must be captured on the Blockchain in such a way that it enables one to trust the exploitation of the data collected by that network. Consequently, errors in SDA sensor data can be random, biased and/or systematic [9], in other words both aleatory and epistemic, respectively. They can also be associated with the observation data, the modeling, the filtering, or the reference satellite ephemerides for calibration. The sensor hardware and all software in the astrometric processing chain can contribute to errors in each category. A representative categorization of these errors is as follows:

- Data
  - Astrometric errors
    - Random (Aleatory)
    - Systematic (Epistemic)
  - Reference frame of derived data
  - Timing bias
  - Aberration correction
  - Media delay corrections
  - Outliers
- Models
  - Dynamic mis-modeling errors
  - Observation modeling errors
- OD Filter (incorrect assumptions)
  - Initial state errors
  - Uncompensated biases
  - Incorrect noise assumed
  - Unmodeled dynamics (e.g. maneuvers)
  - Outliers not filtered
  - Mis-tags of data from miscorrelation (i.e., Type I and II errors)
- Calibration
  - Reference satellite error
  - Interpolation from tabular reference source (e.g. WAAS)
  - Initial state errors from osculating orbit source (e.g. TDRS)
  - Incorrect reference frame

Accordingly, satellites with well-known orbits and accessible ephemeris data are used as calibration ("reference") satellites, or "CalSats" for short. These orbital fiducials include (but may not be limited to) GNSS satellites such as GPS and Beidou, TDRS, and the Wide-Area Augmentation System (WAAS) constellations. Observations are correlated with specific CalSats for which their ephemeris data are collected, mapped into the observation reference frame, and interpolated to the observation timestamps. The calibration process involves computing the residuals between these reference data and the observation values reported. These residuals are then used to assess the quality and noise of the data, to validate that the correct reference frames and timescales have been used, and to estimate any additional biases or systematic errors (i.e., this seeks to eliminate epistemic uncertainties). The optical calibration process identifies a "reference" satellite for which a highly accurate and precise ephemeris is available and tasks it to be tracked. The reference satellite orbit is reduced to derive a reference measurement set at the observation times which are compared to the actual measurements (e.g. topocentric right ascension and declination). Examples of "good" and "biased" calibration metric residuals are shown in Fig. 4.

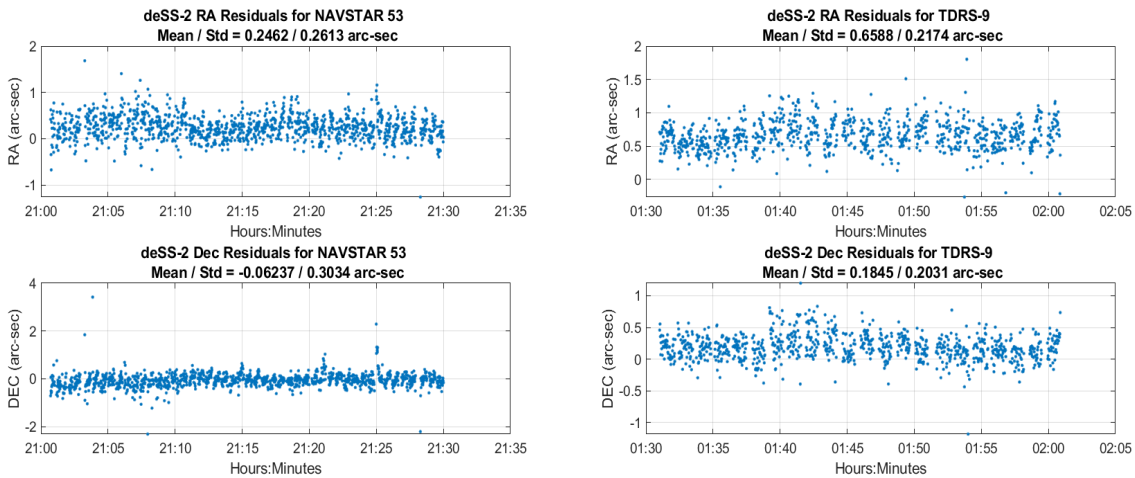


Fig. 4. "Good" (Left) and "Bad" (Right) calibration examples

A possible data curation process for Consensus Protocol #1, to be exercised in near real time (NRT), may involve an estimation implementation that enables certain parameters to be estimated and others only to be considered during the estimation process, e.g. observation biases, until the appropriate reference satellite data are available. To account for, or "consider", the uncertainty associated with non-estimated parameters, the unscented Schmidt-Kalman filter (USKF) is utilized [10]. It incorporates the "consider covariance analysis" concept whereby known errors in model and state parameters can be "considered" to make the estimation uncertainty more representative (realistic). The USKF algorithm used to establish consensus that an independent sensor network is well calibrated is given in Fig. 5.

USKF

Predictive

$$\mathrm{S}_{zz,k-1} = Cholesky(\mathbf{P}_{\boldsymbol{zz},k-1})$$
$$\boldsymbol{Z}_{i,k-1} = \hat{\boldsymbol{z}}_{k-1} \pm \sqrt{n_x + n_c}\boldsymbol{s}_{i,k-1}$$
$$\text{where } \mathrm{S}_{zz} = [\boldsymbol{s}_1, ..., \boldsymbol{s}_{n_x+n_c}]$$
$$w = \frac{1}{2(n_x+n_c)}$$
$$\boldsymbol{Z}_{i,k} \Leftarrow \hat{\boldsymbol{Z}}_i = \boldsymbol{f}(\boldsymbol{Z}_{i,k-1}, t)$$
$$\hat{\boldsymbol{z}}_k = \sum_{i=1}^{2(n_x+n_c)} w_i \boldsymbol{Z}_{i,k}$$
$$\mathbf{P}_{\boldsymbol{zz},k} = \sum_{i=1}^{2(n_x+n_c)} w_i (\boldsymbol{Z}_{i,k} - \hat{\boldsymbol{z}}_k)(\boldsymbol{Z}_{i,k} - \hat{\boldsymbol{z}}_k)^T$$

Corrective

$$\boldsymbol{Y}_i = \boldsymbol{h}(\boldsymbol{Z}_i, t)$$
$$\hat{\boldsymbol{y}} = \sum_{i=1}^{2(n_x+n_c)} w_i \boldsymbol{Y}_i$$
$$\mathbf{P}_{\boldsymbol{yy}} = \sum_{i=1}^{2(n_x+n_c)} w_i (\boldsymbol{Y}_i - \hat{\boldsymbol{y}})(\boldsymbol{Y}_i - \hat{\boldsymbol{y}})^T + \boldsymbol{R}$$
$$\mathbf{P}_{\boldsymbol{zy}} = \sum_{i=1}^{2(n_x+n_c)} w_i (\boldsymbol{Z}_i - \hat{\boldsymbol{z}})(\boldsymbol{Y}_i - \hat{\boldsymbol{y}})^T$$
$$\begin{bmatrix} \mathbf{P}_{\boldsymbol{xy}} \\ \mathbf{P}_{\boldsymbol{cy}} \end{bmatrix} = \mathbf{P}_{\boldsymbol{zy}}$$
$$\mathrm{K}_{\boldsymbol{z}} = \mathbf{P}_{\boldsymbol{zy}}\mathbf{P}_{\boldsymbol{yy}}^{-1} = \begin{bmatrix} \mathrm{K}_{\boldsymbol{x}} \\ \mathrm{K}_{\boldsymbol{c}} \end{bmatrix} \begin{pmatrix} NOTE: \\ \mathrm{K}_{\boldsymbol{c}} \neq 0!! \end{pmatrix}$$
$$\text{Force correction to consider terms to be 0:}$$
$$\hat{\boldsymbol{z}}^+ = \hat{\boldsymbol{z}}^- + \begin{bmatrix} \mathrm{K}_{\boldsymbol{x}} \\ \mathbf{0} \end{bmatrix} (\boldsymbol{y} - \hat{\boldsymbol{y}})$$
$$\mathbf{P}_{\boldsymbol{zz}}^+ = \begin{bmatrix} \mathbf{P}_{\boldsymbol{xx}}^- & \mathbf{P}_{\boldsymbol{xc}}^- \\ \mathbf{P}_{\boldsymbol{cx}}^- & \mathbf{P}_{\boldsymbol{cc}}^- \end{bmatrix} - \begin{bmatrix} \mathrm{K}_{\boldsymbol{x}}\mathbf{P}_{\boldsymbol{yy}}\mathrm{K}_{\boldsymbol{x}}^T & \mathrm{K}_{\boldsymbol{x}}\mathbf{P}_{\boldsymbol{yy}}\mathrm{K}_{\boldsymbol{c}}^T \\ \mathrm{K}_{\boldsymbol{c}}\mathbf{P}_{\boldsymbol{yy}}\mathrm{K}_{\boldsymbol{x}}^T & \mathbf{0} \end{bmatrix}$$

Fig. 5. USKF Formulation

Though, in general, all forms of error (e.g., biases, systematic and periodic errors) are of interest, the subsequent use-cases model a sensor timing bias to illustrate the near real-time calibration using the USKF. Hence, to either estimate or consider the timing bias, it must be included in the USKF state along with any other estimated parameters (e.g. *position, velocity, and solar radiation pressure*). The timing bias finds its way into the USKF via the EO reference measurements derived from the reference satellite. The reference satellite is tracked by the EO sensor and the EO sensor inertial state (derived from the site coordinates) at the measurement time is corrected for the timing bias. At the time of each measurement update the state-vector sigma points are used to compute an equivalent measurement sigma point and these are adjusted for the current best estimate of the timing bias as follows

$$t_{corrected} = t_{observation} - t_{bias} \tag{3}$$

$$\vec{R}_{J2000} = \left[T_{ITRF \to J2000}(t_{corrected})\right] \vec{R}_{ITRF} \tag{4}$$

$$\vec{\rho} = \vec{r}_{J2000} - \vec{R}_{J2000} - \vec{v}_{J2000} \cdot (t_{bias} + \delta t_{LTC}) \tag{5}$$

$$\rho = \|\vec{\rho}\| = \sqrt{\rho_x^2 + \rho_y^2 + \rho_z^2} \tag{6}$$

$$\alpha = \tan^{-1}\left(\frac{\rho_y}{\rho_x}\right) \tag{7}$$

$$\delta = \sin^{-1}\left(\frac{\rho_z}{\rho}\right) \tag{8}$$

where R_{J2000} is the sensor inertial position; r_{J2000} and v_{J2000} are the satellite inertial position and velocity; ρ is the range vector between the sensor and satellite; α and δ are the "computed" optical measurements right ascension and declination; and δt_{LTC} is the light travel time correction that is applied to the optical measurements.

An overview of the multi-satellite multi-sensor scenario is presented in Fig. 6 and illustrates, for two satellites and two EO sensors, how the filter would leverage common observations to enhance information needed to estimate biases and assess performance. An outline of the process to be implemented is as follows:

1. Collect EO data (Optical 1) on a designated GPS (GPS 1) "reference" satellite.
2. Acquire the reference GPS satellite data from an International GNSS Ultra-rapid (IGU) file.
3. Refine the orbit of the tracked GPS (GPS 1) using IGU data (including SRP).
4. Estimate sensor noise and biases for the EO sensor (Optical 1) using the EO data and the refined reference satellite state.
5. Use the EO site with updated biases (Optical 1) to track a satellite in common (GeoSat) with another optical site (Optical 2)
6. Use GeoSat data as "reference for calibrating from Optical 2 sensor.
7. Continue to develop a network of vetted sensors using a multi-state filter which incorporates assessment of data and states to determine data integrity of newly included EO sensors and monitor existing sensors.

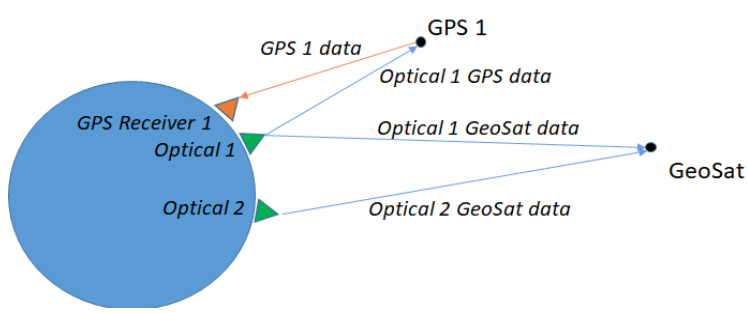


Fig. 6. 2-satellite / 2-sensor Use Case Scenario

Finally, the second part of Consensus Protocol #1 involves confirming the estimation consistency of the multi-state, multi-sensor filter is intact. For this attribute, we utilize a Filter-smoother consistency test. Specifically, a forward filter backward smoother estimation process is implemented such as the Rauch-Tung-Striebel method, the filter-smoother differences in the context of the combined uncertainties can be used as an indication of measurement and/or dynamic inconsistencies present [11].

Once two independent sensor networks are independently curated, Consensus Protocol #2 needs to be established to determine if the probabilistic representations of the two datasets overlap. An example of a statistically based consensus protocol would involve utilizing analytical expressions for the probabilistic distances between two Gaussian densities. For example, if two independently curated probability distributions are estimating debris from a post break up event, then it is likely the distances between their posterior distributions at epoch shall be minimized and there would be strong indications of consensus. In this paper, we use the Bhattacharyya Distance (stated below) as measure of consensus between two independent sensor networks.

$$J_B(p_1, p_2) = \frac{1}{8}(\mu_1 - \mu_2)^T \left[\frac{1}{2}(\Sigma_1 + \Sigma_2)\right]^{-1} (\mu_1 - \mu_2) + \frac{1}{2}\log\frac{\frac{1}{2}(\Sigma_1 + \Sigma_2)}{|\Sigma_1|^{1/2}|\Sigma_2|^{1/2}} \tag{9}$$

4. DATA TRUST USE CASE

In this section, we simulate two independent electro-optical networks trying to come to consensus that a breakup occurred in GEO. Two independent multi-state, multi-sensor use cases are simulated which included both reference data and EO tracking of a GPS reference satellite (GPS-PRN03) from a pair of sensors located in Southern Spain and South Africa (Sensor Network A) and a second pair of sensors located in Italy and India (Sensor Network B). The breakup event occurs on 18 Apr 2018 00:00:00 UTC as depicted in the Gabbard plot in Fig. 7 [12]. In this use case example GPS-PRN03 is the "Reference" and for brevity, we choose six (6) pieces of post-breakup debris to represent the Resident Space Objects ("RSOs") being observed. Additionally, Initial Orbit Determination and Multi-Hypothesis Filtering are neglected in this analysis, and we simply choose to examine agreement/disagreement between two independent sensor networks on the quality of the multi-object, multi-sensor estimation (i.e., data association is assumed). Accordingly, tracking "access" times from both pairs of independent networks are shown in Fig. 8 and Fig. 9.

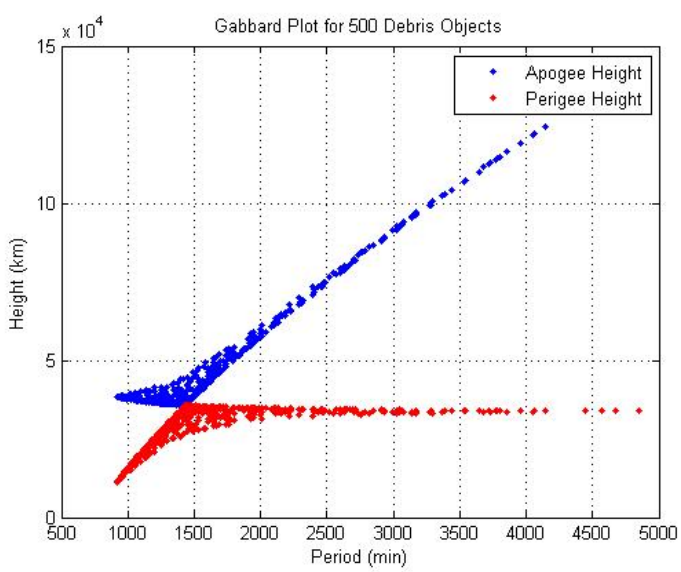


Fig. 7. Gabbard Plot of GEO Breakup generating 500 debris objects. Only six (6) pieces of debris are used in this analysis for brevity. Breakup event occurs on 18 Apr 2018 00:00:00 UTC.

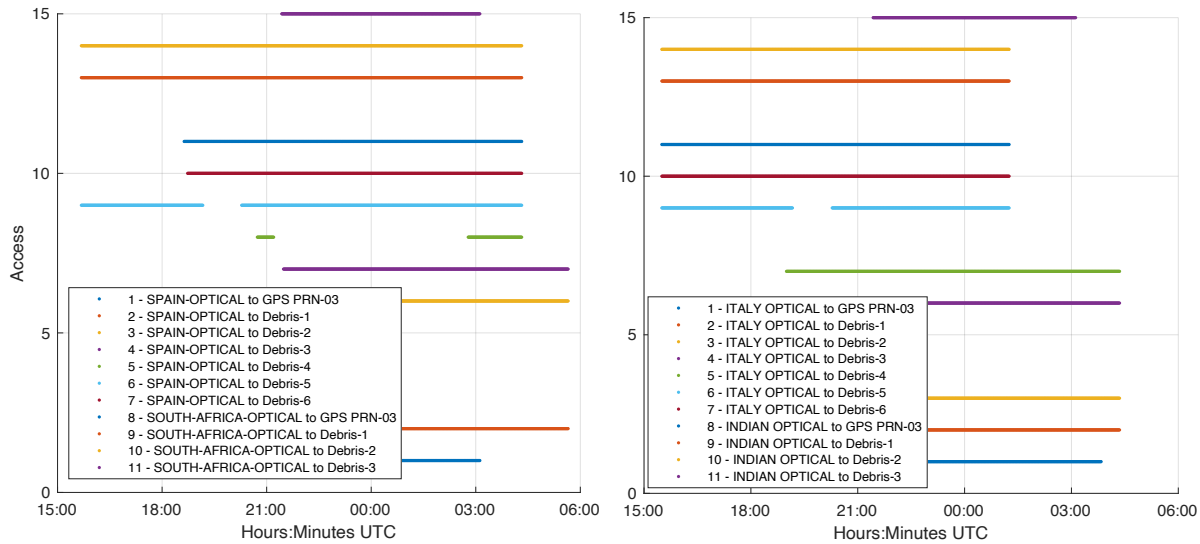


Fig. 8. Debris and GPS Access (i.e., visibility) times from both sensor networks between April 19 and 20, 2018.

The EO sensors were modeled to have a noise value of 0.5 arc-seconds, 1-σ, per right ascension and declination component, whereas each of the GPS IGU state components were generated with a 1-σ noise of 5 cm. The EO measurements were generated at a 60 second sample interval and the GPS state measurements at a 15-minute interval, consistent with the IGU files. Initial position errors of several kilometers, and velocity errors of meters-per-second, were also included in the initial satellite states. SRP errors for each satellite, a timing bias of 250 milliseconds for the Spain and Indian while a timing bias of 350 milliseconds is used for the Italy and South Africa optical sensors, respectively.

Three estimation runs are performed with the USKF: (1) Sensor Network A calibrated for timing biases, (2) Sensor Network B calibrated for timing biases, and (3) Sensor Network B not calibrated for timing biases. The goals of this use case study are the following:

1) Determine an independent sensor network is properly calibrated by holistically looking at its estimation metrics—(a) no evidence of signature in post-fit residuals, (b) posterior state error convergence, and (c) estimation consistency (i.e., filter properly predicts and updates RSO state indicating a 1-to-1 causal relationship between evidence and object).
2) Show consensus in the form of a smaller Bhattacharyya distance between calibrated posterior states for the same RSO.

These two goals represent the two consensus protocols described in the previous section. More specifically, we are curating an independent sensor network by assuring it is well calibrated and then curating agreement/disagreement between the two independent sensor networks that a space object event has occurred. If consensus is not reached on either curation, then the smart contract is not fulfilled, and the block (on which this information was requested) is not chained to previously vetted blocks. Consequently, the position and velocity state errors estimated by Sensor Networks A, B (Calibrated) and B (Uncalibrated) for the Debris-1 RSO are shown in Fig. 9, Fig. 13, and Fig.7, respectively. All errors are initially large but converge to 100's of meters based on the EO measurements. The lack of calibration of Sensor Network B does not appear show any discernable differences in state errors. Furthermore, the lack of calibration does not appear to show any differences in the Filter/Smoother consistency tests in Fig. 11, Fig.15, and Fig. 19 as well. We believe this is due to not using a large enough timing bias error and have elected to study this impact in future studies. Consequently, the measurement residuals for the Sensor Network B (Uncalibrated) run in Fig. 18 clearly show signature since the timing biases were not estimated. This impacts the posterior Debris-1 Bhattacharyya Distance in Fig. 21—although originally smaller, the Sensor Network B (Uncalibrated) case produces a larger Bhattacharyya Distance through the end of the estimation period. Finally, we take the epoch solution for all three estimation runs and backpropagate them to the breakup event epoch (18 Apr 2018 00:00:00 UTC) to study any

discernable difference on the Gabbard plot. The results show minimal differences between the calibrated and uncalibrated runs for Sensor Network A but a slightly more noticeable difference between Sensor A (likely due to sensor geometry). Suffice it to say, there many simulation parameters that can be changed in this analysis to study their impact on the breakup event. However, we have demonstrated a first-cut look at data attribution, immutability, and forensics on a Blockchain and what possible data curation consensus protocols could look like that establish well-vetted and cyber secure SDA intelligence.

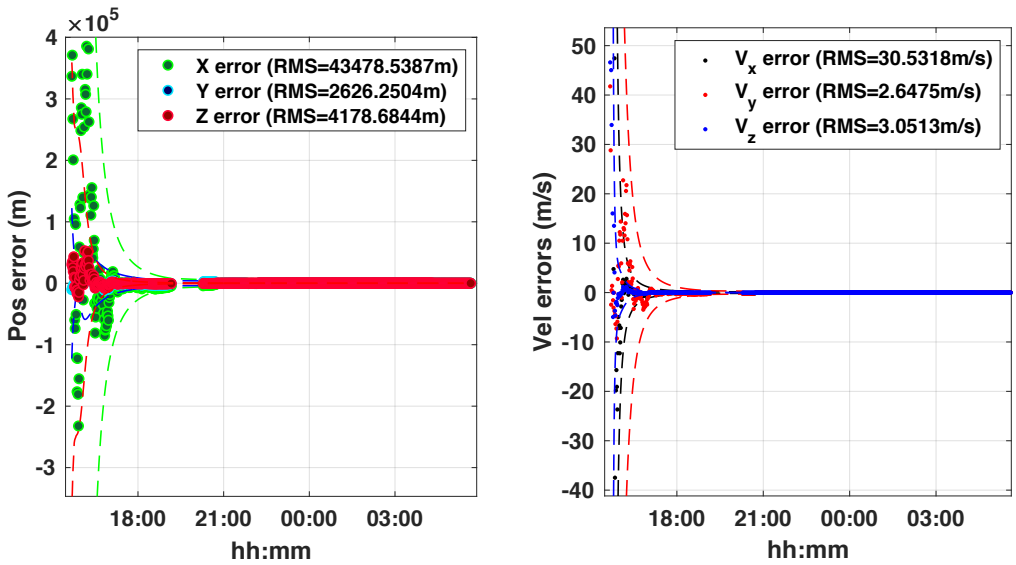


Fig. 9. Sensor Network A (i.e., Spain and South Africa) Debris-1 Position and Velocity Estimation Errors.

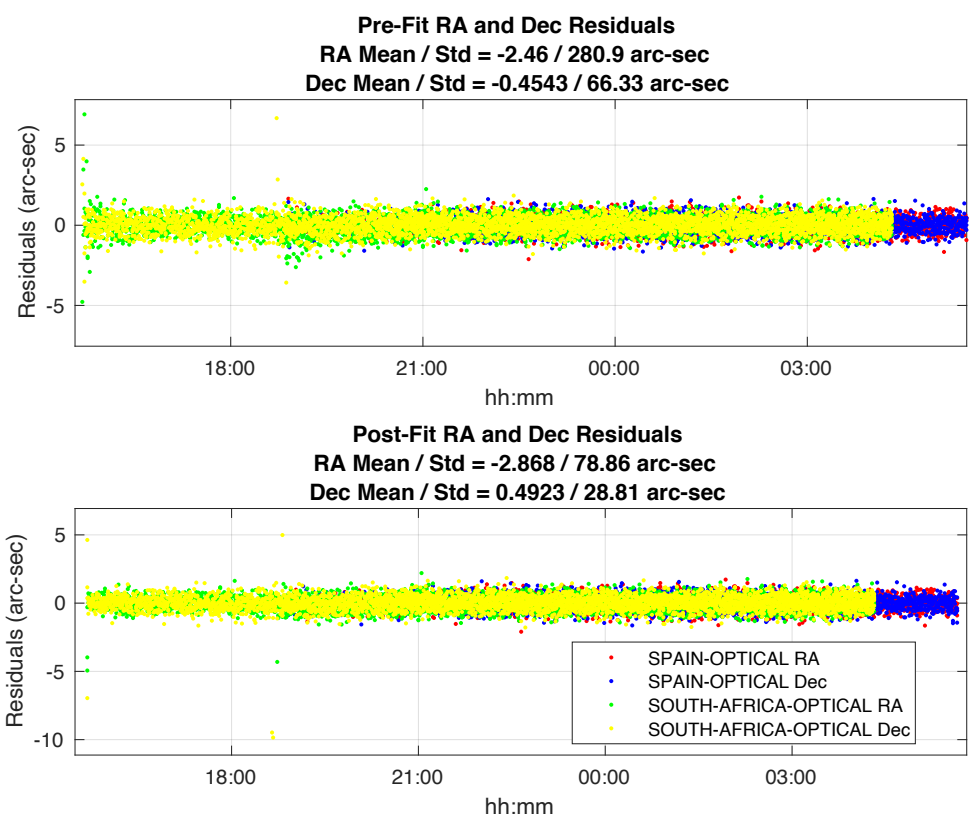


Fig. 10. Sensor Network A (i.e., Spain and South Africa) Right Ascension and Declination Residuals.

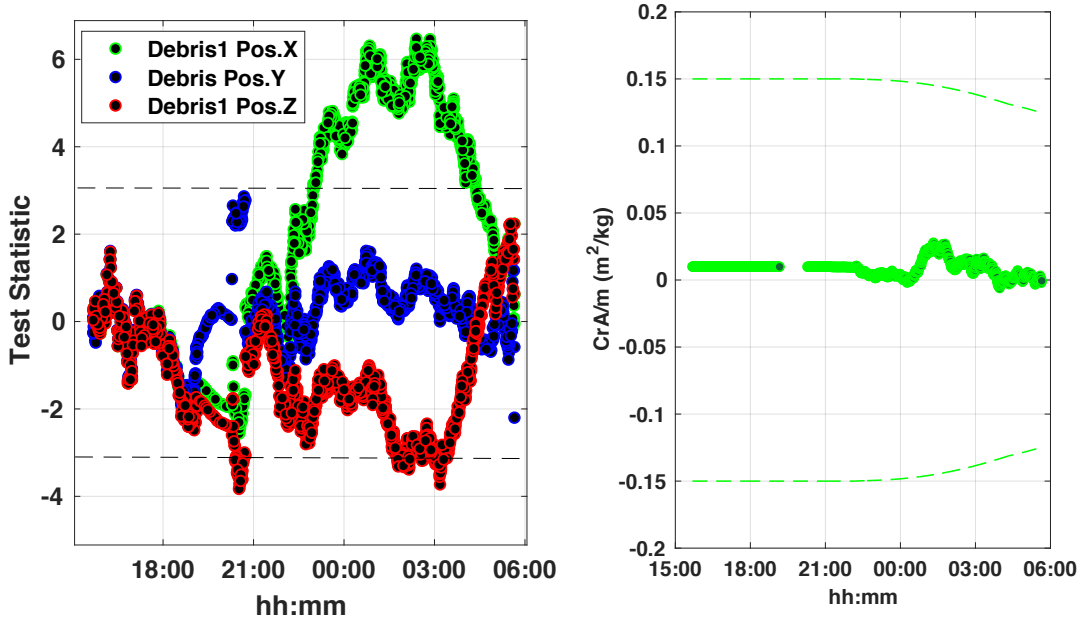


Fig. 11. Sensor Network A (i.e., Spain and South Africa) Debris-1 Filter/Smoother Consistency and CrA/m Estimation Errors.

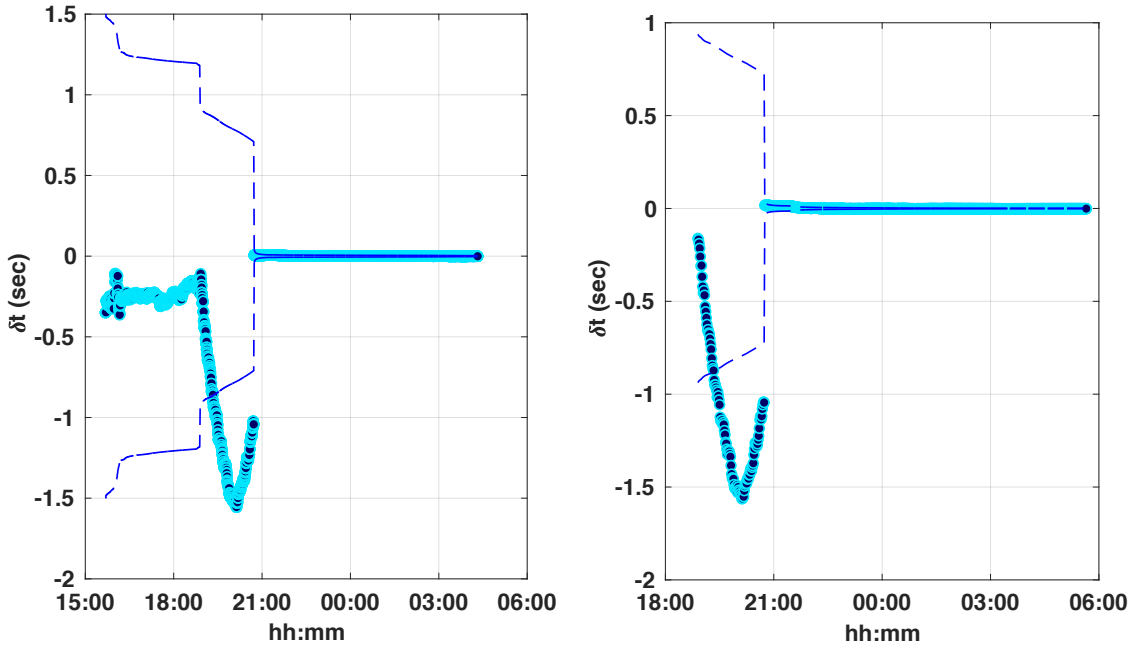


Fig. 12. Sensor Network A (i.e., Spain and South Africa) Timing Bias Correction. Left: Spain. Right: South Africa.

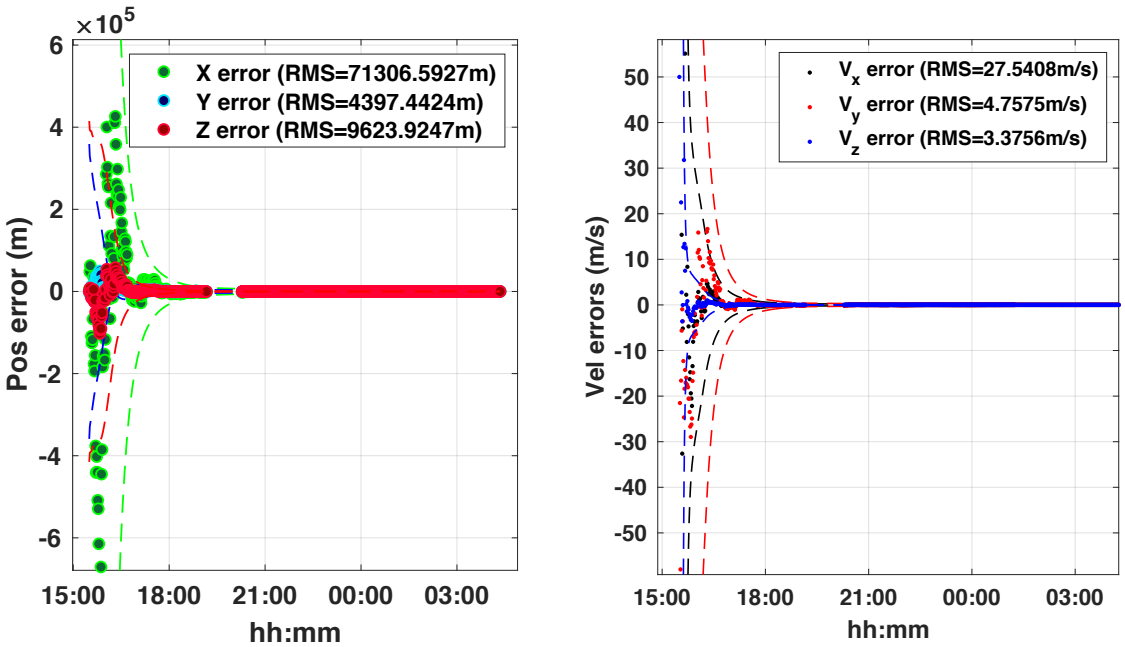


Fig. 13. Sensor Network B—Calibrated (i.e., Italy and India) Debris-1 Position and Velocity Estimation Errors.

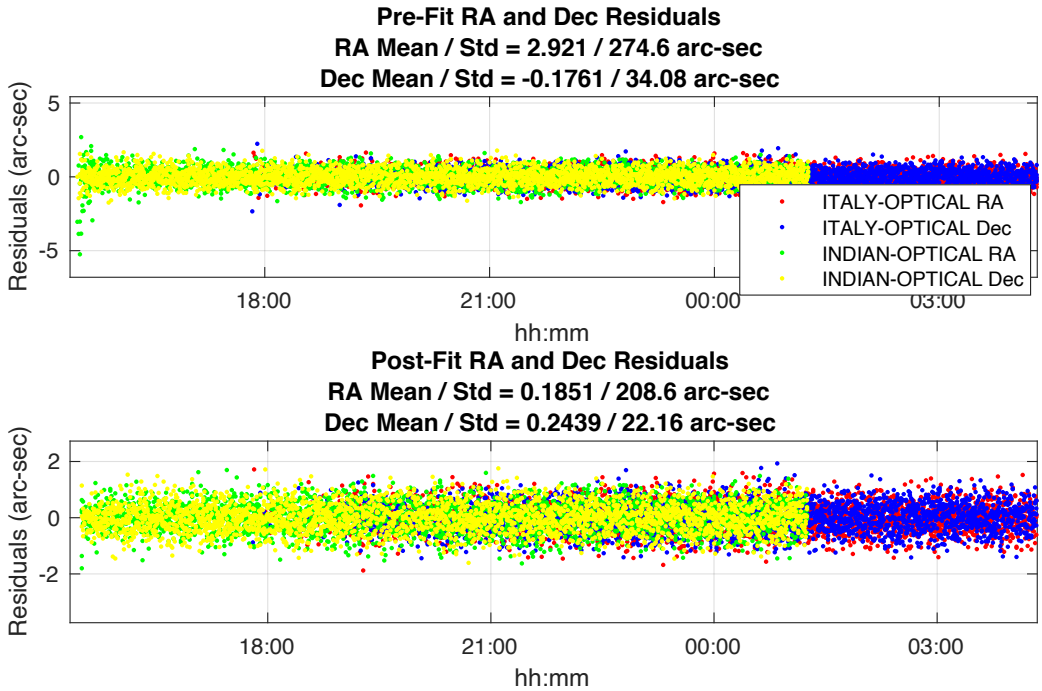


Fig. 14. Sensor Network B—Calibrated (i.e., Italy and India) Right Ascension and Declination Residuals.

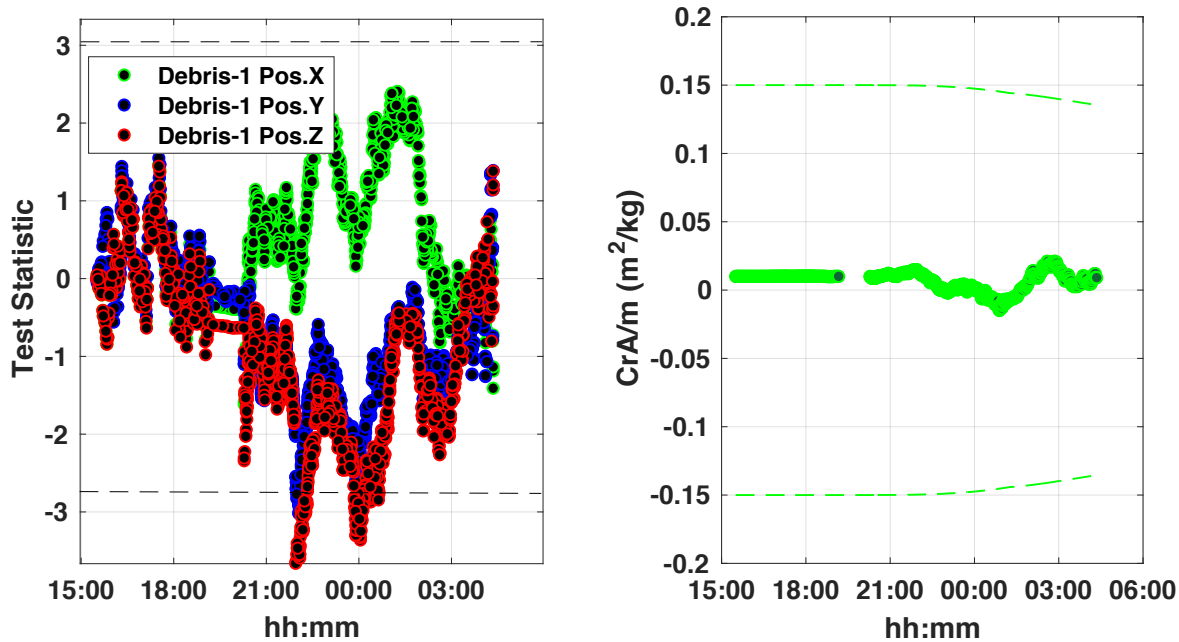


Fig. 15. Sensor Network B—Calibrated (i.e., Italy and India) Debris-1 Filter/Smoother Consistency and CrA/m Estimation Errors.

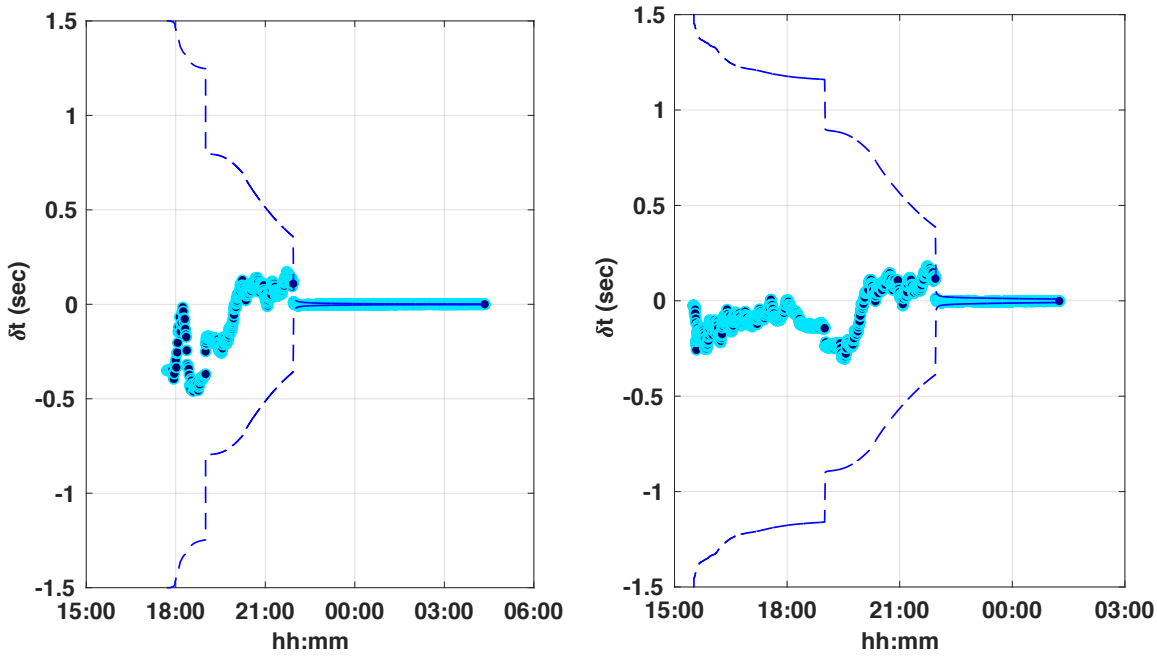


Fig. 16. Sensor Network B (i.e., Italy and India) Timing Bias Correction. Left: Italy. Right: India.

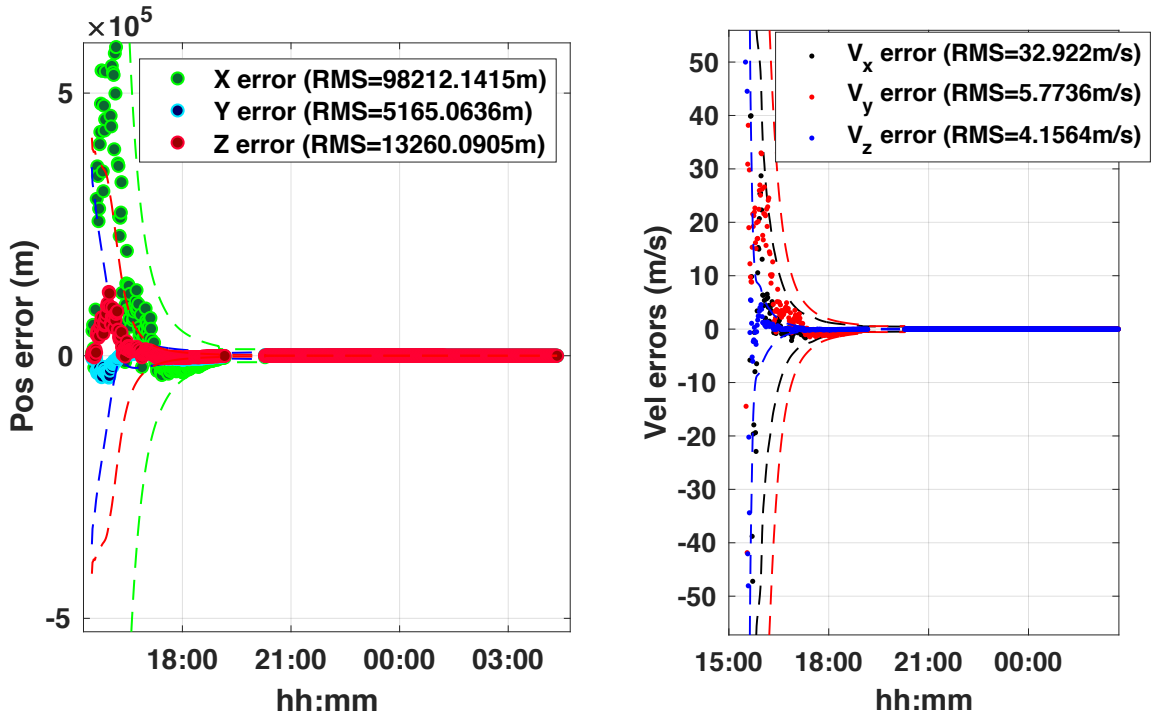


Fig. 17. Sensor Network B—Uncalibrated (i.e., Italy and India) Debris-1 Position and Velocity Estimation Errors.

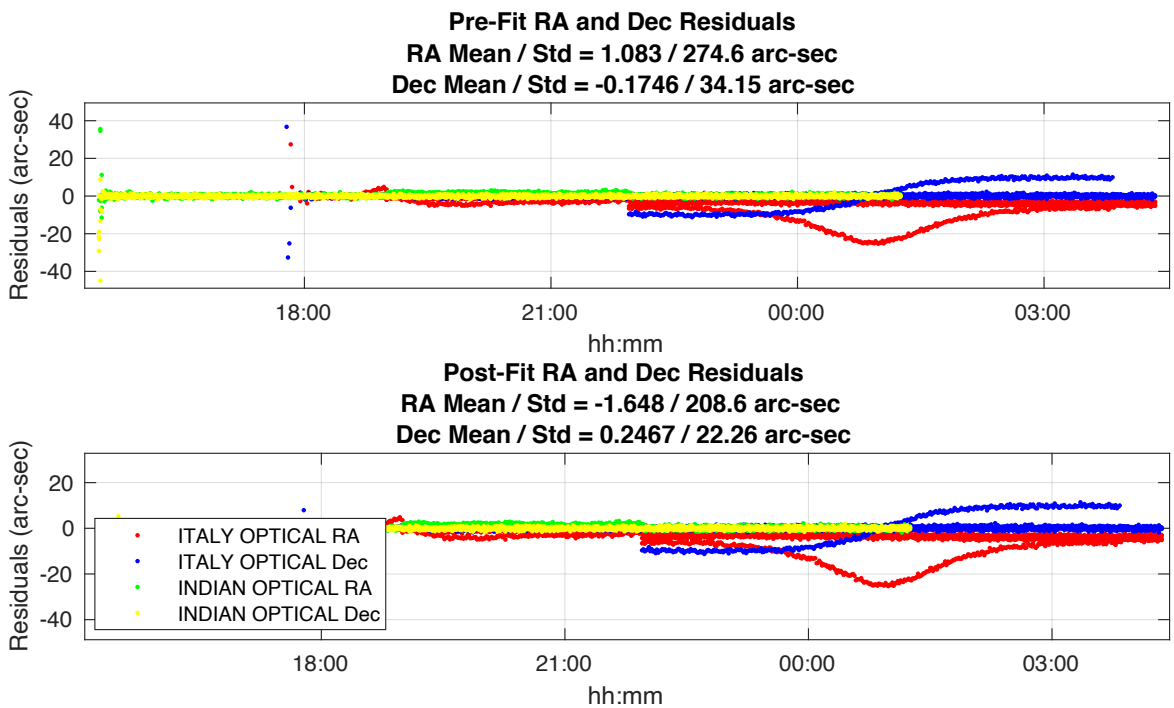


Fig. 18. Sensor Network B—Uncalibrated (i.e., Italy and India) Right Ascension and Declination Residuals.

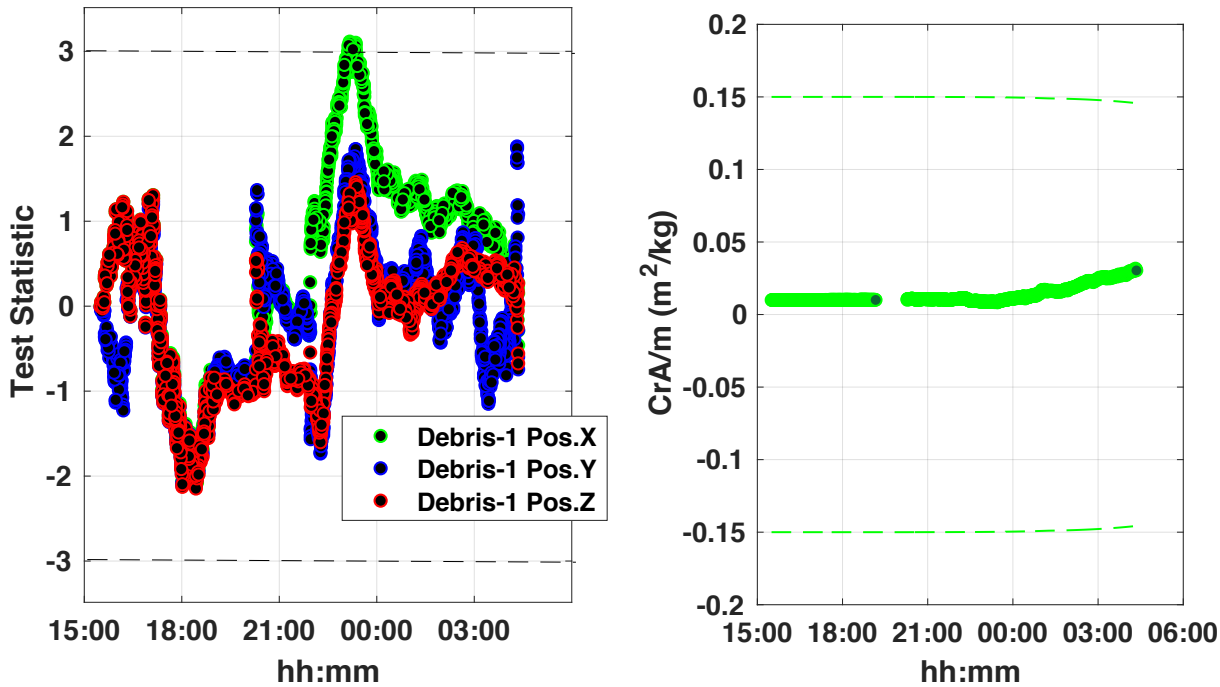


Fig. 19. Sensor Network B—Uncalibrated (i.e., Italy and India) Debris-1 Filter/Smoother Consistency and CrA/m Estimation Errors.

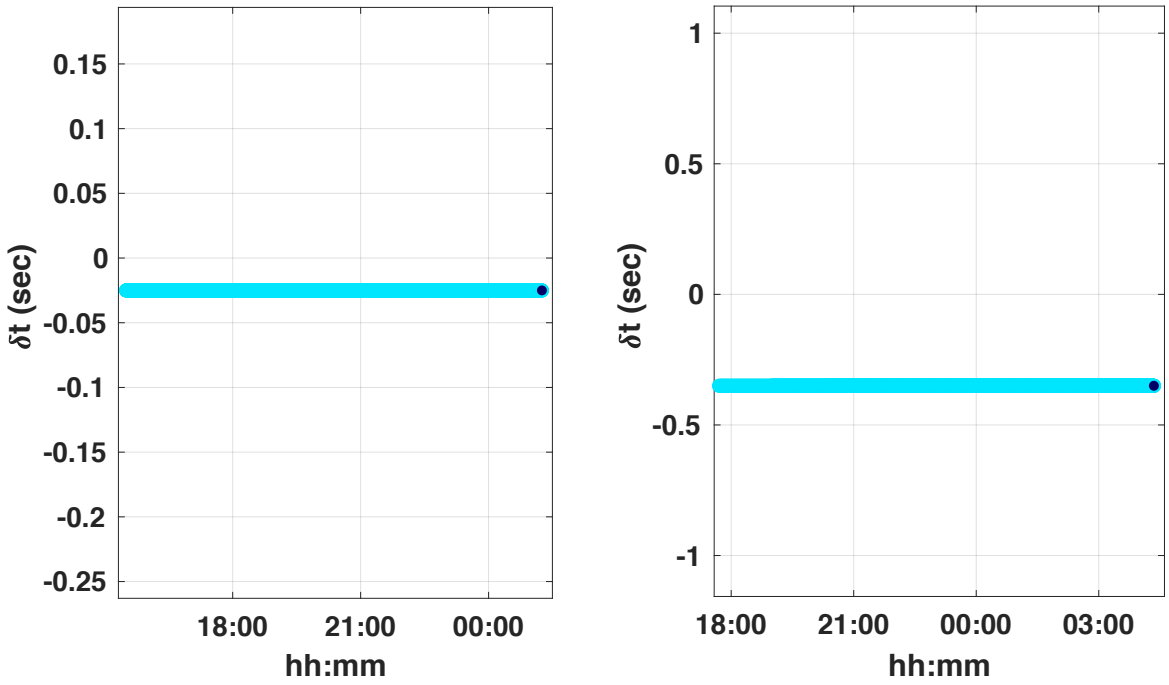


Fig. 20. Sensor Network B (i.e., Italy and India) Timing Bias Correction. Left: India. Right: Italy.

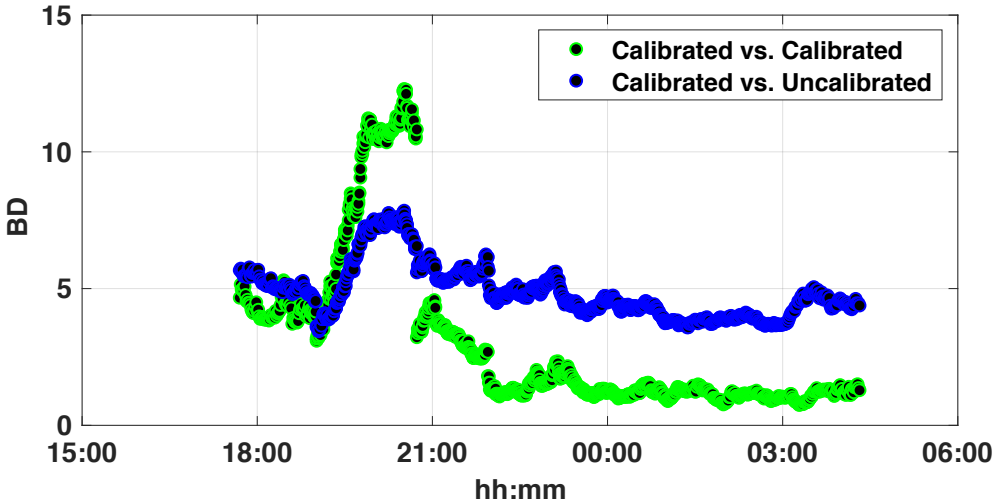


Fig. 21. Bhattacharyya Distance History Between Sensor Networks A and B (Calibrated an Uncalibrated) indicating a potential measure of empirical consensus.

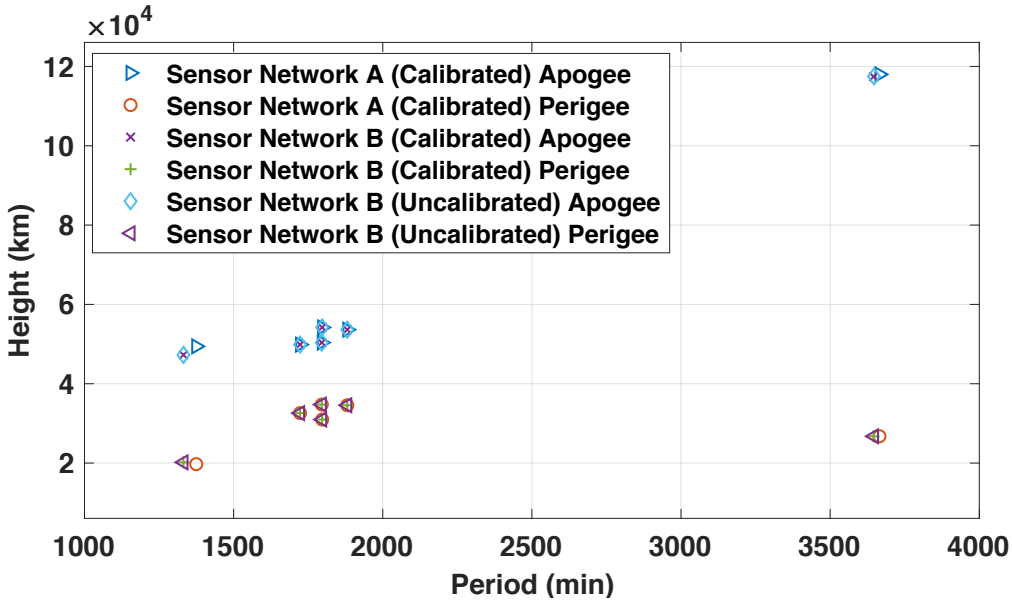


Fig. 22. Gabbard Plot of Breakup with Backpropagated states from all three estimation runs.

5. CONCLUSION

This paper offers a possible framework to not only capture the digital forensics of an SDA space object event but also carefully establishes a method to trust independent SDA sensor data that leads to operational consensus between allies. Topics such the establishment of spacecraft norms of behavior will ultimately lead to contesting or supporting such norms with independent sensor network data—a process that surely involves consensus between those who established those norms. With that said, there is much work needed to be done to completely operationalize and evolve the proposed framework in a global SDA theater. Blockchain requires security tasks such as identity (i.e., cyber security) and access management (i.e., communications and transmission infrastructure) as well as interfaces to a plethora of decentralized participants, should they elect to participate. Integration of the proposed framework may occur either

to existing data lakes or directly to data provider and curator RESTful interfaces. Nonetheless, a baseline for data attribution, immutability, and forensics is established while possible consensus protocols revealing well calibrated sensor networks and disparate sensor network agreement is offered as the first steps to a global SDA construct.

6. REFERENCES

[1] Space Policy Directive-3, National Space Traffic Management Policy. 18 June 2018, https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/ (accessed 02.10.20).

[2] Space Domain Awareness. Department of the Air Force. Memorandum for Headquarters Air Force Space Command. 14th Air Force. Space and Missile Systems Center. 2010, 14 October.

[3] US Space Force to begin sharing technical space data with UK. 18 Aug 2020, https://dailyhodl.com/2020/09/24/u-s-space-force-using-blockchain-technology-to-protect-sensitive-data/ (Accessed. 08.31.2021).

[4] Hale, L. et al, "Partnering Not Bossing: Better Leveraging International Capabilities for Space Domain Awareness." Position Paper. The Aerospace Corporation, Aug 2021.

[5] The Difference Between Blockchain and Distributed Ledger Technology. 30 Jan 2018, https://tradeix.com/distributed-ledger-technology/. (Accessed. 08.03.2021).

[6] Applications of the Merkle Tree Data Structure. 16 Jun 2020, https://medium.com/@brianrusseldavis/applications-of-the-merkle-tree-data-structure-f6696d07f7ac (Accessed. 08.31.2021).

[7] L. Wang, R. Jones. Big Data Analytics for Disparate Data. American Journal of Intelligent Systems. 7(2) (2017) 39-46.

[8] T.J. Koury (CEO, DigitalArsenal.io), personal conversation, 3 Dec 2020.

[9] Kelecy, T., R. Knox and R. Cognion, "The Extended HANDS Characterization and Analysis of Metric Biases," AMOS Technical Conference, Wailea, Maui, HI Sept 16-19, 2008.

[10] J. Stauch and M. Jah, On the Unscented Schmidt-Kalman Filter Algorithm. Journal of Guidance, Control, and Dynamics 38(1): 117-123, 2014. [11] N. Reiff. Blockchain Explained. Investopedia. 01.02.2020.

[11] Wright, J. R., "McReynolds' Filter-Smoother Consistency Test," Internal Analytical Graphics Inc. white paper, May 15, 2009.

[12] Kelecy, T & Lambert, J. "GEO Object Post-Breakup Orbit Dynamics." Technical Analysis Presentation. 23 Dec 2009.