Partial Decoding of the GPS Extended Prediction Orbit File

Vinnikov, Vladimir

IEEE Computer Society
2021-05-12

Vinnikov , V , Pshehotskaya , E & Gritsevich , M 2021 , Partial Decoding of the GPS Extended Prediction Orbit File . in S Balandin , Y Koucheryavy & T Tyutina (eds) , Proceedings of the 29th Conference of Open Innovations Association FRUCT, FRUCT 2021 . , 9435474 , Conference of Open Innovation Association, FRUCT , vol. 2021-May , IEEE Computer Society , pp. 375-384 , 29th Conference of Open Innovations Association FRUCT, FRUCT 2021 , Virtual, Tampere , Finland , 12/05/2021 . https://doi.org/10.23919/FRUCT52173.2021.9435474

http://hdl.handle.net/10138/354513
https://doi.org/10.23919/FRUCT52173.2021.9435474

unspecified
acceptedVersion

Partial Decoding of the GPS Extended Prediction Orbit File

Vladimir Vinnikov
Higher School of Economics
Moscow, Russian Federation
vvinnikov@list.ru

Ekaterina Pshehotskaya
Moscow Polytechnic University
Moscow, Russian Federation
pshehotskaya@gmail.com

Maria Gritsevich
Finnish Geospatial Research Institute (FGI)
Masala, Finland
University of Helsinki
Helsinki, Finland
Ural Federal University
Ekaterinburg, Russian Federation
maria.gritsevich@helsinki.fi

***Abstract*—The paper is concerned with decoding the Extended Prediction Orbit data format file for an Assisted-GPS web-service via cypher-text only attack. We consider mandatory data content of the file and reveal the changes of this content at different moments. The frequency of changes hints at the location of records for current GPS date and satellite orbits information. Comparing the repeating data patterns against reference orbits information, we obtain the meaning of data fields of the orbit record for each operational satellite. The partially deciphered GPS almanac data layout is provided as a table within the paper.**

I. Introduction

Global navigation satellite systems (GNSS) are playing a vital role in modern civilization. Initially devised for military navigation, these systems are now employed in commercial activity and even in everyday life. The latter became possible due to the widespread use of portable devices like smartphones, or fitness-trackers equipped with inexpensive antenna-on-chip integral schemes. The success of accurate positioning requires the knowledge of satellite coordinates at any required moment on the receiver side to estimate receiver position from its distances from satellites.

The coordinates satisfy the equations of celestial mechanics and constitute satellite orbits. Various perturbations affect the satellites and degrade the precision of once-estimated orbits. To overcome this obstacle the orbit is described simultaneously as a rough long-term almanac and more accurate short-term ephemeris. An almanac is relied upon for the initial locking on for the visible satellites. However, a receiver after a cold start does not contain an actual almanac and requires an update. The almanac retrieval from the satellites takes considerable time. In a worst-case scenario a GPS almanac downloads as long as 12 minutes for GPS due to a low data rate of only 50 bit/s. Such prolonged initialization time affects the usability of the freshly started device. However, one can improve the receiver performance via faster download of the almanac and the ephemerides into consumer receivers that are usually within the coverage of web-services.

Almost all smartphone manufacturers operate their A-GPS services. The most used services are provided by Google (for GlobalLocate chipset), Qualcomm (for gpsOne chipset), Mediatek (for SiRFStarIII chipset). In this paper, we consider an A-GPS file of Mediatek. This binary file is called Extended Prediction Orbit (EPO) and is used by various device manufacturers (e.g. see table I).

TABLE I
PROVIDERS OF AN EPO-FILE

Provider	URL
Mediatek	http://nsdu.atwebpages.com/packedephemeris.ee
Mediatek	http://epodownload.mediatek.com/EPO.DAT
Sony	http://control.d-imaging.sony.co.jp/GPS/assistme.dat
Nikon	https://downloadcenter.nikonimglib.com/en/download/fw/110.html
Nikon	https://downloadcenter.nikonimglib.com/en/download/fw/111.html
Nikon	https://downloadcenter.nikonimglib.com/en/download/fw/112.html
Olympus	http://sdl.olympus-imaging.com/agps/index.en.html
Garmin	https://www.javawa.nl/epo_en.html

Since the above-mentioned A-GPS services are associated with chipsets of different architecture, the orbits are stored in proprietary binary formats without standard data layout. Therefore, a mapping of file contents to data structures is a priori unknown. Such obscurity of the data layout is the cause of several notable problems:

- the excessive expense of computational resources;
- the non-interoperability;
- the inscrutability.

The expense of computational resources means that different A-GPS providers maintain proprietary infrastructure to calculate the orbit predictions and to keep the respective binary files available on demand. This contradicts the paradigm of carbon reduction since the positioning precision of devices like smartphones, fitness-bracelets, and digital cameras do not justify proprietary orbit calculations. Instead, the devices can easily rely on the public orbit predictions from governmental institutions like NASA or ESA.

The non-interoperability of binary files is almost self-explanatory and means that one arbitrary selected device is just unable to pull orbit data from the device with the GPS-chip of another manufacturer. This is the case with Qualcomm and Google A-GPS files. However, it is interesting enough that some GPS-chip providers use binary files of the same format.

For example, a comparison revealed that Mediatek, Sony, some Garmin watches, as well as some Nikon and Olympus cameras accept A-GPS files of the same data layout. Indeed, Sony and Mediatek provide GPS-chips for Nikon, Olympus, and Garmin products. Nevertheless, this information is not explicitly published and can only be deduced through some research. Therefore, the non-interoperability problem remains in a larger scope, and it is desirable to develop a file-converter between proprietary formats.

The inscrutability of binary files is also a problem since no malware detector is capable of scanning the proprietary contents. This problem is the most obvious of all mentioned above and is discussed below in detail.

The exposure of A-GPS file data layout is a significant factor for improving information security and reducing risks of various exploits designed to compromise end-point user devices. For example, there were reported at least two vulnerability issues for the gpsOne service (see [3], [4]). One issue was concerned with MitM-attack through unsecured HTTP able to substitute correct binary file with the fake. The other issue was the ingestion of a fake binary file of large size leading to a system crash of Android OS. These vulnerabilities allowed cumulative exploits undetectable by any antiviral scans due to the unknown structure of the binary files. The most recent issue for Suunto and Garmin devices (see [5]) was on the ingestion of the expired A-GPS file, leading to significant misalignment of obtained position. Such a problem never occurred, if the binary content could be checked independently against publicly available orbit predictions.

To resolve the MitM-issue the provider implemented a secured HTTPS access and introduced a digital signature for the A-GPS file. However, the signature per se indicates only that the initial content is unchanged since the integrity and validity of the underlying data can be only assessed through parsing, Moreover, the nature of A-GPS service with regularly provided files permits not only deciphering/decoding of the stored orbits data but also deciphering the signature algorithm as well. Once the signature algorithm is revealed, one can alter or generate anew the content of the A-GPS file and resign it. The obvious-like solution to encrypt the A-GPS file completely seems feasible only at first glance. Encryption would require key-handling procedures within the decryption parts of the client-side decoding program installed on every chip of the respective A-GPS provider. Since the A-GPS file comes in essentially one instance for all respective devices (e.g. smartphones), there can only be a singular easily extracted key to decipher the contents, which profanes the whole idea.

Thus, the knowledge of the file structure permits one to safely parse the data fields and check for any inconsistencies thus facilitating protection against potential exploits.

Usually, there are various approaches to determine the layout of the A-GPS data format, namely: data analysis, software analysis, and reverse engineering of the decoding software. The complexity of both techniques depends on many factors such as available software and hardware resources as well as a level of complement for technical documentation. According to various open-source git-repositories with Android utilities for GNSS navigation, the applications only retrieve the A-GPS file from the respective URL and proceed with an injection of the file content into the proprietary provider library. So, the software analysis yields no relevant information on the layout of the considered binary file format. The library itself usually acts as an interface to the chip firmware. This circumstance significantly complicates the latter approach, since it requires specialized software and hardware tools to obtain and reverse engineer the decoding firmware from the chip for the following analysis. As officially stated, the details on the file format and how the digital signature is verified are only available to OEMs directly from the chip manufacturer. Thus, only the former approach remains. Data analysis does not require intrusion into proprietary Android applications or tampering with chip firmware. The only research requirement is a large bulk of A-GPS binary files in the public domain that are easy to obtain.

II. The purpose of the paper

We consider the paper to play the role of the initial step, and address the problems, stated above, especially to solve the problems of non-interoperability and inscrutability. The complete solution to these two problems would require full decoding of the data layout for the majority of existing A-GPS formats. The data layouts would allow one to convert A-GPS files from one format to another, as well as to compare decoded data with ”benchmarks” published by the space agencies.

As one can see, this is a complex task that can be solved using a single approach to decoding the binary content of the A-GPS files via cryptographic attacks. To begin with, we should note the existing terminological ambiguity for the classical attacks. From our point of view, the classical attacks are the ones having historical precedence. For example, the cyphertext-only attacks on Enigma are considered by us to be classical. Moreover, these attacks were done without detailed knowledge of the encryption algorithm in the form of a mechanical blueprint. Additionally, our case always provides an approximate plaintext-cyphertext pair, while our goal is to deduce the encoding algorithm. Moreover, the A-GPS file is not truly encrypted but just encoded without concern of any encryption strength. However, we believe that this fact doesn’t invalidate the employed technique.

We aim to outline a decoding technique for A-GPS files that uses standard cryptography attacks on data redundancy and repetition. We believe that this technique is applicable not only for Mediatek EPO format but for all A-GPS formats of other providers, (e.g. Google GlobalLocate).

III. Related works

To the best of our knowledge, there are almost no publications concerned with describing of A-GPS EPO data format. The exhaustive bibliographical search yielded no relevant results except for the paper [1], considering the decoding of A-GPS data layout for Qualcomm gpsOne binary format. The decoding had a degree of success, since the almanac part of the file was recovered completely.

Most publications consider general uses of assisted GPS technologies, and, especially, its extended ephemeris (ee) part (see e.g. [6]). Such scarcity of information can be explained through ”know-how” limitations since the generation of prognostic extended ephemeris is an expensive computational task. The extended ephemeris, contained within every A-GPS file, is a valuable asset, used in various commercial sectors, in particular, in the IoT sector. A large fraction of the IoT sector is critically dependent on cold start GNSS acquisition and positioning time interval. Thus, the integrity and validity of relied upon A-GPS services are of paramount importance. For example, the recent GPS-week rollover issue caused A-GPS service inconsistency leading to severe IoT-problems and required a firmware update to more than 100000 devices (see [7]). Given the nature of the GPS-week rollover (GPS-week number presentation as modulo 1024), we regard this as a minor issue for modern devices, since it can be fixed while knowing the current date.

The lack of similar publications makes us believe that the present paper has a high level of originality. We are unable to point out other independent works on this topic.

IV. Decoding of the binary file content

A. Considerations on the file layout

A binary A-GPS file includes at least an almanac of the considered GNSS for the actual timeframe. In the case of EPO-properties, the file also contains predicted almanacs for a future timeframe. It is also worth preliminarily assume that both actual and predicted almanacs for each GNSS are represented uniformly. Currently, there are four global satellite systems: GPS, GLONASS (GLN), BEIDOU (BDS), GALILEO (GAL). However, the most used systems are GPS and GLONASS due to their long history of robust operation and completeness of orbital constellations. Therefore, it is safe to consider, that every EPO-file compulsorily contains a sequence of GPS almanacs at various successive timestamps. The descriptions usually state the EPO-file validity for 7–28 days to prolong device independence of the web-connectivity.

Since the initial broadcast GNSS-navigation messages have strict data format, an assumption can be taken that EPO-file is also coded with fix-ordered data-fields. Usually, binary files containing such data structures display periodic patterns. These patterns can hint at the size of data structures. It is also worth considering that data is stored in fields of numeric types with a minimum required byte-length to provide efficient storage.

Additionally, one should keep in mind the possibility of two different binary bitwise representations known as “Little Endian” and “Big Endian”. The former is usually used in x86 architecture, while the latter is implemented in ARM CPUs of mobile devices like smartphones.

Due to predominantly educational nature of our study, we consider the binary file for Nikon cameras, containing a GPS-only almanac (filename ”NMT_14A.ee”). An excerpts of the binary files are presented in the table II.

TABLE II
Side-to-side binary content of the files dated 09 September 2020 and 09 December 2020

Offset	00	01	02	03	04	05	06	07	00	01	02	03	04	05	06	07
0x0000	C0	70	05	**01**	23	03	20	02	48	79	05	**01**	51	01	8C	D6
0x0008	C4	21	3E	2D	A4	08	28	F8	10	DE	3E	2D	96	0F	B3	05
0x0010	66	33	02	F8	E8	21	3E	2D	90	2D	76	05	03	DE	3E	2D
0x0018	F4	3A	A8	F8	52	0F	0F	80	88	03	40	07	86	0D	D4	82
0x0020	23	8D	F1	07	91	B1	82	28	DD	87	F1	07	A5	21	8F	B4
0x0028	7F	64	24	02	C3	83	03	A6	CE	C4	3C	02	64	AF	03	A6
0x0030	E5	95	B3	37	67	2E	F4	20	F4	5F	61	E9	BA	37	04	2F
0x0038	21	91	A9	21	1C	00	00	10	94	F6	94	21	1C	00	00	10
0x0040	00	00	00	07	1A	8C	12	D1	00	00	00	04	16	07	68	B6
0x0048	C0	70	05	**02**	7F	02	20	D2	48	79	05	**02**	A6	01	8C	D8
0x0050	14	EE	3E	2D	D6	3C	3D	F9	1E	EE	3E	2D	56	22	F5	04
0x0058	25	02	C1	F9	BF	11	3E	2D	65	1D	AC	04	D1	EE	3E	2D
0x0060	05	06	E7	F8	52	3C	61	84	1B	30	32	07	BD	FA	A3	85
0x0068	45	BC	F1	07	E6	CD	36	3E	07	B0	F1	07	E7	A1	D2	BB
0x0070	6C	BF	2C	0D	72	26	00	A6	0C	3F	58	0D	48	9A	02	A6
0x0078	AB	BF	85	2A	01	81	10	20	58	45	24	EC	13	EE	22	20
0x0080	92	B2	91	BE	1C	00	00	10	38	84	B5	BF	1C	00	00	10
0x0088	00	00	10	00	29	ED	A0	9A	00	00	00	00	7F	16	8B	2C
0x0090	C0	70	05	**03**	24	02	20	A1	48	79	05	**03**	78	3E	8C	A8
0x0098	67	FE	3E	2D	03	30	FF	F9	6E	FE	3E	2D	E2	30	7A	F0
0x00A0	B3	0D	F6	F9	7F	FE	3E	2D	D6	0D	7A	FF	4A	01	3E	2D
0x00A8	D7	20	1D	07	1B	66	B8	84	A7	23	E9	F8	C2	36	B1	80
0x00B0	03	A7	F1	07	42	D6	2C	06	29	A7	F1	07	DA	24	01	84
0x00B8	E2	EA	AB	06	D6	01	00	A6	11	4C	A2	06	AD	90	03	A6
0x00C0	8C	22	11	5C	ED	DC	6F	20	98	CC	CE	1F	66	70	62	20
0x00C8	30	01	E1	22	1C	00	00	10	B7	9B	60	24	1C	00	00	10
0x00D0	00	00	00	01	B8	6C	60	CF	00	00	00	FF	5F	E8	4C	0B
0x00D8	C0	70	05	**04**	3A	3E	20	DB	48	79	05	**04**	ED	00	8C	E2
0x00E0	1D	8E	3E	2D	90	43	FF	FB	24	8E	3E	2D	FD	41	C4	FC
0x00E8	D2	62	A3	FB	C4	71	3E	2D	F2	67	9E	FB	1A	8E	3E	2D
0x00F0	32	68	FE	F8	AD	D1	75	87	36	64	1D	07	89	DF	34	86
0x00F8	B5	D9	F1	07	64	F2	89	6E	6B	D8	F1	07	5A	32	A6	FE
0x0100	EC	A2	64	07	E3	64	03	A6	0D	8A	72	07	D4	91	02	A6
0x0108	D6	FE	19	80	8E	DD	2C	20	D2	E3	CF	43	C5	4A	15	20
0x0110	D1	79	C1	8C	1C	00	00	10	CC	8C	DD	82	1C	00	00	10
0x0018	00	00	00	00	B5	9E	19	54	00	00	00	00	04	30	DA	C9
0x0120	C0	70	05	**05**	89	02	20	F9	48	79	05	**05**	15	3F	8C	F8
0x0128	3F	9E	3E	2D	5A	54	F0	F9	3E	9E	3E	2D	F7	55	2A	F0
0x0130	68	6A	C8	F8	D9	61	3E	2D	74	6A	F5	F0	C7	61	3E	2D
0x0138	99	40	4F	07	FF	32	31	84	55	40	B7	F8	10	77	F1	85
0x0140	B1	C5	F1	07	76	89	1E	A1	26	C4	F1	07	F5	FC	92	20
0x0148	F9	DA	2E	04	1D	A9	03	A6	BF	B4	17	04	8B	59	00	A6

B. Considerations on the cryptography attacks exploiting data redundancy

It is known that binary A-GPS files have a proprietary format, but are not truly encrypted, since encryption will only raise costs without any real benefit. Nevertheless, the obscurity of data layout can still be treated as some kind of encryption. This is the case of the paradigm ”security through obscurity”, which implementations are widely recognized as bad practice. However, this circumstance facilitates the recovery of underlying data structure in contrast to obtaining layout from proper classical encryption.

The data structure of the EPO binary file is defined by the sequential non-intersecting ranges of bytes that map into various numeric data types. The common approach to determine the fields of this data structure is to establish matches between numeric values and their reference counterparts. The sought-for numeric values vary with a timestamp of the binary file, so we implement quasi-differential cryptanalysis to reveal change patterns within the data on different timescales. In contrast to the true differential cryptanalysis, this study relies on a partial quasi-known-plaintext attack instead of a chosenplaintext attack. Usually, the attacker resorts to a quasi-known-plaintext attack if he still lacks the original plaintext but has some hints on the magnitude and sign of encoded numeric values.

These approaches to cryptanalysis require a large corpus of cyphertexts with at least partially known differences of the respective plaintexts. The properties of the A-GPS service fulfill the requirements since the underlying data on-orbit elements change several times in a day. Therefore, one can assemble the demanded volume of cyphertexts with respective timestamps within a reasonable timeframe.

C. Analysis of an EPO binary file

Since the GNSS-positioning technology by design relies heavily on timing, the primary parameter is the timestamp of data origin. This timestamp is expressed in terms of GPS-week and GPS-day numbers (e.g. [8]), as well as seconds, elapsed from some reference instance. Usually, the precise GNSS-positioning operates on the timescale of milliseconds, so it is possible to encounter a data field holding the number of milliseconds. However, such precision is not fully required for A-GPS applications that use the only almanac for fast satellite acquisition.

At the initial stage, we obtain the set of binary files with varying distances between the respective timestamps. The temporal step between the changes of the file content can be as short as about 45 minutes, but the step of 12 hours is usually sufficient for decoding the almanac.

At the main stage, we perform a byte-to-byte comparison of the downloaded files via one of the hexadecimal viewers. Our practice suggests that it is more convenient to start comparing the files with the maximum timestamp distance between them. Table III shows the excerpt of a binary difference of the files dated 09 September 2020 and 09 December 2020, while the table IV corresponds to the dates of 17 August 2020 and 11 December 2020.

As one can see, binary differences for various timestamp intervals still have common numeric values at some offsets (see table V). The results reveal that byte-values occupying offsets 0x0002, 0x004A, 0x0092, 0x00DA, and 0x0122 are constant across all obtained binary files, while byte-values at the positions following next form an incremental sequence starting from one. Considering this, we assume that the sequence contains PRN designators (PRN$\in$[1;32]) of GPS satellites. This assumption leads us to the size of a single record holding an almanac for the GPS satellite with respective PRN designator. Deducting offsets (e.g. 0x004B minus 0x0003) we obtain the record size equal to 0x0048 or in decimal system 72 bytes.

Knowing record size we can continue the main stage with auto-comparison of records within the same binary file. Analyzing 32 first records of the same file we reveal two types of content, namely content for operational GPS satellites, and content for nonoperational GPS satellites. Table VI contains common byte-values for records of the file dated 09 September 2020 as well as of the file dated 11 September 2020.

As one can see, the records for both operational and nonoperational satellites contain common three bytes, starting at zero offsets. If we parse the file further, then we encounter different three bytes common to the next 32 records at the same relative zero offsets. Thus, each bunch of 32 records is associated with a three-byte value. The sequences of these record headers for files with different timestamps are presented in the table VII.

The revealed sequences consist of monotonically increasing numeric values. Moreover, these values increase uniformly. However, the exact difference between successive values depends on a binary representation. If data is stored in "Little Endian" format then the constant step equals 6. In the case of the acting "Big Endian" convention, the step is 393216. To deduce the type of "Endianness" we compare first record headers and the full timestamps of the respective EPO-files (see table VIII).

Considering record headers for timestamps of 11 and 12 September 2020, we assume that the order of bytes corresponds to "Little Endian" encoding. Thus, the three-byte record header contains the number of hours since some reference point of time, and the discrete timestep between the successive records is 6 hours.

Analyzing table VII we revealed that the same tree-byte headers are written at different offsets in EPO-files with different timestamps. This circumstance allows one to compare predicted and actual orbit data for every operational satellite at the same moment (see table IX). It is also useful to proceed with the same comparison for nonoperational satellites (see table X).

At first, the table IX doesn't provide any obvious insight on the data layout of the record. One can only point out the common three bytes "0x1C 0x00 0x00" at the offset 0x003C. On the contrary, table X gives more information on the layout. The differences between records for nonoperational PRN14 in different files are sparse. The regularly varying bytes are at the offsets 0x0006, 0x0023. These bytes form a sequence presented in table XI and follow the temporal pattern.

Additionally, one can see the offset pattern of differences in records for nonoperational PRN14. The four-byte-arrangement of the table IX hints at the correlation of the last 32-bit integer in the record at offset 0x0044, and the 32-bit integers at offsets 0x0004 and 0x0020. Since the common design of the record structure puts a control checksum at the end of the record, we assume that the last 32-bit integer is indeed a checksum in the form of XOR operations on the sequence of 32-bit integers.

The significant part of the deciphering technique is the PRN-wise comparison of actual orbit data within EPO-file with independent official data, provided by one of the space agencies [9]. To facilitate such comparison it is convenient to rearrange unknown EPO-file contents into rows of signed decimal integers, single PRN per row. Using the signed integers is essential since we aim to match the sign patterns of orbit data from two different sources.

The table XII contains the signs of orbital parameters at the date of 7 Feb 2021 provided in [9]. The signs of 32-bit

TABLE III
BINARY DIFFERENCE OF THE FILES DATED 09 SEPTEMBER 2020 AND 09 DECEMBER 2020

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
0x0000	--	--	05	01	--	--	--	--	--	--	3E	2D	--	--	--	--	--	--	--	--	--	--	3E	2D	--	--	--	--	--	--	--	--
0x0020	--	--	F1	07	--	--	--	--	--	--	--	02	--	--	03	A6	--	--	--	--	--	--	--	--	--	--	--	21	1C	00	00	10
0x0040	00	00	00	--	--	--	--	--	--	--	05	02	--	--	--	--	--	EE	3E	2D	--	--	--	--	--	--	--	--	--	--	3E	2D
0x0060	--	--	--	--	--	--	--	--	--	--	F1	07	--	--	--	--	--	--	--	0D	--	--	--	A6	--	--	--	--	--	--	--	20
0x0080	--	--	--	--	1C	00	00	10	00	00	--	00	--	--	--	--	--	--	05	03	--	--	--	--	--	FE	3E	2D	--	30	--	--
0x00A0	--	0D	--	--	--	--	3E	2D	--	--	--	--	--	--	--	--	--	A7	F1	07	--	--	--	--	--	--	--	06	--	--	--	A6
0x00C0	--	--	--	--	--	--	--	20	--	--	--	--	1C	00	00	10	00	00	00	--	--	--	--	--	--	--	05	04	--	--	--	--
0x00E0	--	8E	3E	2D	--	--	--	--	--	--	--	FB	--	--	3E	2D	32	68	--	--	--	--	--	--	--	--	F1	07	--	--	--	--
0x0100	--	--	--	07	--	--	--	A6	--	--	--	--	--	--	--	20	--	--	--	--	1C	00	00	10	00	00	00	00	--	--	--	--
0x0120	--	--	05	05	--	--	--	--	--	9E	3E	2D	--	--	--	--	--	6A	--	--	--	61	3E	2D	--	40	--	--	--	--	--	--
0x0140	--	--	F1	07	--	--	--	--	--	--	--	04	--	--	--	A6	--	--	--	--	--	--	--	21	--	--	--	--	1C	00	00	10

TABLE IV
BINARY DIFFERENCE OF THE FILES DATED 17 AUGUST 2020 AND 11 DECEMBER 2020

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
0x0000	--	--	05	01	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	DE	--	--	--	--	--	--	--	--	--
0x0020	--	--	F1	07	--	--	--	--	--	--	--	02	--	--	03	A6	--	--	--	--	--	--	--	--	--	--	--	21	1C	00	00	10
0x0040	00	00	00	--	--	--	--	--	--	--	05	02	--	--	--	--	--	EE	--	--	--	20	--	--	--	--	--	--	--	--	--	--
0x0060	--	--	--	--	--	--	--	85	--	--	F1	07	--	--	--	--	--	--	--	0D	--	--	--	A6	--	--	--	--	--	--	--	20
0x0080	--	--	--	--	1C	00	00	10	00	00	--	00	--	--	--	--	--	--	05	03	--	--	--	--	--	FE	--	--	--	--	--	--
0x00A0	--	--	--	--	--	--	--	--	--	--	07	--	--	--	--	--	--	--	F1	07	--	--	--	--	--	--	--	06	--	--	--	A6
0x00C0	--	--	--	--	--	--	--	20	--	--	--	--	1C	00	00	10	00	00	--	--	--	--	--	--	--	--	05	04	--	--	--	--
0x00E0	--	8E	--	--	--	--	--	--	--	--	--	--	--	8E	--	--	32	68	--	--	--	--	--	--	--	86	--	D9	F1	07	--	--
0x0100	--	--	--	07	--	--	--	A6	--	--	--	--	--	--	--	20	--	--	--	--	1C	00	00	10	00	00	00	00	--	--	--	--
0x0120	--	--	05	05	--	01	--	--	--	9E	--	--	--	--	--	--	--	--	--	--	--	61	--	--	--	--	--	--	--	--	--	--
0x0140	--	--	F1	07	--	--	--	--	--	--	--	04	--	--	--	A6	--	--	--	--	--	--	--	21	--	--	--	--	1C	00	00	10

TABLE V
COMMON NUMERIC VALUES FOR BINARY DIFFERENCES OF THE FILES DATED 09 SEPTEMBER 2020 AND 09 DECEMBER 2020, AND 17 AUGUST 2020 AND 11 DECEMBER 2020

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
0x0000	--	--	05	01	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
0x0020	--	--	F1	07	--	--	--	--	--	--	--	02	--	--	03	A6	--	--	--	--	--	--	--	--	--	--	--	21	1C	00	00	10
0x0040	00	00	00	--	--	--	--	--	--	--	05	02	--	--	--	--	--	EE	--	--	--	--	--	--	--	--	--	--	--	--	--	--
0x0060	--	--	--	--	--	--	--	--	--	--	F1	07	--	--	--	--	--	--	--	0D	--	--	--	A6	--	--	--	--	--	--	--	20
0x0080	--	--	--	--	1C	00	00	10	00	00	--	00	--	--	--	--	--	--	05	03	--	--	--	--	--	FE	--	--	--	--	--	--
0x00A0	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	F1	07	--	--	--	--	--	--	--	06	--	--	--	A6
0x00C0	--	--	--	--	--	--	--	20	--	--	--	--	1C	00	00	10	00	00	--	--	--	--	--	--	--	--	05	04	--	--	--	--
0x00E0	--	8E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	32	68	--	--	--	--	--	--	--	--	--	--	--	--	--	--
0x0100	--	--	--	07	--	--	--	A6	--	--	--	--	--	--	--	20	--	--	--	--	1C	00	00	10	00	00	00	00	--	--	--	--
0x0120	--	--	05	05	--	--	--	--	--	9E	--	--	--	--	--	--	--	--	--	--	--	61	--	--	--	--	--	--	--	--	--	--
0x0140	--	--	F1	07	--	--	--	--	--	--	--	04	--	--	--	A6	--	--	--	--	--	--	--	21	--	--	--	--	1C	00	00	10

TABLE VI
BINARY AUTO-DIFFERENCES OF THE FIRST 32 RECORDS DATED 09 SEPTEMBER 2020 AND 11 SEPTEMBER 2020

	operational GPS								nonoperational GPS								operational GPS								nonoperational GPS							
Offset	00	01	02	03	04	05	06	07	00	01	02	03	04	05	06	07	00	01	02	03	04	05	06	07	00	01	02	03	04	05	06	07
0x0000	C0	70	05	--	--	--	20	--	C0	70	05	00	00	00	20	00	08	71	05	--	--	--	2C	--	08	71	05	00	00	00	2C	00
0x0008	--	--	3E	2D	--	--	--	--	C6	31	0E	07	C6	31	0E	07	--	--	76	6E	--	--	--	--	C6	31	0E	07	C6	31	0E	07
0x0010	--	--	--	--	--	--	3E	2D	C6	31	0E	07	C6	31	0E	07	--	--	--	--	--	--	76	6E	C6	31	0E	07	C6	31	0E	07
0x0018	--	--	--	--	--	--	--	--	C6	31	0E	07	C6	31	--	--	--	--	--	--	--	--	--	A6	C6	31	0E	07	C6	31	--	38
0x0020	--	--	F1	07	--	--	--	--	C6	31	0E	07	C6	31	0E	07	--	--	--	--	--	--	--	--	C6	31	0E	07	C6	31	0E	07
0x0028	--	--	--	--	--	--	--	A6	C6	31	0E	07	C6	31	0E	07	--	--	--	--	--	--	--	--	C6	31	0E	07	C6	31	0E	07
0x0030	--	--	--	--	--	--	--	20	C6	31	0E	07	C6	31	0E	07	--	--	--	--	--	--	--	--	C6	31	0E	07	C6	31	0E	07
0x0038	--	--	--	--	1C	00	00	10	00	00	00	00	1C	00	00	90	--	--	--	--	1C	00	00	10	00	00	00	00	1C	00	00	90
0x0040	00	00	--	--	--	--	--	--	00	00	--	--	DC	70	--	40	00	00	--	--	--	--	--	--	00	00	--	EF	14	71	--	40

integers constituting each record of the EPO-file at the date 10 Feb 2021 are given in the table XIII. The column headers designate respective offsets from the start of the record. The sign comparison reveals that column 0x30 corresponds to the column $L\Omega$. The same goes for column 0x38 and column ω. circumstance allows one to compare predicted and actual orbit data for every operational satellite at the same moment. Some matching positions can also be observed for column 0x04 and column af_1.

Despite the established sign matches, the values in the corresponding columns are different (see table XIV). Computing row-wise or column-wise ratios between the said values one can easily see that the relationship is not the same for different PRN-designators. This means that either the relationship is nonlinear, or the contents of an EPO-file are computed with significantly lower precision, than the counterparts in the official resources provided by the space agencies. We also considered the 64-bit integer record-layout that keeps the

TABLE VII

THE THREE BYTE RECORD HEADERS OF FILES WITH DIFFERENT TIMESTAMPS

i	Offset	09 Sep 2020	11 Sep 2020	09 Dec 2020	11 Dec 2020
000	0x000000	C0 70 05	08 71 05	48 79 05	78 79 05
001	0x000900	C6 70 05	0E 71 05	4E 79 05	7E 79 05
002	0x001200	CC 70 05	14 71 05	54 79 05	84 79 05
003	0x001B00	D2 70 05	1A 71 05	5A 79 05	8A 79 05
004	0x002400	D8 70 05	20 71 05	60 79 05	90 79 05
005	0x002D00	DE 70 05	26 71 05	66 79 05	96 79 05
006	0x003600	E4 70 05	2C 71 05	6C 79 05	9C 79 05
007	0x003F00	EA 70 05	32 71 05	72 79 05	A2 79 05
008	0x004800	F0 70 05	38 71 05	78 79 05	A8 79 05
009	0x005100	F6 70 05	3E 71 05	7E 79 05	AE 79 05
010	0x005A00	FC 70 05	44 71 05	84 79 05	B4 79 05
011	0x006300	02 71 05	4A 71 05	8A 79 05	BA 79 05
012	0x006C00	08 71 05	50 71 05	90 79 05	C0 79 05
013	0x007500	14 71 05	56 71 05	96 79 05	C6 79 05
014	0x007E00	1A 71 05	5C 71 05	9C 79 05	CC 79 05
015	0x008700	20 71 05	62 71 05	A2 79 05	D2 79 05
016	0x009000	26 71 05	68 71 05	A8 79 05	D8 79 05
...	...	...	...	...	
n	0x0900*i	0x0570C0+6i	0x057108+6i	0x057948+6i	0x057978+6i
...	...	...	...	...	
119	0x042F00	8A 73 05	D2 73 05	12 7C 05	42 7C 05

TABLE VIII

COMPARISON OF RECORD HEADERS AND FULL TIMESTAMPS OF RESPECTIVE EPO-FILES

Date	Time	Header
09 Sep 2020	00:32	C0 70 05
09 Sep 2020	20:10	D8 70 05
10 Sep 2020	22:13	F0 70 05
11 Sep 2020	22:50	08 71 05
12 Sep 2020	22:50	20 71 05
13 Sep 2020	19:41	38 71 05
14 Sep 2020	18:08	50 71 05
09 Dec 2020	02:29	48 79 05
11 Dec 2020	01:59	78 79 05

TABLE IX

THE RECORDS FOR OPERATIONAL SATELLITE AT THE SAME TIMESTAMP WITHIN THE FILES WITH DIFFERENT TIMESTAMPS

Offset	17 Aug 2020 23:45	07 Sep 2020 21:12	09 Sep 2020 00:32	09 Sep 2020 20:10	10 Sep 2020 22:13	11 Sep 2020 22:50
0x0000	08 71 05 01	08 71 05 01	08 71 05 01	08 71 05 01	08 71 05 01	08 71 05 01
0x0004	4E 00 C8 12	59 00 1C 03	58 00 20 02	58 00 24 02	58 00 28 01	58 00 2C 01
0x0008	D4 21 76 6E	C5 21 76 6E	C4 21 76 6E	C4 21 76 6E	C7 21 76 6E	C7 21 76 6E
0x000C	38 08 FF F0	3A 08 FF F0	3A 08 FF F0	3A 08 FF F0	3D 08 FF F0	3A 08 FF F0
0x0010	B0 2D B5 FF	BF 2D B3 FF	BF 2D B2 FF	BF 2D B2 FF	BF 2D B2 FF	BF 2D B2 FF
0x0014	D2 21 76 6E	D2 21 76 6E	D2 21 76 6E	D2 21 76 6E	D2 21 76 6E	D2 21 76 6E
0x0018	ED 03 B2 F8	ED 03 B2 F8	ED 03 B2 F8	ED 03 B2 F8	ED 03 B2 F8	ED 03 B2 F8
0x001C	F6 62 4F B8	B2 0E 4F A0	E8 0E 4F A0	CC 0E 4F 80	12 0F 4F 80	7C 0F 0F 80
0x0020	46 8A F1 63	47 8A F1 17	47 8A F1 0B	47 8A F1 0F	47 8A F1 03	47 8A F1 07
0x0024	D2 DC ED 34	25 47 EA 34	15 42 EA 34	F1 47 EA 34	49 45 EA 34	D2 44 EA 34
0x0028	0C 12 24 02	44 0D 24 02	91 0A 24 02	F1 0A 24 02	B0 0A 24 02	43 0A 24 02
0x002C	B0 85 03 A6	4B 82 03 A6	45 82 03 A6	47 82 03 A6	BC 82 03 A6	BE 82 03 A6
0x0030	23 BE A6 37	56 BF A6 37	67 BF A6 37	6C BF A6 37	77 BF A6 37	76 BF A6 37
0x0034	46 4D F4 20	5C 4D F4 20	50 4D F4 20	56 4D F4 20	4B 4D F4 20	48 4D F4 20
0x0038	41 C3 A9 21	75 A9 A9 21	B6 AD A9 21	81 AB A9 21	8D AD A9 21	21 AD A9 21
0x003C	1C 00 00 10	1C 00 00 10	1C 00 00 10	1C 00 00 10	1C 00 00 10	1C 00 00 10
0x0040	00 00 87 FF	00 00 11 1F	00 00 00 1F	00 00 00 1F	00 00 00 0D	00 00 00 06
0x0044	C3 C4 3D 76	92 40 7E EB	DD 46 52 F6	45 45 56 D2	97 40 5A CF	3A 41 1E C0

revealed sign patterns. However, this layout yielded neither new sign patterns nor improved precision of the matched contents of an EPO-file.

TABLE X

THE RECORDS FOR NONOPERATIONAL SATELLITE PRN14 AT THE SAME TIMESTAMP WITHIN THE FILES WITH DIFFERENT TIMESTAMPS

Offset	17 Aug 2020	18 Aug 2020	19 Aug 2020	20 Aug 2020	21 Aug 2020	22 Aug 2020	23 Aug 2020	25 Aug 2020
0x0000	50 71 05 00	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x0004	00 00 C8 00	-- -- CC --	-- -- D0 --	-- -- D4 --	-- -- D8 --	-- -- DC --	-- -- E0 --	-- -- E8 --
0x0008	C6 31 0E 07	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x000C	C6 31 0E 07	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x0010	C6 31 0E 07	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x0014	C6 31 0E 07	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x0018	C6 31 0E 07	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x001C	C6 31 8E 38	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- 4E --	-- -- -- --	-- -- -- --
0x0020	C6 31 0E 77	-- -- -- 6B	-- -- -- 6F	-- -- -- 63	-- -- -- 67	-- -- -- 5B	-- -- -- 5F	-- -- -- 57
0x0024	C6 31 0E 07	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x0028	C6 31 0E 07	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x002C	C6 31 0E 07	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x0030	C6 31 0E 07	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x0034	C6 31 0E 07	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x0038	00 00 00 00	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x003C	1C 00 00 90	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x0040	00 00 05 EF	-- -- EF --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --
0x0044	4C 71 48 30	-- -- A6 2C	-- -- BA 28	-- -- BE 24	-- -- B2 20	-- -- 76 1C	-- -- 8A 18	-- -- 82 10

TABLE XI

THE TEMPORAL PATTERN FOR THE SEQUENCE OF BYTES AT THE OFFSETS 0x0006, 0x0023 FOR NONOPERATIONAL SATELLITE PRN14

Offset	
0x0006	.. .. C8 CC D0 D4 D8 DC E0 E8 EC F0 F4 F8 FC .. 04 08 0C 10 14 18 1C 20 24 28 .. 30 34 38
0x0023	.. .. 77 6B 6F 63 67 5B 5F 57 4B 4F 43 47 3B .. 33 37 2B 2F 23 27 1B 1F 13 17 .. 0F 03 07

TABLE XII

THE SIGN PATTERN FOR GPS ORBITAL PARAMETERS AT THE DATE 07 FEB 2021

PRN	t	e	i	$\frac{d\Omega}{dt}$	A	$L\Omega$	ω	m	af_0	af_1
01	503808	+	+	−	+	−	+	−	+	−
02	503808	+	+	−	+	−	−	−	−	−
03	503808	+	+	−	+	−	+	−	−	−
04	503808	+	+	−	+	+	−	+	−	−
05	503808	+	+	−	+	−	+	+	−	0
06	503808	+	+	−	+	−	−	−	−	0
07	503808	+	+	−	+	+	−	−	+	+
08	503808	+	+	−	+	−	−	+	−	0
09	503808	+	+	−	+	+	+	+	−	−
10	503808	+	+	−	+	−	−	+	−	−
11										
12	503808	+	+	−	+	+	+	−	0	−
13	503808	+	+	−	+	+	+	−	+	+
14	503808	+	+	−	+	+	+	−	+	+
15	503808	+	+	−	+	+	+	−	−	+
16	503808	+	+	−	+	+	+	+	−	−
17	503808	+	+	−	+	−	−	+	+	+
18	503808	+	+	−	+	−	+	−	+	+
19	503808	+	+	−	+	−	+	+	−	+
20	503808	+	+	−	+	−	+	−	+	0
21	503808	+	+	−	+	−	−	+	+	+
22	503808	+	+	−	+	−	−	−	−	+
23	503808	+	+	−	+	−	+	−	+	0
24	503808	+	+	−	+	+	+	−	+	0
25	503808	+	+	−	+	+	+	+	+	+
26	503808	+	+	−	+	+	+	+	+	+
27	503808	+	+	−	+	−	+	+	−	−
28	503808	+	+	−	+	+	−	+	+	−
29	503808	+	+	−	+	−	+	+	−	−
30	503808	+	+	−	+	+	−	−	−	−
31	503808	+	+	−	+	+	+	−	−	−
32	503808	+	+	−	+	+	−	+	+	0

TABLE XIII

THE SIGN PATTERN FOR THE EPO-FILE CONTENTS AT THE DATE 10 FEB 2021

PRN	0x04	0x08	0x0C	0x10	0x14	0x18	0x1C	0x20	0x24	0x28	0x2C	0x30	0x34	0x38	0x3C	0x40
01	−	+	−	−	+	−	−	+	+	+	−	−	+	+	+	+
02	−	+	−	−	+	−	−	+	+	+	−	−	+	−	+	+
03	−	+	−	−	+	+	−	+	−	+	−	−	+	+	+	0
04	−	+	+	+	+	+	−	+	+	+	−	+	+	−	+	+
05	−	+	−	−	+	−	−	+	−	+	−	−	+	+	+	+
06	+	+	−	−	+	−	−	+	+	+	−	−	+	−	+	+
07	+	+	−	−	+	+	−	+	−	+	−	+	+	−	+	+
08	−	+	+	+	+	−	−	+	+	+	−	−	+	−	+	+
09	−	+	+	+	+	+	−	+	+	+	−	+	+	+	+	+
10	−	+	−	−	+	+	−	+	−	+	−	−	+	−	+	+
11																
12	−	+	+	+	+	+	−	+	−	+	−	+	+	+	+	+
13	+	+	+	+	+	+	−	+	+	+	−	+	+	+	+	0
14	+	+	+	+	+	+	−	+	+	+	−	+	+	+	+	+
15	+	+	+	+	+	−	−	+	+	+	−	+	+	+	+	+
16	−	+	+	+	+	−	−	+	−	+	−	+	+	+	+	+
17	+	+	+	+	+	+	−	+	+	+	−	−	+	−	+	+
18	+	+	−	−	+	+	−	+	+	+	−	−	+	+	+	+
19	+	+	+	+	+	+	−	+	−	+	−	−	+	+	+	+
20	−	+	−	−	+	+	−	+	−	+	−	−	+	+	+	0
21	+	+	+	+	+	+	−	+	+	+	−	−	+	−	+	+
22	+	+	−	−	+	+	−	+	+	+	−	−	+	−	+	+
23	+	+	−	−	+	−	−	+	+	+	−	−	+	+	+	+
24	−	+	−	−	+	−	−	+	+	+	−	+	+	+	+	+
25	+	+	+	+	+	+	−	+	−	+	−	+	+	+	+	+
26	+	+	+	+	+	−	−	+	−	+	−	+	+	+	+	+
27	−	+	+	+	+	−	−	+	+	+	−	−	+	+	+	+
28	−	+	+	+	+	+	−	+	−	+	−	+	+	−	+	+
29	−	+	+	+	+	−	−	+	+	+	−	−	+	+	+	+
30	−	+	−	−	+	+	−	+	−	+	−	+	+	−	+	+
31	−	+	−	+	+	+	−	+	−	+	−	+	+	+	+	+
32	+	+	+	+	+	−	−	+	−	+	−	+	+	−	+	+

TABLE XIV

THE VALUES PATTERN FOR GPS ORBITAL PARAMETERS AT THE DATE 07 FEB 2021 AND THE CONTENT OF EPO-FILE AT THE DATE 10 FEB 2021

PRN	af_1	0x04	$L\Omega$	0x30	ω	0x38
1	-7.28E-12	-1081589970	-89.43931	-948627797	47.01554	561220456
2	-3.64E-12	-578273726	-94.1208	-1171680626	-88.61856	-1058489288
3	-1.09E-11	-1467466334	-29.91264	-306110181	48.89377	583843908
4	-3.64E-12	-393738555	31.94854	297956208	-172.76076	-2064761077
5	0.00E+00	-142066328	-31.94408	-296508494	50.69094	604860944
6	0.00E+00	143146573	-89.91252	-953464943	-61.84833	-742144835
7	1.46E-11	2022194710	90.56425	1198675376	-134.81145	-1608465929
8	0.00E+00	-192412776	-150.93232	-1817111601	-1.78672	-22547071
9	-3.64E-12	-527956435	29.08474	332168422	104.04894	1240223073
10	-7.28E-12	-1199030987	-30.08039	-306312911	-148.62075	-1774595638
11	--	--	--	--	--	--
12	-3.64E-12	-762823949	154.14758	1790934298	67.53588	804605419
13	3.64E-12	646448855	37.50441	498183837	58.91073	704144680
14	3.64E-12	512244547	152.68696	1806103650	120.72417	1430512865
15	3.64E-12	394790632	23.56765	400156231	55.38438	660424220
16	-7.28E-12	-829932690	155.22401	1769648911	37.28067	443637694
17	7.28E-12	780665777	-146.55459	-1865213091	-90.42096	-1078974466
18	3.64E-12	310918825	-88.67653	-972448648	173.84193	2075727230
19	3.64E-12	747111217	-143.96163	-1631885917	102.01173	1216018300
20	0.00E+00	-24626118	-38.07031	-502513092	163.66897	1951231961
21	3.64E-12	495468374	-94.07822	-1172247605	-68.34889	-817092929
22	7.28E-12	1082670438	-35.40067	-504993835	-59.59019	-711971343
23	0.00E+00	92814681	-31.39403	-288432322	139.78873	1663428561
24	0.00E+00	-91734068	86.17584	978460340	41.84225	498688595
25	7.28E-12	1149778490	150.01323	1842267526	53.85927	641358736
26	7.28E-12	831011397	147.71371	1846606609	15.59765	183559440
27	-7.28E-12	-1098382236	-149.99359	-1838821951	32.85618	391757442
28	-3.64E-12	-779601034	155.42972	1771375189	-77.40778	-923562658
29	-7.28E-12	-1031273504	-145.8529	-1621881273	123.26265	1470756853
30	-7.28E-12	-846709205	91.63759	1177560493	-163.16056	-1946940231
31	-3.64E-12	-326615484	91.51753	1176943662	14.10904	167921235
32	0.00E+00	227018267	29.6335	304781260	-139.78334	-1669072477

V. Results and discussion

At the end of this preliminary study, we partially succeeded in decoding the content of the Mediatek EPO-file. The partial layout is provided in the table XV. The Mediatek EPO-file format differs from the straightforward almanac counterpart of Qualcomm A-GPS format [1]. The respective binary file for Qualcomm gpsOne A-GPS service is provided in the table XVI.

We assume that either the contents of the Mediatek EPO-file are heavily obfuscated or contain some additional data since the record size is more than enough to hold all necessary orbital elements for the satellite almanac. It is also possible, that the data on orbits is stored in the form of interpolation coefficients and, therefore, is unmatchable to the data, provided by the space agencies.

TABLE XV
The block structure for EPO-file

Offset	Type	Content	Range	Comment
0x00	U3	time		
0x03	U1	PRN	0x01	GPS PRN
			...	
			0x20	
0x04	U4	$f\,(af_1)$		Rate of clock correction
0x08	U4	Unmatched		
...	...	...	...	...
0x28	U4	Unmatched		
0x30	I4	$f\,(L\Omega)$		Longitude of ascending node
0x34	U4	Unmatched		
0x38	I4	$f\,(\omega)$		Argument of perigee
0x40	U4	Unmatched		
0x44	U4	CRC		XOR between 32-bit integers with offsets from 0x00 to 0x40

TABLE XVI
Binary content of the Qualcomm gpsOne file (big Endian)

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0x0000	01	1B	08	01	02	15	01	24	05	BB	13	00	00	96	DE	08
0x0010	24	16	01	DF	FD	08	24	15	E3	07	00	06	1C	01	00	25
0x0020	14	07	10	0F	0E	0D	0C	0B	0A	0C	37	08	10	10	0F	0E
0x0030	0D	0C	0A	09	0E	53	08	11	0F	0E	0E	0C	0C	09	08	0D
0x0040	96	02	0B	05	02	03	03	C2	1F	**01**	00	4B	6A	90	17	81
0x0050	FD	62	00	A1	0C	CA	FF	F2	84	DF	00	1E	F2	F4	00	5B
0x0060	E1	04	FF	07	FF	FD	08	24	**02**	00	A0	8E	90	09	D6	FD
0x0070	55	00	A1	0C	6D	FF	EF	8B	58	FF	BB	3F	64	00	67	D6
0x0080	9B	FE	7B	FF	FE	08	24	**03**	00	15	65	90	0E	51	FD	43
0x0090	00	A1	0C	B8	00	1C	EE	72	00	1F	D7	39	00	2C	17	D1
0x00A0	FF	C4	FF	FE	08	24	**04**	FF	03	5D	7B	0B	15	FD	55	00
0x00B0	A1	0D	7A	00	48	E5	9A	FF	93	67	AF	FF	8F	0A	EC	FF
0x00C0	E8	FF	FF	08	24	**05**	00	2F	87	90	05	C9	FD	36	00	A1
0x00D0	0C	0A	00	1B	B8	75	00	20	CB	86	FF	D0	8D	52	FF	FB
0x00E0	00	00	08	24	**06**	00	0D	F9	90	17	40	FD	65	00	A1	0D
0x00F0	6B	FF	F2	2E	BB	FF	CF	03	85	00	6A	75	E5	FF	58	FF
0x0100	FD	08	24	**07**	00	6C	2A	90	07	B9	FD	50	00	A1	0D	52
0x0110	00	72	C3	B3	FF	9D	60	35	00	3F	3A	B1	FF	49	FF	FE
0x0120	08	24	**08**	00	28	08	90	11	E2	FD	45	00	A1	0C	70	FF
0x0130	C6	FB	81	FF	F6	DF	3E	FF	BD	BB	1A	FF	EE	00	00	08
0x0140	24	**09**	00	0E	03	90	06	4A	FD	4A	00	A1	0B	DF	00	46
0x0150	F7	7C	00	44	A6	6A	FF	C9	94	0C	FF	89	FF	FD	08	24

TABLE XVII
The block structure for GPS almanac (address 0x0049+0x001E*(PRN-1) of the Qualcomm gpsOne binary file, big Endian)

Offset	Type	Content	Value	Comment
0x00	U1	PRN	0x01	
			...	
			0x20	
0x01	U1	Unmatched	0x00	Health ???
0x02	U2	e – Eccentricity	$\tilde{e}$	e =
0x03				$\tilde{e} \cdot 4.77\text{E}{-7}$
0x04	U1	Unmatched		
0x05	I2	i – Orbital,	$\tilde{i}$	i =
0x06		inclination, (deg)		$180{\cdot}(0.3 + \tilde{i} \cdot 1.91{\cdot}\text{E}{-6})$
0x07	I2	$d\Omega/dt$ – Rate of	$\tilde{\Omega}$	$d\Omega/dt$ =
0x08		right ascension W, (deg/s)		$180 \cdot \tilde{\Omega} \cdot 3.64\text{E}{-12}$
0x09	U4	A – Semi-major	$\tilde{A}$	A =
0x0A		axis, (km)		$(\tilde{A} \cdot 4.88\text{E}{-04})^2$
0x0B				
0x0C				
0x0D	I4	$L\Omega$ – Longitude of	$\tilde{L\Omega}$	$L\Omega$ =
0x0E		ascending node		$180 \cdot \tilde{L\Omega} \cdot 1.19\text{E}{-7}$
0x0F		on 00h.00min.00sec		
0x10		base date, (deg)		
0x11	I4	ω – Argument of	$\tilde{\omega}$	ω =
0x12		perigee, (deg)		$180 \cdot \tilde{\omega} \cdot 1.19\text{E}{-7}$
0x13				
0x14				
0x15	I4	m – Mean	$\tilde{m}$	m =
0x16		anomaly, (deg)		$180 \cdot \tilde{m} \cdot 1.19\text{E}{-7}$
0x17				
0x18				
0x19	I2	$af0$ – Clock	$\tilde{af}0$	$af0$ =
0x1A		correction, (sec)		$\tilde{af}0 \cdot 9.54\text{E}{-7}$
0x1B	I2	$af1$ – Rate of	$\tilde{af}1$	$af1$ =
0x1C		clock correction, (sec/sec)		$\tilde{af}1 \cdot 3.64\text{E}{-12}$
1x1D	U2	Reference time		Full GPS week 1-st epoch
0x1E		without rollover		for 2 days ahead

VI. Conclusion

In the presented study we considered the proprietary layout of a Mediatek binary EPO-file for the A-GPS web service. Employing differential cryptanalysis in the form of quasi-known-plaintext attack, we deduced the partial structures of the record, containing some functions of orbital elements for each operational satellite. The comparison of the deciphered orbital elements (longitude of ascending node and argument of perigee) with reference counterparts showed a good correlation.

References

[1] V. Vinnikov and E. Pshehotskaya, "Deciphering of the gpsOne file format for assisted GPS service.". *Proc. Fifth International Congress on Information and Communication Technology. Advances in Intelligent Systems and Computing*, vol 1184, 2021. https://doi.org/10.1007/978-981-15-5859-7_37

[2] Qualcomm Press Release, Qualcomm Introduces gpsOneXTRA Assistance to Expand Capabilities of Standalone GPS, Feb 12, 2007 San Diego, Web: https://www.qualcomm.com/news/releases/2007/02/12/qualcomm-introduces-gpsonextra-assistance-expand-capabilities-standalone

[3] Nightwatch Cybersecurity, Advisory: Insecure Transmission of Qualcomm Assisted-GPS Data [CVE-2016-5341], Web: https://wwws.nightwatchcybersecurity.com/2016/12/05/cve-2016-5341/

[4] Nightwatch Cybersecurity, Advisory: Crashing Android devices with large Assisted-GPS Data Files [CVE-2016-5348], Web: https://wwws.nightwatchcybersecurity.com/2016/10/04/advisory-cve-2016-5348-2/

[5] DC RAINMAKER: New 2021 GPS Accuracy Issue Impacting Some Garmin, Suunto, other GPS Devices, JANUARY 2, 2021, Web: https://www.dcrainmaker.com/2021/01/gps-accuracy-impacting-devices.html

[6] W. Zhang, *New GNSS navigation messages for Inherent fast TTFF and high sensitivity-underlying theory study and system analysis. PhD thesis on geomatics engineering*. Calgary, Alberta, 2018, Web: https://prism.ucalgary.ca/bitstream/handle/1880/106628/ucalgary_2018_zhang_wentao.pdf?sequence=1\&isAllowed=y

[7] Qualcomm Developer Network forums (2019) Software. Qualcomm LTE for IoT. SDKgpsOneXTRA not working, Web: https://developer.qualcomm.com/comment/17055

[8] GPS Date Calendar, Web: http://navigationservices.agi.com/GNSSWeb/

[9] Information and Analysis Center for Positioning, Navigation and Timing, Korolyov, Russia, Web: https://www.glonass-iac.ru/en/GPS/ephemeris.php

[10] Official U.S. government information about the Global Positioning System (GPS) and related topics, Interface Control Document ICD-GPS-240, Web: https://www.gps.gov/technical/icwg/ICD-GPS-870A.pdf

[11] Global Positioning Systems Directorate, System Engineering & Integration, Interface Specification IS-GPS-200, Navstar GPS Space Segment/Navigation User Interfaces, Web: https://www.gps.gov/technical/icwg/IS-GPS-200G.pdf