Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3096587 A1 2019/11/07

(21) 3 096 587

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2018/05/04
(87) Date publication PCT/PCT Publication Date: 2019/11/07
(85) Entrée phase nationale/National Entry: 2020/10/08
(86) N° demande PCT/PCT Application No.: US 2018/031222
(87) N° publication PCT/PCT Publication No.: 2019/212573

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01), *G06F 21/60* (2013.01), *H04B 7/06* (2006.01), *H04B 7/185* (2006.01), *H04N 21/61* (2011.01), *H04W 12/00* (2009.01), *H04W 84/06* (2009.01)

(71) Demandeur/Applicant:
THE BOEING COMPANY, US

(72) Inventeurs/Inventors:
CHEN, YI-FENG JAMES, US;
KRIKORIAN, HAIG F., US;
WINIG, ROBERT J., US

(74) Agent: SMART & BIGGAR LLP

(54) Titre : OPERATIONS DE CHARGE UTILE MULTI-OPERATEURS PROTEGEES
(54) Title: PROTECTED MULTI-OPERATORS PAYLOAD OPERATIONS

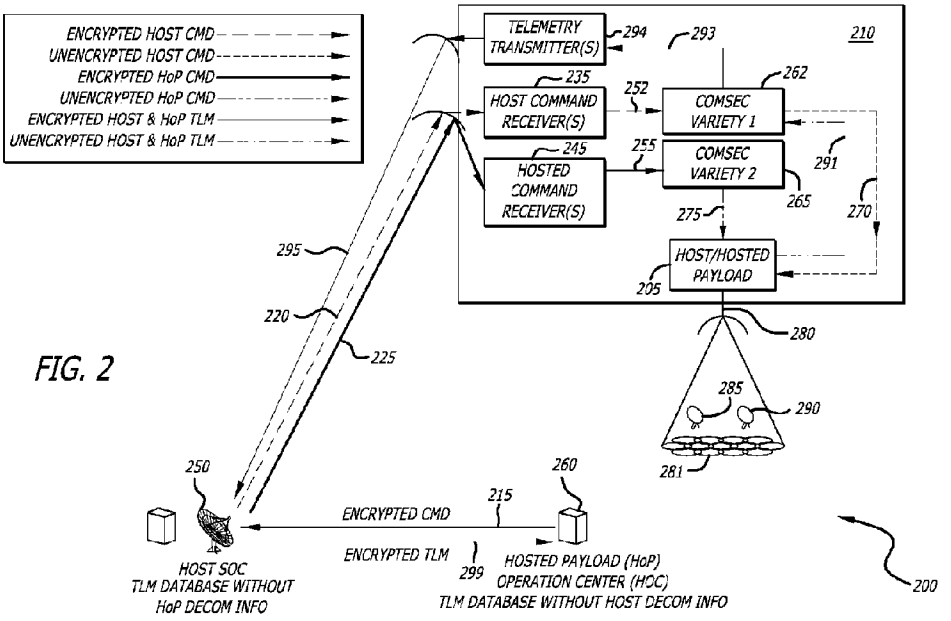


FIG. 2

(57) Abrégé/Abstract:
Systems, methods, and apparatus for protected multi-operators payload operations are disclosed. In one or more embodiments, a disclosed method for protected multi-operators payload operations comprises transmitting, by a hosted payload (HoP) operation center (HOC), encrypted hosted commands to a host spacecraft operations center (SOC). Also, the method comprises transmitting, by the host SOC, encrypted host commands and the encrypted hosted commands to a vehicle. In addition, the method comprises reconfiguring a payload on the vehicle according to unencrypted host commands and unencrypted hosted commands. Additionally, the method comprises transmitting, by a payload antenna on the vehicle, payload data to a host receiving antenna and a hosted receiving antenna. Also, the method comprises transmitting, by a telemetry transmitter on the vehicle, encrypted host telemetry and encrypted hosted telemetry to the host SOC. Further, the method comprises transmitting, by the host SOC, the encrypted hosted telemetry to the HOC.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
07 November 2019 (07.11.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/212573 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 84/06* (2009.01)
G06F 21/60 (2013.01) *H04B 7/06* (2006.01)
H04B 7/185 (2006.01) *H04W 12/00* (2009.01)
H04N 21/61 (2011.01)

(21) International Application Number:
PCT/US2018/031222

(22) International Filing Date:
04 May 2018 (04.05.2018)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **THE BOEING COMPANY** [US/US]; 100 North Riverside Plaza, Chicago, Illinois 60606-1596 (US).

(72) Inventors: **CHEN, Yi-Feng James**; 100 North Riverside Plaza, Chicago, Illinois 60606-1596 (US). **KRIKORIAN, Haig F.**; 100 North Riverside Plaza, Chicago, Illinois 60606-1596 (US). **WINIG, Robert J.**; 100 North Riverside Plaza, Chicago, Illinois 60606-1596 (US).

(74) Agent: **DIXON, Cynthia A.**; Suite 700, 2323 Victory Avenue, Dallas, Texas 75219 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) Title: PROTECTED MULTI-OPERATORS PAYLOAD OPERATIONS

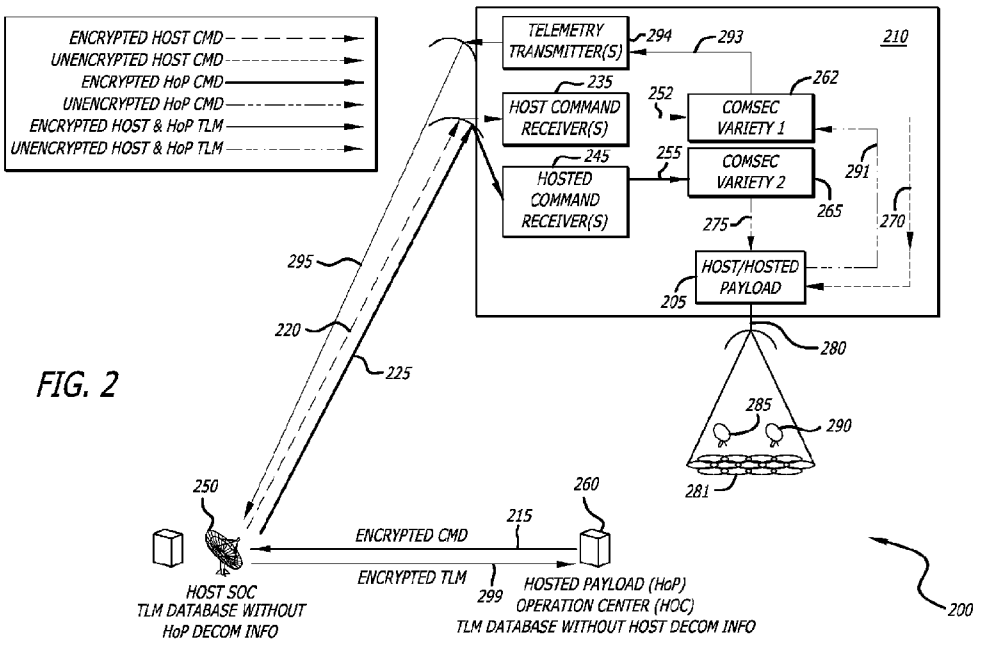


FIG. 2

(57) **Abstract:** Systems, methods, and apparatus for protected multi-operators payload operations are disclosed. In one or more embodiments, a disclosed method for protected multi-operators payload operations comprises transmitting, by a hosted payload (HoP) operation center (HOC), encrypted hosted commands to a host spacecraft operations center (SOC). Also, the method comprises transmitting, by the host SOC, encrypted host commands and the encrypted hosted commands to a vehicle. In addition, the method comprises reconfiguring a payload on the vehicle according to unencrypted host commands and unencrypted hosted commands. Additionally, the method comprises transmitting, by a payload antenna on the vehicle, payload data to a host receiving antenna and a hosted receiving antenna. Also, the method comprises transmitting, by a telemetry transmitter on the vehicle, encrypted host telemetry and encrypted hosted telemetry to the host SOC. Further, the method comprises transmitting, by the host SOC, the encrypted hosted telemetry to the HOC.

WO 2019/212573 A1

[Continued on next page]

WO 2019/212573 A1

SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

PROTECTED MULTI-OPERATORS PAYLOAD OPERATIONS

FIELD

[0001] The present disclosure relates to payload operations. In particular, it relates to protected multi-operators payload operations.

BACKGROUND

[0002] Currently, typical transponders on a vehicle (e.g., a satellite) have the ability to perform switching of inputs to outputs of the payload. All of this switching on the payload is commanded and controlled by a single satellite controller with no resource allocation privacy. For example, in a digital transponder, when a user request for a channel with specific bandwidth and antenna characteristics is made, the channel is then set up, used, and then disconnected.

[0003] As such, there is a need for an improved transponder design that allows for privacy in the allocation of resources on the payload.

SUMMARY

[0004] The present disclosure relates to a method, system, and apparatus for protected multi-operators payload operations. In one or more embodiments, a method for protected multi-operators payload operations comprises transmitting, by a hosted payload (HoP) operation center (HOC), encrypted hosted commands to a host spacecraft operations center (SOC). Also, the method comprises transmitting, by the host SOC, encrypted host commands and the encrypted hosted commands to a vehicle. In one or more embodiments, the encrypted host commands are encrypted utilizing a first communication security (COMSEC) variety and the encrypted hosted commands are encrypted utilizing a second COMSEC variety. In addition, the method comprises decrypting, by a first communication security module on the vehicle, the encrypted host commands utilizing the first COMSEC variety to generate unencrypted host commands. Additionally, decrypting, by a second communication security module on the vehicle, the encrypted hosted commands utilizing the second COMSEC variety to generate unencrypted hosted commands. Also, the method comprises reconfiguring a payload on the vehicle according to the unencrypted host commands and the unencrypted hosted commands. In addition, transmitting, by a payload antenna on the vehicle, payload data to a host receiving antenna and a hosted receiving antenna. Additionally, encrypting, by the first communication security module, unencrypted host telemetry and the unencrypted hosted telemetry from the payload by utilizing the first COMSEC variety to generate encrypted host telemetry and encrypted hosted telemetry. Also, the method comprises transmitting, by a telemetry transmitter on the vehicle, the encrypted host telemetry and the encrypted hosted telemetry to the host SOC. Further, the method comprises transmitting, by the host SOC, the encrypted hosted telemetry to the HOC.

[0005] In at least one embodiment, the reconfiguring of the payload according to the unencrypted host commands and the unencrypted hosted commands comprises adjusting transponder power, transponder spectrum monitoring, transponder connectivity, transponder gain settings, transponder limiter settings, transponder automatic level control settings, transponder phase settings, internal gain generation, bandwidth for at least one beam, at least one frequency band for at least one beam, transponder beamforming settings, effective isotropic radiation power (EIRP) for at least one beam, transponder channels, and/or beam steering.

[0006] In one or more embodiments, the reconfiguring of the payload according to the unencrypted host commands and the unencrypted hosted commands comprises reconfiguring at least one antenna, at least one analog-to-digital converter, at least one digital-to-analog converter, at least one beamformer, at least one digital channelizer, at least one demodulator, at least one modulator, at least one digital switch matrix, and/or at least one digital combiner.

[0007] In at least one embodiment, the vehicle is an airborne vehicle. In one or more embodiments, the airborne vehicle is a satellite, aircraft, unmanned aerial vehicle (UAV), or space plane.

[0008] In one or more embodiments, the method further comprises encrypting, by the HOC, the unencrypted hosted commands by utilizing the second COMSEC variety to produce the encrypted hosted commands. Further, the method comprises encrypting, by the host SOC, the unencrypted host commands by utilizing the first COMSEC variety to produce the encrypted host commands.

[0009] In at least one embodiment, the method further comprises receiving, by a host command receiver on the vehicle, the encrypted host commands. Also, the method comprises receiving, by a hosted command receiver on the vehicle, the encrypted hosted commands. In addition, the method comprises transmitting, by the host command receiver, the encrypted host commands to the first communication security module. Further, the method comprises transmitting, by the hosted command receiver, the encrypted hosted commands to the second communication security module.

[0010] In one or more embodiments, the method further comprises transmitting, by the first communication security module, the unencrypted host commands to the payload. Also, the method comprises transmitting, by the second communication security module, the unencrypted hosted commands to the payload.

[0011] In at least one embodiment, the method further comprises transmitting, by the payload, to the first communication security module the unencrypted host telemetry and the unencrypted hosted telemetry.

[0012] In one or more embodiments, the method further comprises transmitting, by the first communication security module, the encrypted host telemetry and the encrypted hosted telemetry to the telemetry transmitter.

[0013] In at least one embodiment, the method further comprises decrypting, by the host SOC, the encrypted host telemetry utilizing the first COMSEC variety and utilizing a database without hosted decommutated information to generate the unencrypted host telemetry. Also, the method comprises decrypting, by the HOC, the encrypted hosted telemetry utilizing the first COMSEC variety and utilizing a database without host decommutated information to generate the unencrypted hosted telemetry.

[0014] In one or more embodiments, a method for protected multi-operators payload operations comprises transmitting, by the HOC, the encrypted hosted commands to a host spacecraft operations center (SOC). The method further comprises transmitting, by the host SOC, the encrypted host commands and the encrypted hosted commands to a vehicle. Also, the method comprises decrypting, by the first communication security module, the encrypted host commands utilizing the first COMSEC variety to generate the unencrypted host commands. In addition, the method comprises decrypting, by the second communication security module, the encrypted hosted commands utilizing the second COMSEC variety to generate the unencrypted hosted commands. Additionally, the method comprises reconfiguring the payload according to the unencrypted host commands and the unencrypted hosted commands. Also, the method comprises transmitting, by a payload antenna on the vehicle, payload data to a host receiving antenna and a hosted receiving antenna. In addition, the method comprises encrypting, by the first communication security module, the unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry. Additionally, the method comprises transmitting, by the host telemetry transmitter, the encrypted host telemetry to the host SOC. Also, the method comprises encrypting, by the second communication security module, the unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry. In addition, the method comprises transmitting, by the hosted telemetry transmitter, the encrypted hosted telemetry to the host SOC. Further, the method comprises transmitting, by the host SOC, the encrypted hosted telemetry to the HOC.

[0015] In at least one embodiment, a method for protected multi-operators payload operations comprises transmitting, by a hosted payload (HoP) operation center (HOC), encrypted hosted commands to a vehicle. The method further comprises transmitting, by the host SOC, encrypted host commands to the vehicle. Also, the method comprises decrypting, by a first communication security module on the vehicle, the encrypted host commands utilizing a first COMSEC variety to generate unencrypted host commands. In addition, the method comprises decrypting, by a

second communication security module on the vehicle, the encrypted hosted commands utilizing a second COMSEC variety to generate unencrypted hosted commands. Additionally, the method comprises reconfiguring the payload according to the unencrypted host commands and the unencrypted hosted commands. Also, the method comprises transmitting, by a payload antenna on the vehicle, payload data to a host receiving antenna and a hosted receiving antenna. In addition, the method comprises encrypting, by the first communication security module, unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry. Additionally, the method comprises transmitting, by a host telemetry transmitter on the vehicle, the encrypted host telemetry to the host SOC. Also, the method comprises encrypting, by the second communication security module, unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry. Further, the method comprises transmitting, by the hosted telemetry transmitter, the encrypted hosted telemetry to the HOC.

[0016] In one or more embodiments, a system for protected multi-operators payload operations comprises a hosted payload (HoP) operation center (HOC) to transmit encrypted hosted commands to a host spacecraft operations center (SOC). The system further comprises the host SOC to transmit encrypted host commands and the encrypted hosted commands to a vehicle. In one or more embodiments, the encrypted host commands are encrypted utilizing a first communication security (COMSEC) variety and the encrypted hosted commands are encrypted utilizing a second COMSEC variety. Also, the system comprises a first communication security module on the vehicle to decrypt the encrypted host commands utilizing the first COMSEC variety to generate unencrypted host commands. In addition, the system comprises a second communication security module on the vehicle to decrypt the encrypted hosted commands utilizing the second COMSEC variety to generate unencrypted hosted commands. Additionally, the system comprises a payload on the vehicle reconfigured according to the unencrypted host commands and the unencrypted hosted commands. Also, the system comprises a payload antenna on the vehicle to transmit payload data to a host receiving antenna and a hosted receiving antenna. In addition, the system comprises the first communication security module to encrypt unencrypted host telemetry and unencrypted hosted telemetry from the payload by utilizing the first COMSEC variety to generate encrypted host telemetry and encrypted hosted telemetry. Additionally, the system comprises a telemetry transmitter on the vehicle to transmit the encrypted host telemetry and the encrypted hosted telemetry to the host SOC. Further, the system comprises the host SOC to transmit the encrypted hosted telemetry to the HOC.

[0017] In at least one embodiment, a system for protected multi-operators payload operations comprises a hosted payload (HoP) operation center (HOC) to transmit encrypted hosted

commands to a host spacecraft operations center (SOC). The system further comprises the host SOC to transmit encrypted host commands and the encrypted hosted commands to a vehicle. In one or more embodiments, the encrypted host commands are encrypted utilizing a first COMSEC variety and the encrypted hosted commands are encrypted utilizing a second COMSEC variety. Also, the system comprises a first communication security module to decrypt the encrypted host commands utilizing the first COMSEC variety to generate unencrypted host commands. In addition, the system comprises a second communication security module to decrypt the encrypted hosted commands utilizing the second COMSEC variety to generate the unencrypted hosted commands. Additionally, the system comprises a payload reconfigured according to the unencrypted host commands and the unencrypted hosted commands. Also, the system comprises a payload antenna on the vehicle to transmit payload data to a host receiving antenna and a hosted receiving antenna. In addition, the system comprises the first communication security module to encrypt unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry. Also, the system comprises a host telemetry transmitter to transmit the encrypted host telemetry to the host SOC. In addition, the system comprises the second communication security module to encrypt unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry. Also, the system comprises a hosted telemetry transmitter to transmit the encrypted hosted telemetry to the host SOC. Further, the system comprises the host SOC to transmit the encrypted hosted telemetry to the HOC.

[0018] In one or more embodiments, a system for protected multi-operators payload operations comprises a hosted payload (HoP) operation center (HOC) to transmit encrypted hosted commands to a vehicle. The system further comprises a host spacecraft operations center (SOC) to transmit encrypted host commands to the vehicle. In one or more embodiments, the encrypted host commands are encrypted utilizing a first communication security (COMSEC) variety and the encrypted hosted commands are encrypted utilizing a second COMSEC variety. Also, the system comprises a first communication security module on the vehicle to decrypt the encrypted host commands utilizing the first COMSEC variety to generate unencrypted host commands. In addition, the system comprises a second communication security module on the vehicle to decrypt the encrypted hosted commands utilizing the second COMSEC variety to generate unencrypted hosted commands. Also, the system comprises a payload reconfigured according to the unencrypted host commands and the unencrypted hosted commands. In addition, the system comprises a payload antenna on the vehicle to transmit payload data to a host receiving antenna and a hosted receiving antenna. Additionally, the system comprises the first communication security module to encrypt unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry. Also, the system comprises a host

telemetry transmitter on the vehicle to transmit the encrypted host telemetry to the host SOC. In addition, the system comprises the second communication security module to encrypt unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry. Further, the system comprises a hosted telemetry transmitter to transmit the encrypted hosted telemetry to the HOC.

[0019] The features, functions, and advantages can be achieved independently in various embodiments of the present disclosure or may be combined in yet other embodiments.

DRAWINGS

[0020] These and other features, aspects, and advantages of the present disclosure will become better understood with regard to the following description, appended claims, and accompanying drawings where:

[0021] FIG. 1 is a diagram showing simplified architecture for the disclosed system for protected multi-operators payload operations, in accordance with at least one embodiment of the present disclosure.

[0022] FIG. 2 is a diagram showing the disclosed system for protected multi-operators payload operations where the host user transmits encrypted host commands (encrypted utilizing a first COMSEC variety) and encrypted hosted commands (encrypted utilizing the second COMSEC variety) to a vehicle, and where the host telemetry and the hosted telemetry are both encrypted using the first COMSEC variety, in accordance with at least one embodiment of the present disclosure.

[0023] FIGS. 3A, 3B, and 3C together show a flow chart for the disclosed method for protected multi-operators payload operations where the host user transmits encrypted host commands (encrypted utilizing a first COMSEC variety) and encrypted hosted commands (encrypted utilizing the second COMSEC variety) to a vehicle, and where the host telemetry and the hosted telemetry are both encrypted using the first COMSEC variety, in accordance with at least one embodiment of the present disclosure.

[0024] FIG. 4 is a diagram showing the disclosed system for protected multi-operators payload operations where the host user transmits encrypted host commands (encrypted utilizing a first COMSEC variety) and encrypted hosted commands (encrypted utilizing a second COMSEC variety) to a vehicle, and where the host telemetry is encrypted using the first COMSEC variety and the hosted telemetry is encrypted using the second COMSEC variety, in accordance with at least one embodiment of the present disclosure.

[0025] FIGS. 5A, 5B, 5C, and 5D together show a flow chart for the disclosed method for protected multi-operators payload operations where the host user transmits encrypted host commands (encrypted utilizing a first COMSEC variety) and encrypted hosted commands

(encrypted utilizing a second COMSEC variety) to a vehicle, and where the host telemetry is encrypted using the first COMSEC variety and the hosted telemetry is encrypted using the second COMSEC variety, in accordance with at least one embodiment of the present disclosure.

[0026] FIG. 6 is a diagram showing the disclosed system for protected multi-operators payload operations where the host user transmits encrypted host commands (encrypted utilizing a first COMSEC variety) to a vehicle and the hosted user transmits encrypted hosted commands (encrypted utilizing a second COMSEC variety) to the vehicle, and where the host telemetry is encrypted using the first COMSEC variety and the hosted telemetry is encrypted using the second COMSEC variety, in accordance with at least one embodiment of the present disclosure.

[0027] FIGS. 7A, 7B, and 7C together show a flow chart for the disclosed method for protected multi-operators payload operations where the host user transmits encrypted host commands (encrypted utilizing a first COMSEC variety) to a vehicle and the hosted user transmits encrypted hosted commands (encrypted utilizing a second COMSEC variety) to the vehicle, and where the host telemetry is encrypted using the first COMSEC variety and the hosted telemetry is encrypted using the second COMSEC variety, in accordance with at least one embodiment of the present disclosure.

[0028] FIG. 8 is a diagram showing components of an exemplary virtual transponder that may be employed by the disclosed system for protected multi-operators payload operations, in accordance with at least one embodiment of the present disclosure.

DESCRIPTION

[0029] The methods and apparatus disclosed herein provide an operative system for protected multi-operators payload operations. The system of the present disclosure allows for vehicle operators to privately share vehicle resources.

[0030] As previously mentioned above, currently, typical transponders on a vehicle (e.g., a satellite) have the ability to perform switching of inputs to outputs of the payload. All of this switching on the payload is commanded and controlled by a single satellite controller with no resource allocation privacy. For example, in a digital transponder, when a user request for a channel with specific bandwidth and antenna characteristics is made, the channel is then set up, used, and then disconnected.

[0031] The disclosed system allows for private vehicle resource allocation and control that provides vehicle users the ability to privately, dynamically, allocate resources on demand. In particular, the disclosed system employs a virtual transponder, which is a transponder partitioned into multiple transponders with independent command and control. In one or more embodiments, an exemplary virtual transponder includes a digital transponder with a digital channelizer, a digital switch matrix, and a digital combiner that is configured to partition a digital transponder

into multiple transponders with independent command and control. Command and control of the virtual transponder is achieved via ground software that provides dynamic allocation and privatization of the digital switch matrix for bandwidth on demand.

[0032] It should be noted that the disclosed system for private vehicle resource allocation and control may employ various different types of transponders for the virtual transponder other than the specific disclosed embodiments (e.g., depicted FIG. 8) for the virtual transponder. For example, various different types of transponders may be employed for the virtual transponder including, but not limited to, various different types of digital transponders, various different types of analog transponders (e.g., conventional repeater-type transponders), and various different types of combination analog/digital transponders.

[0033] In the following description, numerous details are set forth in order to provide a more thorough description of the system. It will be apparent, however, to one skilled in the art, that the disclosed system may be practiced without these specific details. In the other instances, well known features have not been described in detail so as not to unnecessarily obscure the system.

[0034] Embodiments of the present disclosure may be described herein in terms of functional and/or logical components and various processing steps. It should be appreciated that such components may be realized by any number of hardware, software, and/or firmware components configured to perform the specified functions. For example, an embodiment of the present disclosure may employ various integrated circuit components (e.g., memory elements, digital signal processing elements, logic elements, look-up tables, or the like), which may carry out a variety of functions under the control of one or more processors, microprocessors, or other control devices. In addition, those skilled in the art will appreciate that embodiments of the present disclosure may be practiced in conjunction with other components, and that the system described herein is merely one example embodiment of the present disclosure.

[0035] For the sake of brevity, conventional techniques and components related to satellite communication systems, and other functional aspects of the system (and the individual operating components of the systems) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent example functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in an embodiment of the present disclosure.

[0036] FIG. 1 is a diagram 100 showing simplified architecture for the disclosed system for protected multi-operators payload operations, in accordance with at least one embodiment of the present disclosure. In this figure, a simplified view of multiple possible hosted payload configurations is illustrated. In particular, this figure shows a space segment 110 and a ground

segment 120. The space segment 110 represents a vehicle. Various different types of vehicles may be employed for the vehicle including, but not limited to, an airborne vehicle. And, various different types of airborne vehicles may be employed for the vehicle including, but not limited to, a satellite, an aircraft, an unmanned aerial vehicle (UAV), and a space plane.

[0037] In the case of a satellite being employed for the vehicle, it should be noted that satellites typically include computer-controlled systems. A satellite generally includes a bus 130 and a payload 140. The bus 130 may include systems (which include components) that control the satellite. These systems perform tasks, such as power generation and control, thermal control, telemetry, attitude control, orbit control, and other suitable operations.

[0038] The payload 140 of the satellite provides functions to users of the satellite. The payload 140 may include antennas, transponders, and other suitable devices. For example, with respect to communications, the payload 140 in a satellite may be used to provide Internet access, telephone communications, radio, television, and other types of communications.

[0039] The payload 140 of the satellite may be used by different entities. For example, the payload 140 may be used by the owner of the satellite (i.e. the host user), one or more customers (i.e. the hosted user(s)), or some combination thereof.

[0040] For example, the owner of a satellite may lease different portions of the payload 140 to different customers. In one example, one group of antenna beams generated by the payload 140 of the satellite may be leased to one customer, while a second group of antenna beams may be leased to a second customer. In another example, one group of antenna beams generated by the payload 140 of the satellite may be utilized by the owner of the satellite, while a second group of antenna beams may be leased to a customer. In yet another example, some or all of the antenna beams generated by the payload 140 of the satellite may be shared by one customer and a second customer. In another example, some or all of the antenna beams generated by the payload 140 of the satellite may be shared by the owner of the satellite and a customer. When satellites are shared by different users, users may have a shared communications link (e.g., Interface A) to the satellite, or each user may have a separate communications link (e.g., Interfaces A and D) to the satellite.

[0041] Leasing a satellite to multiple customers may increase the revenues that an owner of a satellite can obtain. Further, a customer may use a subset of the total resources in a satellite for a cost that is less than the cost for the customer to purchase and operate a satellite, to build and operate a satellite, or to lease an entire satellite.

[0042] Referring back to FIG. 1, the ground segment 120 comprises a host spacecraft operations center (SOC) (e.g., a ground station associated with the owner of the satellite) 150, and a hosted payload (HoP) operation center(s) (HOC(s)) (e.g., a ground station(s) associated

with a customer(s) that is leasing at least a portion of the payload of the satellite from the owner) 160.

[0043] FIG. 1 shows a number of different possible communication links (i.e. Interfaces A – E). It should be noted that the disclosed system may employ some or all of these illustrated communication links. Interface A, which may comprise multiple links, is an out-of-band command and telemetry link from the host SOC 150 to command the satellite. Interface B, which may comprise multiple links, is a communication link, between the bus 130 and the payload 140. Interface B may be used to control essential items, such as power. Information that may be communicated from the bus 130 to the payload 140 via Interface B may include, but is not limited to, time, ephemeris, and payload commands. Information that may be communicated from the payload 140 to the bus 130 via Interface B may include, but is not limited to, payload telemetry.

[0044] Interface C, which may comprise multiple links, is an inband command and telemetry link for bus and/or payload. Interface D, which may comprise multiple links, is a command and telemetry link from the HOC(s) 160 to command the satellite. Interface E, which may comprise multiple links, between the host SOC 150 and the HOCs 160 allows for requests from the HOCs for resource sharing of the payload 140.

[0045] FIGS. 2 – 7C show exemplary systems and methods for protected multi-operators payload operations, in accordance with at least one embodiment of the present disclosure.

[0046] FIG. 2 is a diagram 200 showing the disclosed system for protected multi-operators payload operations where the host user (i.e. the host SOC) 250 transmits encrypted host commands (encrypted utilizing a first COMSEC variety) and encrypted hosted commands (encrypted utilizing the second COMSEC variety) to a vehicle, and where the host telemetry and the hosted telemetry are both encrypted using the first COMSEC variety, in accordance with at least one embodiment of the present disclosure. In this figure, a vehicle 210, a host SOC 250, and a HOC 260 are shown. The HOC 260 has leased at least a portion (e.g., a virtual transponder(s)) of the payload 205 of the vehicle 210 from the owner of a satellite (i.e. the host SOC) 250. It should be noted that in some embodiments, the HOC 260 may lease all of the payload 205 of the vehicle 210 from the owner of a satellite (i.e. the host SOC) 250. Also, it should be noted that is some embodiments, the HOC 260 may own the payload 205 (e.g., a steerable antenna) of the vehicle 210, and contract the host SOC 250 to transmit encrypted hosted commands to the vehicle 210.

[0047] During operation, the HOC 260 encrypts unencrypted hosted commands (i.e. unencrypted HoP CMD), by utilizing a second COMSEC variety, to produce encrypted hosted commands (i.e. encrypted HoP CMD). The hosted commands are commands that are used to

configure the portion (e.g., a virtual transponder(s)) of the payload 205 that the HOC 260 is leasing from the host SOC 250. The host SOC 250 encrypts unencrypted host commands (i.e. unencrypted host CMD), by utilizing a first COMSEC variety, to produce encrypted host commands (i.e. encrypted host CMD). The host commands are commands that are used to configure the portion (e.g., a transponder(s)) of the payload 205 that host SOC 250 is utilizing for itself.

[0048] It should be noted that, although in FIG. 2 the host SOC 250 is depicted to have its ground antenna located right next to its operations building; in other embodiments, the host SOC 250 may have its ground antenna located very far away from the its operations building (e.g., the ground antenna may be located in another country than the operations building).

[0049] Also, it should be noted that the first COMSEC variety may include at least one encryption key and/or at least one algorithm (e.g., a Type 1 encryption algorithm or a Type 2 encryption algorithm). Additionally, it should be noted that the second COMSEC variety may include at least one encryption key and/or at least one encryption algorithm (e.g., a Type 1 encryption algorithm or a Type 2 encryption algorithm).

[0050] The HOC 260 then transmits 215 the encrypted hosted commands to the host SOC 250. After the host SOC 250 receives the encrypted hosted commands, the host SOC 250 transmits 220 the encrypted host commands and transmits 225 the encrypted hosted commands to the vehicle 210. The host SOC 250 transmits 220, 225 the encrypted host commands and the encrypted hosted commands utilizing an out-of-band frequency band(s) (i.e. a frequency band(s) that is not the same frequency band(s) utilized to transmit payload data). The host command receiver 235 on the vehicle 210 receives the encrypted host commands. In addition, the hosted command receiver 245 on the vehicle 210 receives the encrypted hosted commands.

[0051] The host command receiver 235 then transmits 252 the encrypted host commands to a first communication security module 262. The first communication security module 262 decrypts the encrypted host commands utilizing the first COMSEC variety (i.e. COMSEC Variety 1) to generate unencrypted host commands.

[0052] It should be noted that the first communication security module 262 may comprise one or more modules. In addition, the first communication security module 262 may comprise one or more processors.

[0053] The hosted command receiver 245 then transmits 255 the encrypted hosted commands to a second communication security module 265. The second communication security module 265 decrypts the encrypted hosted commands utilizing the second COMSEC variety (i.e. COMSEC Variety 2) to generate unencrypted hosted commands.

[0054] It should be noted that the second communication security module 265 may comprise one or more modules. In addition, the second communication security module 265 may comprise one or more processors.

[0055] The first communication security module 262 then transmits 270 the unencrypted host commands to the payload (i.e. the shared host/hosted payload) 205. The second communication security module 265 transmits 275 the unencrypted hosted commands to the payload (i.e. the shared host/hosted payload) 205. The payload 205 is reconfigured according to the unencrypted host commands and the unencrypted hosted commands. A payload antenna 280 then transmits (e.g., in one or more antenna beams 281) payload data to a host receiving antenna 285 and a hosted receiving antenna 290 on the ground.

[0056] Also, it should be noted that, although in FIG. 2, antenna beams 281 is shown to include a plurality of circular spot beams; in other embodiments, antenna beams 281 may include more or less number of beams than is shown in FIG. 2 (e.g., antenna beams 281 may only include a single beam), and antenna beams 281 may include beams of different shapes than circular spot beams as is shown in FIG. 2 (e.g., antenna beams 281 may include elliptical beams and/or shaped beams of various different shapes).

[0057] It should be noted that in one or more embodiments, the payload antenna 280 may comprise one or more reflector dishes including, but not limited to, parabolic reflectors and/or shaped reflectors. In some embodiments, the payload antenna 280 may comprise one or more multifeed antenna arrays.

[0058] The payload 205 transmits 291 unencrypted host telemetry (i.e. unencrypted host TLM, which is telemetry data related to the portion of the payload 205 that is utilized by the host SOC 250) and unencrypted hosted telemetry (i.e. unencrypted HoP TLM, which is telemetry data related to the portion of the payload 205 that is leased by the HOC 260) to the first communication security module 262. The first communication security module 262 then encrypts the unencrypted host telemetry and unencrypted hosted telemetry utilizing the first COMSEC variety to generate encrypted telemetry (i.e. encrypted TLM) (i.e. encrypted host telemetry and encrypted hosted telemetry).

[0059] The first communication security module 262 then transmits 293 the encrypted telemetry to a telemetry transmitter 294. The telemetry transmitter 294 then transmits 295 the encrypted telemetry to the host SOC 250. The telemetry transmitter 294 transmits 295 the encrypted telemetry utilizing an out-of-band frequency band(s). The host SOC 250 then decrypts the encrypted telemetry utilizing the first COMSEC variety to generate the unencrypted telemetry. The host SOC 250 then utilizes a database that comprises host payload decommutated information and does not comprise hosted payload decommutated information (i.e. a database

without hosted payload decommutated information) to read to unencrypted telemetry to determine the telemetry data related to the portion of the payload 205 that is utilized by the host SOC 250.

[0060] The host SOC 250 then transmits 299 the encrypted telemetry to the HOC 260. The HOC 260 then decrypts the encrypted telemetry utilizing the first COMSEC variety to generate the unencrypted telemetry. The HOC 260 then utilizes a database that comprises hosted payload decommutated information and does not comprise host payload decommutated information (i.e. a database without host payload decommutated information) to read to unencrypted telemetry to determine the telemetry data related to the portion of the payload 205 that is utilized by the HOC 260.

[0061] FIGS. 3A, 3B, and 3C together show a flow chart for the disclosed method for protected multi-operators payload operations where the host user transmits encrypted host commands (encrypted utilizing a first COMSEC variety) and encrypted hosted commands (encrypted utilizing the second COMSEC variety) to a vehicle, and where the host telemetry and the hosted telemetry are both encrypted using the first COMSEC variety, in accordance with at least one embodiment of the present disclosure. At the start 300 of the method, a hosted payload (HoP) operation center (HOC) encrypts unencrypted hosted commands by utilizing a second COMSEC variety to produce encrypted hosted commands 305. Then, the HOC transmits the encrypted hosted commands to a host spacecraft operations center (SOC) 310. The host SOC encrypts unencrypted host commands by utilizing a first COMSEC variety to produce encrypted host commands 315. Then, the host SOC transmits (out-of-band) the encrypted host commands and the encrypted hosted commands to a vehicle 320.

[0062] Then, a host command receiver on the vehicle receives the encrypted host commands 325. And, a hosted command receiver on the vehicle receives the encrypted hosted commands 330. The host command receiver transmits the encrypted host commands to a first communication security module 335. The hosted command receiver transmits the encrypted hosted commands to a second communication security module 340. The first communication security module then decrypts the encrypted host commands utilizing the first COMSEC variety to generate the unencrypted host commands 345. The second communication security module then decrypts the encrypted hosted commands utilizing the second COMSEC variety to generate the unencrypted hosted commands 350.

[0063] The first communication security module then transmits the unencrypted host commands to the payload 355. The second communication security module then transmits the unencrypted hosted commands to the payload 360. Then, the payload is reconfigured according to the unencrypted host commands and the unencrypted hosted commands 365. A payload

antenna on the vehicle then transmits payload data to a host receiving antenna and a hosted receiving antenna 370.

[0064] Then, the payload transmits to the first communication security module unencrypted host telemetry and unencrypted hosted telemetry 375. Then, the first communication security module encrypts the unencrypted host telemetry and the unencrypted hosted telemetry utilizing the first COMSEC variety to generate encrypted host telemetry and encrypted hosted telemetry 380. The first communication security module then transmits the encrypted host telemetry and the encrypted hosted telemetry to a telemetry transmitter 385. Then, the telemetry transmitter transmits the encrypted host telemetry and the encrypted hosted telemetry to the host SOC 390. The host SOC then decrypts the encrypted host telemetry utilizing the first COMSEC variety to generate the unencrypted host telemetry 395.

[0065] The host SOC transmits the encrypted hosted telemetry to the HOC 396. Then, the HOC decrypts the encrypted hosted telemetry utilizing the first COMSEC variety to generate the unencrypted hosted telemetry 397. Then, the method ends 398.

[0066] FIG. 4 is a diagram 400 showing the disclosed system for protected multi-operators payload operations where the host user (i.e. the host SOC) 450 transmits encrypted host commands (encrypted utilizing a first COMSEC variety) and encrypted hosted commands (encrypted utilizing a second COMSEC variety) to a vehicle, and where the host telemetry is encrypted using the first COMSEC variety and the hosted telemetry is encrypted using the second COMSEC variety, in accordance with at least one embodiment of the present disclosure. In this figure, a vehicle 410, a host SOC 450, and a HOC 460 are shown. The HOC 460 has leased at least a portion (e.g., a virtual transponder(s)) of the payload 405 of the vehicle 410 from the owner of a satellite (i.e. the host SOC) 450. It should be noted that in some embodiments, the HOC 460 may lease all of the payload 405 of the vehicle 410 from the owner of a satellite (i.e. the host SOC) 450. Also, it should be noted that is some embodiments, the HOC 460 may own the payload 405 (e.g., a steerable antenna) of the vehicle 410, and contract the host SOC 450 to transmit encrypted hosted commands to the vehicle 410.

[0067] During operation, the HOC 460 encrypts unencrypted hosted commands (i.e. unencrypted HoP CMD), by utilizing a second COMSEC variety, to produce encrypted hosted commands (i.e. encrypted HoP CMD). The hosted commands are commands that are used to configure the portion (e.g., a virtual transponder(s)) of the payload 405 that the HOC 460 is leasing from the host SOC 450. The host SOC 450 encrypts unencrypted host commands (i.e. unencrypted host CMD), by utilizing a first COMSEC variety, to produce encrypted host commands (i.e. encrypted host CMD). The host commands are commands that are used to

configure the portion (e.g., a transponder(s)) of the payload 405 that host SOC 450 is utilizing for itself.

[0068] It should be noted that, although in FIG. 4 the host SOC 450 is depicted to have its ground antenna located right next to its operations building; in other embodiments, the host SOC 450 may have its ground antenna located very far away from the its operations building (e.g., the ground antenna may be located in another country than the operations building).

[0069] Also, it should be noted that the first COMSEC variety may include at least one encryption key and/or at least one algorithm (e.g., a Type 1 encryption algorithm or a Type 2 encryption algorithm). Additionally, it should be noted that the second COMSEC variety may include at least one encryption key and/or at least one encryption algorithm (e.g., a Type 1 encryption algorithm or a Type 2 encryption algorithm).

[0070] The HOC 460 then transmits 415 the encrypted hosted commands to the host SOC 450. After the host SOC 450 receives the encrypted hosted commands, the host SOC 450 transmits 420 the encrypted host commands and transmits 425 the encrypted hosted commands to the vehicle 410. The host SOC 450 transmits 420, 425 the encrypted host commands and the encrypted hosted commands utilizing an out-of-band frequency band(s) (i.e. a frequency band(s) that is not the same frequency band(s) utilized to transmit payload data). The host command receiver 435 on the vehicle 410 receives the encrypted host commands. In addition, the hosted command receiver 445 on the vehicle 410 receives the encrypted hosted commands.

[0071] The host command receiver 435 then transmits 452 the encrypted host commands to a first communication security module 462. The first communication security module 462 decrypts the encrypted host commands utilizing the first COMSEC variety (i.e. COMSEC Variety 1) to generate unencrypted host commands.

[0072] It should be noted that the first communication security module 462 may comprise one or more modules. In addition, the first communication security module 462 may comprise one or more processors.

[0073] The hosted command receiver 445 then transmits 455 the encrypted hosted commands to a second communication security module 465. The second communication security module 465 decrypts the encrypted hosted commands utilizing the second COMSEC variety (i.e. COMSEC Variety 2) to generate unencrypted hosted commands.

[0074] It should be noted that the second communication security module 465 may comprise one or more modules. In addition, the second communication security module 465 may comprise one or more processors.

[0075] The first communication security module 462 then transmits 470 the unencrypted host commands to the payload (i.e. the shared host/hosted payload) 405. The second communication

security module 465 transmits 475 the unencrypted hosted commands to the payload (i.e. the shared host/hosted payload) 405. The payload 405 is reconfigured according to the unencrypted host commands and the unencrypted hosted commands. A payload antenna 480 then transmits (e.g., in one or more antenna beams 481) payload data to a host receiving antenna 485 and a hosted receiving antenna 490 on the ground.

[0076] Also, it should be noted that, although in FIG. 4, antenna beams 481 is shown to include a plurality of circular spot beams; in other embodiments, antenna beams 481 may include more or less number of beams than is shown in FIG. 4 (e.g., antenna beams 481 may only include a single beam), and antenna beams 481 may include beams of different shapes than circular spot beams as is shown in FIG. 4 (e.g., antenna beams 481 may include elliptical beams and/or shaped beams of various different shapes).

[0077] It should be noted that in one or more embodiments, the payload antenna 480 may comprise one or more reflector dishes including, but not limited to, parabolic reflectors and/or shaped reflectors. In some embodiments, the payload antenna 480 may comprise one or more multifeed antenna arrays.

[0078] The payload 405 transmits 491 unencrypted host telemetry (i.e. unencrypted host TLM, which is telemetry data related to the portion of the payload 405 that is utilized by the host SOC 450) to the first communication security module 462. The first communication security module 462 then encrypts the unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry (i.e. encrypted host TLM).

[0079] The payload 405 transmits 492 unencrypted hosted telemetry (i.e. unencrypted HoP TLM, which is telemetry data related to the portion of the payload 405 that is leased by the HOC 460) to the second communication security module 465. The second communication security module 465 then encrypts the unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry (i.e. encrypted HoP TLM).

[0080] The first communication security module 462 then transmits 493 the encrypted host telemetry to a host telemetry transmitter 494. The host telemetry transmitter 494 then transmits 495 the encrypted host telemetry to the host SOC 450. The telemetry transmitter 494 transmits 495 the encrypted host telemetry utilizing an out-of-band frequency band(s). The host SOC 450 then decrypts the encrypted host telemetry utilizing the first COMSEC variety to generate the unencrypted host telemetry.

[0081] The second communication security module 465 then transmits 496 the encrypted hosted telemetry to a hosted telemetry transmitter 498. The hosted telemetry transmitter 498 then transmits 497 the encrypted hosted telemetry to the host SOC 450. The telemetry transmitter 498 transmits 497 the encrypted hosted telemetry utilizing an out-of-band frequency band(s). The host

SOC 450 then transmits 499 the encrypted hosted telemetry to the HOC 460. The HOC 460 then decrypts the encrypted hosted telemetry utilizing the second COMSEC variety to generate the unencrypted hosted telemetry.

[0082] FIGS. 5A, 5B, 5C, and 5D together show a flow chart for the disclosed method for protected multi-operators payload operations where the host user transmits encrypted host commands (encrypted utilizing a first COMSEC variety) and encrypted hosted commands (encrypted utilizing a second COMSEC variety) to a vehicle, and where the host telemetry is encrypted using the first COMSEC variety and the hosted telemetry is encrypted using the second COMSEC variety, in accordance with at least one embodiment of the present disclosure. At the start 500 of the method, a hosted payload (HoP) operation center (HOC) encrypts unencrypted hosted commands by utilizing a second COMSEC variety to produce encrypted hosted commands 505. Then, the HOC transmits the encrypted hosted commands to a host spacecraft operations center (SOC) 510. The host SOC encrypts unencrypted host commands by utilizing a first COMSEC variety to produce encrypted host commands 515. Then, the host SOC transmits (out-of-band) the encrypted host commands and the encrypted hosted commands to a vehicle 520.

[0083] Then, a host command receiver on the vehicle receives the encrypted host commands 525. And, a hosted command receiver on the vehicle receives the encrypted hosted commands 530. The host command receiver transmits the encrypted host commands to a first communication security module 535. The hosted command receiver transmits the encrypted hosted commands to a second communication security module 540. The first communication security module then decrypts the encrypted host commands utilizing the first COMSEC variety to generate the unencrypted host commands 545. The second communication security module then decrypts the encrypted hosted commands utilizing the second COMSEC variety to generate the unencrypted hosted commands 550.

[0084] The first communication security module then transmits the unencrypted host commands to the payload 555. The second communication security module then transmits the unencrypted hosted commands to the payload 560. Then, the payload is reconfigured according to the unencrypted host commands and the unencrypted hosted commands 565. A payload antenna on the vehicle then transmits payload data to a host receiving antenna and a hosted receiving antenna 570.

[0085] Then, the payload transmits to the first communication security module unencrypted host telemetry 575. The first communication security module then encrypts the unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry 580. Then, the first communication security module transmits the encrypted host telemetry to a host telemetry

transmitter 585. The host telemetry transmitter then transmits the encrypted host telemetry to the host SOC 590. Then, the host SOC decrypts the encrypted host telemetry utilizing the first COMSEC variety to generate the unencrypted host telemetry 591.

[0086] The payload transmits to the second communication security module unencrypted hosted telemetry 592. Then, the second communication security module encrypts the unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry 593. The second communication security module then transmits the encrypted hosted telemetry to a hosted telemetry transmitter 594. Then, the hosted telemetry transmitter transmits the encrypted hosted telemetry to the host SOC 595. The host SOC then transmits the encrypted hosted telemetry to the HOC 596. Then the HOC decrypts the encrypted hosted telemetry utilizing the second COMSEC variety to generate the unencrypted hosted telemetry 597. Then, the method ends 598.

[0087] FIG. 6 is a diagram 600 showing the disclosed system for protected multi-operators payload operations where the host user (i.e. the host SOC) 650 transmits encrypted host commands (encrypted utilizing a first COMSEC variety) to a vehicle and the hosted user (i.e. the HOC) 660 transmits encrypted hosted commands (encrypted utilizing a second COMSEC variety) to the vehicle, and where the host telemetry is encrypted using the first COMSEC variety and the hosted telemetry is encrypted using the second COMSEC variety, in accordance with at least one embodiment of the present disclosure. In this figure, a vehicle 610, a host SOC 650, and a HOC 660 are shown. The HOC 660 has leased at least a portion (e.g., a virtual transponder(s)) of the payload 605 of the vehicle 610 from the owner of a satellite (i.e. the host SOC) 650. It should be noted that in some embodiments, the HOC 660 may lease all of the payload 605 of the vehicle 610 from the owner of a satellite (i.e. the host SOC) 650. Also, it should be noted that is some embodiments, the HOC 660 may own the payload 605 (e.g., a steerable antenna) of the vehicle 610.

[0088] During operation, the HOC 660 encrypts unencrypted hosted commands (i.e. unencrypted HoP CMD), by utilizing a second COMSEC variety, to produce encrypted hosted commands (i.e. encrypted HoP CMD). The hosted commands are commands that are used to configure the portion (e.g., a virtual transponder(s)) of the payload 605 that the HOC 660 is leasing from the host SOC 650. The host SOC 650 encrypts unencrypted host commands (i.e. unencrypted host CMD), by utilizing a first COMSEC variety, to produce encrypted host commands (i.e. encrypted host CMD). The host commands are commands that are used to configure the portion (e.g., a transponder(s)) of the payload 605 that host SOC 650 is utilizing for itself.

[0089] It should be noted that, although in FIG. 6 the host SOC 650 is depicted to have its ground antenna located right next to its operations building; in other embodiments, the host SOC 650 may have its ground antenna located very far away from the its operations building (e.g., the ground antenna may be located in another country than the operations building).

[0090] Also, it should be noted that the first COMSEC variety may include at least one encryption key and/or at least one algorithm (e.g., a Type 1 encryption algorithm or a Type 2 encryption algorithm). Additionally, it should be noted that the second COMSEC variety may include at least one encryption key and/or at least one encryption algorithm (e.g., a Type 1 encryption algorithm or a Type 2 encryption algorithm).

[0091] The host SOC 650 transmits 620 the encrypted host commands to the vehicle 610. The host SOC 650 transmits 620 the encrypted host commands utilizing an out-of-band frequency band(s) (i.e. a frequency band(s) that is not the same frequency band(s) utilized to transmit payload data).

[0092] The HOC 660 transmits 625 the encrypted hosted commands to the vehicle 610. The HOC 660 transmits 625 the encrypted hosted commands utilizing an out-of-band frequency band(s).

[0093] The host command receiver 635 on the vehicle 610 receives the encrypted host commands. In addition, the hosted command receiver 645 on the vehicle 610 receives the encrypted hosted commands.

[0094] The host command receiver 635 then transmits 652 the encrypted host commands to a first communication security module 662. The first communication security module 662 decrypts the encrypted host commands utilizing the first COMSEC variety (i.e. COMSEC Variety 1) to generate unencrypted host commands.

[0095] It should be noted that the first communication security module 662 may comprise one or more modules. In addition, the first communication security module 662 may comprise one or more processors.

[0096] The hosted command receiver 645 then transmits 655 the encrypted hosted commands to a second communication security module 665. The second communication security module 665 decrypts the encrypted hosted commands utilizing the second COMSEC variety (i.e. COMSEC Variety 2) to generate unencrypted hosted commands.

[0097] It should be noted that the second communication security module 665 may comprise one or more modules. In addition, the second communication security module 665 may comprise one or more processors.

[0098] The first communication security module 662 then transmits 670 the unencrypted host commands to the payload (i.e. the shared host/hosted payload) 605. The second communication

security module 665 transmits 675 the unencrypted hosted commands to the payload (i.e. the shared host/hosted payload) 605. The payload 605 is reconfigured according to the unencrypted host commands and the unencrypted hosted commands. A payload antenna 680 then transmits (e.g., in one or more antenna beams 681) payload data to a host receiving antenna 685 and a hosted receiving antenna 690 on the ground.

[0099] Also, it should be noted that, although in FIG. 6, antenna beams 681 is shown to include a plurality of circular spot beams; in other embodiments, antenna beams 681 may include more or less number of beams than is shown in FIG. 6 (e.g., antenna beams 681 may only include a single beam), and antenna beams 681 may include beams of different shapes than circular spot beams as is shown in FIG. 6 (e.g., antenna beams 681 may include elliptical beams and/or shaped beams of various different shapes).

[00100] It should be noted that in one or more embodiments, the payload antenna 680 may comprise one or more reflector dishes including, but not limited to, parabolic reflectors and/or shaped reflectors. In some embodiments, the payload antenna 680 may comprise one or more multifeed antenna arrays.

[00101] The payload 605 transmits 691 unencrypted host telemetry (i.e. unencrypted host TLM, which is telemetry data related to the portion of the payload 605 that is utilized by the host SOC 650) to the first communication security module 662. The first communication security module 662 then encrypts the unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry (i.e. encrypted host TLM).

[00102] The payload 605 transmits 692 unencrypted hosted telemetry (i.e. unencrypted HoP TLM, which is telemetry data related to the portion of the payload 605 that is leased by the HOC 660) to the second communication security module 665. The second communication security module 665 then encrypts the unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry (i.e. encrypted HoP TLM).

[00103] The first communication security module 662 then transmits 693 the encrypted host telemetry to a host telemetry transmitter 694. The host telemetry transmitter 694 then transmits 695 the encrypted host telemetry to the host SOC 650. The telemetry transmitter 694 transmits 695 the encrypted host telemetry utilizing an out-of-band frequency band(s). The host SOC 650 then decrypts the encrypted host telemetry utilizing the first COMSEC variety to generate the unencrypted host telemetry.

[00104] The second communication security module 665 then transmits 696 the encrypted hosted telemetry to a hosted telemetry transmitter 698. The hosted telemetry transmitter 698 then transmits 697 the encrypted hosted telemetry to the HOC 660. The telemetry transmitter 698 transmits 697 the encrypted hosted telemetry utilizing an out-of-band frequency band(s). The

HOC 660 then decrypts the encrypted hosted telemetry utilizing the second COMSEC variety to generate the unencrypted hosted telemetry.

[00105] FIGS. 7A, 7B, and 7C together show a flow chart for the disclosed method for protected multi-operators payload operations where the host user transmits encrypted host commands (encrypted utilizing a first COMSEC variety) to a vehicle and the hosted user transmits encrypted hosted commands (encrypted utilizing a second COMSEC variety) to the vehicle, and where the host telemetry is encrypted using the first COMSEC variety and the hosted telemetry is encrypted using the second COMSEC variety, in accordance with at least one embodiment of the present disclosure. At the start 700 of the method, a hosted payload (HoP) operation center (HOC) encrypts unencrypted hosted commands by utilizing a second COMSEC variety to produce encrypted hosted commands 705. Then, the HOC transmits (out-of-band) the encrypted hosted commands to a vehicle 710. The host spacecraft operations center (SOC) encrypts unencrypted host commands by utilizing a first COMSEC variety to produce encrypted host commands 715. Then, the host SOC transmits (out-of-band) the encrypted host commands to the vehicle 720.

[00106] Then, a host command receiver on the vehicle receives the encrypted host commands 725. And, a hosted command receiver on the vehicle receives the encrypted hosted commands 730. The host command receiver transmits the encrypted host commands to a first communication security module 735. The hosted command receiver transmits the encrypted hosted commands to a second communication security module 740. The first communication security module then decrypts the encrypted host commands utilizing the first COMSEC variety to generate the unencrypted host commands 745. The second communication security module then decrypts the encrypted hosted commands utilizing the second COMSEC variety to generate the unencrypted hosted commands 750.

[00107] The first communication security module then transmits the unencrypted host commands to the payload 755. The second communication security module then transmits the unencrypted hosted commands to the payload 760. Then, the payload is reconfigured according to the unencrypted host commands and the unencrypted hosted commands 765. A payload antenna on the vehicle then transmits payload data to a host receiving antenna and a hosted receiving antenna 770.

[00108] Then, the payload transmits to the first communication security module unencrypted host telemetry 775. Then, the first communication security module encrypts the unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry 780. The first communication security module then transmits the encrypted host telemetry to a host telemetry transmitter 785. Then, the host telemetry transmitter transmits the encrypted host telemetry to the

host SOC 790. Then, the host SOC decrypts the encrypted host telemetry utilizing the first COMSEC variety to generate the unencrypted host telemetry 791.

[00109] The payload transmits to the second communication security module unencrypted hosted telemetry 792. Then, the second communication security module encrypts the unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry 793. The second communication security module then transmits the encrypted hosted telemetry to a hosted telemetry transmitter 794. Then, the hosted telemetry transmitter transmits the encrypted hosted telemetry to the HOC 795. The HOC then decrypts the encrypted hosted telemetry utilizing the second COMSEC variety to generate the unencrypted hosted telemetry 796. Then, the method ends 797.

[00110] FIG. 8 is a diagram 800 showing components of an exemplary virtual transponder that may be employed by the disclosed system for protected multi-operators payload operations, in accordance with at least one embodiment of the present disclosure. In this figure, various components are shown that may be configured according to the unencrypted host commands (e.g., the host channel 830) and unencrypted hosted commands (e.g., the hosted channel 820).

[00111] In this figure, the uplink antenna 840, the downlink antenna 850, and various components of an all-digital payload 860 (including the analog-to-digital (A/D) converter 865, the digital channelizer 875, the digital switch matrix 895, the digital combiner 815, and the digital-to-analog (D/A) converter 835) are shown that may be configured according to the unencrypted host commands (e.g., the host channel 830) and unencrypted hosted commands (e.g., the hosted channel 820). In addition, some other components of the all-digital payload 860 (including the uplink beamforming 870, the demodulator 880, the modulator 890, and the downlink beamforming 825) may optionally be configured according to the unencrypted host commands (e.g., the host channel 830) and unencrypted hosted commands (e.g., the hosted channel 820).

[00112] Although particular embodiments have been shown and described, it should be understood that the above discussion is not intended to limit the scope of these embodiments. While embodiments and variations of the many aspects of the present disclosure have been disclosed and described herein, such disclosure is provided for purposes of explanation and illustration only. Thus, various changes and modifications may be made without departing from the scope of the claims.

[00113] Where methods described above indicate certain events occurring in certain order, those of ordinary skill in the art having the benefit of this disclosure would recognize that the ordering may be modified and that such modifications are in accordance with the variations of the present disclosure. Additionally, parts of methods may be performed concurrently in a

parallel process when possible, as well as performed sequentially. In addition, more parts or less part of the methods may be performed.

[00114] Accordingly, embodiments are intended to exemplify alternatives, modifications, and equivalents that may fall within the scope of the claims.

[00115] Although certain illustrative embodiments and methods have been disclosed herein, it can be apparent from the foregoing disclosure to those skilled in the art that variations and modifications of such embodiments and methods can be made without departing from the true spirit and scope of the art disclosed. Many other examples of the art disclosed exist, each differing from others in matters of detail only. Accordingly, it is intended that the art disclosed shall be limited only to the extent required by the appended claims and the rules and principles of applicable law.

WE CLAIM:

1. A method for protected multi-operators payload operations, the method comprising:

transmitting, by a hosted payload (HoP) operation center (HOC), encrypted hosted commands to a host spacecraft operations center (SOC);

transmitting, by the host SOC, encrypted host commands and the encrypted hosted commands to a vehicle, wherein the encrypted host commands are encrypted utilizing a first communication security (COMSEC) variety and the encrypted hosted commands are encrypted utilizing a second COMSEC variety;

decrypting, by a first communication security module on the vehicle, the encrypted host commands utilizing the first COMSEC variety to generate unencrypted host commands;

decrypting, by a second communication security module on the vehicle, the encrypted hosted commands utilizing the second COMSEC variety to generate unencrypted hosted commands;

reconfiguring a payload on the vehicle according to the unencrypted host commands and the unencrypted hosted commands;

transmitting, by a payload antenna on the vehicle, payload data to a host receiving antenna and a hosted receiving antenna;

encrypting, by the first communication security module, unencrypted host telemetry and unencrypted hosted telemetry from the payload by utilizing the first COMSEC variety to generate encrypted host telemetry and encrypted hosted telemetry;

transmitting, by a telemetry transmitter on the vehicle, the encrypted host telemetry and the encrypted hosted telemetry to the host SOC; and

transmitting, by the host SOC, the encrypted hosted telemetry to the HOC.

2. The method of claim 1, wherein the reconfiguring of the payload according to the unencrypted host commands and the unencrypted hosted commands comprises adjusting at least one of: transponder power, transponder spectrum monitoring, transponder connectivity, transponder gain settings, transponder limiter settings, transponder automatic level control settings, transponder phase settings, internal gain generation, bandwidth for at least one beam, at least one frequency band for at least one of the at least one beam, transponder beamforming settings, effective isotropic radiation power (EIRP) for at least one of the at least one beam, transponder channels, or beam steering.

3. The method of claim 1, wherein the reconfiguring of the payload according to the unencrypted host commands and the unencrypted hosted commands comprises reconfiguring at least one of: at least one antenna, at least one analog-to-digital converter, at least one digital-to-analog converter, at least one beamformer, at least one digital channelizer, at least one demodulator, at least one modulator, at least one digital switch matrix, or at least one digital combiner.

4. The method of claim 1, wherein the vehicle is an airborne vehicle.

5. The method of claim 4, wherein the airborne vehicle is one of a satellite, aircraft, unmanned aerial vehicle (UAV), or space plane.

6. The method of claim 1, wherein the method further comprises:

encrypting, by the HOC, the unencrypted hosted commands by utilizing the second COMSEC variety to produce the encrypted hosted commands; and

encrypting, by the host SOC, the unencrypted host commands by utilizing the first COMSEC variety to produce the encrypted host commands.

7. The method of claim 1, wherein the method further comprises:

receiving, by a host command receiver on the vehicle, the encrypted host commands;

receiving, by a hosted command receiver on the vehicle, the encrypted hosted commands;

transmitting, by the host command receiver, the encrypted host commands to the first communication security module; and

transmitting, by the hosted command receiver, the encrypted hosted commands to the second communication security module.

8. The method of claim 1, wherein the method further comprises:

transmitting, by the first communication security module, the unencrypted host commands to the payload; and

transmitting, by the second communication security module, the unencrypted hosted commands to the payload.

9. The method of claim 1, wherein the method further comprises transmitting, by the payload, to the first communication security module the unencrypted host telemetry and the unencrypted hosted telemetry.

10. The method of claim 1, wherein the method further comprises transmitting, by the first communication security module, the encrypted host telemetry and the encrypted hosted telemetry to the telemetry transmitter.

11. The method of claim 1, wherein the method further comprises:

decrypting, by the host SOC, the encrypted host telemetry utilizing the first COMSEC variety and utilizing a database without hosted decommutated information to generate the unencrypted host telemetry; and

decrypting, by the HOC, the encrypted hosted telemetry utilizing the first COMSEC variety and utilizing a database without host decommutated information to generate the unencrypted hosted telemetry.

12. A method for protected multi-operators payload operations, the method comprising:

transmitting, by a hosted payload (HoP) operation center (HOC), encrypted hosted commands to a host spacecraft operations center (SOC);

transmitting, by the host SOC, encrypted host commands and the encrypted hosted commands to a vehicle, wherein the encrypted host commands are encrypted utilizing a first COMSEC variety and the encrypted hosted commands are encrypted utilizing a second COMSEC variety;

decrypting, by a first communication security module, the encrypted host commands utilizing the first COMSEC variety to generate unencrypted host commands;

decrypting, by a second communication security module, the encrypted hosted commands utilizing the second COMSEC variety to generate the unencrypted hosted commands;

reconfiguring a payload according to the unencrypted host commands and the unencrypted hosted commands;

transmitting, by a payload antenna on the vehicle, payload data to a host receiving antenna and a hosted receiving antenna;

encrypting, by the first communication security module, unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry;

transmitting, by a host telemetry transmitter, the encrypted host telemetry to the host SOC;

encrypting, by the second communication security module, unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry;

transmitting, by a hosted telemetry transmitter, the encrypted hosted telemetry to the host SOC; and

transmitting, by the host SOC, the encrypted hosted telemetry to the HOC.

13. The method of claim 12, wherein the reconfiguring of the payload according to the unencrypted host commands and the unencrypted hosted commands comprises adjusting at least one of: transponder power, transponder spectrum monitoring, transponder connectivity, transponder gain settings, transponder limiter settings, transponder automatic level control settings, transponder phase settings, internal gain generation, bandwidth for at least one beam, at least one frequency band for at least one of the at least one beam, transponder beamforming settings, effective isotropic radiation power (EIRP) for at least one of the at least one beam, transponder channels, or beam steering.

14. The method of claim 12, wherein the reconfiguring of the payload according to the unencrypted host commands and the unencrypted hosted commands comprises reconfiguring at least one of: at least one antenna, at least one analog-to-digital converter, at least one digital-to-analog converter, at least one beamformer, at least one digital channelizer, at least one demodulator, at least one modulator, at least one digital switch matrix, or at least one digital combiner.

15. The method of claim 12, wherein the vehicle is an airborne vehicle.

16. The method of claim 15, wherein the airborne vehicle is one of a satellite, aircraft, unmanned aerial vehicle (UAV), or space plane.

17. A method for protected multi-operators payload operations, the method comprising:

transmitting, by a hosted payload (HoP) operation center (HOC), encrypted hosted commands to a vehicle;

transmitting, by a host spacecraft operations center (SOC), encrypted host commands to the vehicle, wherein the encrypted host commands are encrypted utilizing a first communication security (COMSEC) variety and the encrypted hosted commands are encrypted utilizing a second COMSEC variety;

decrypting, by a first communication security module on the vehicle, the encrypted host commands utilizing the first COMSEC variety to generate unencrypted host commands;

decrypting, by a second communication security module on the vehicle, the encrypted hosted commands utilizing the second COMSEC variety to generate unencrypted hosted commands;

reconfiguring a payload according to the unencrypted host commands and the unencrypted hosted commands;

transmitting, by a payload antenna on the vehicle, payload data to a host receiving antenna and a hosted receiving antenna;

encrypting, by the first communication security module, unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry;

transmitting, by a host telemetry transmitter on the vehicle, the encrypted host telemetry to the host SOC;

encrypting, by the second communication security module, unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry; and

transmitting, by a hosted telemetry transmitter, the encrypted hosted telemetry to the HOC.

18. The method of claim 17, wherein the reconfiguring of the payload according to the unencrypted host commands and the unencrypted hosted commands comprises adjusting at least one of: transponder power, transponder spectrum monitoring, transponder connectivity, transponder gain settings, transponder limiter settings, transponder automatic level control settings, transponder phase settings, internal gain generation, bandwidth for at least one beam, at least one frequency band for at least one of the at least one beam, transponder beamforming settings, effective isotropic radiation power (EIRP) for at least one of the at least one beam, transponder channels, or beam steering.

19. The method of claim 17, wherein the reconfiguring of the payload according to the unencrypted host commands and the unencrypted hosted commands comprises reconfiguring at least one of: at least one antenna, at least one analog-to-digital converter, at least one digital-to-analog converter, at least one beamformer, at least one digital channelizer, at least one demodulator, at least one modulator, at least one digital switch matrix, or at least one digital combiner.

20. The method of claim 17, wherein the vehicle is an airborne vehicle, and

wherein the airborne vehicle is one of a satellite, aircraft, unmanned aerial vehicle (UAV), or space plane.

21. A system for protected multi-operators payload operations, the system comprising:

a hosted payload (HoP) operation center (HOC) to transmit encrypted hosted commands to a host spacecraft operations center (SOC);

the host SOC to transmit encrypted host commands and the encrypted hosted commands to a vehicle, wherein the encrypted host commands are encrypted utilizing a first communication security (COMSEC) variety and the encrypted hosted commands are encrypted utilizing a second COMSEC variety;

a first communication security module on the vehicle to decrypt the encrypted host commands utilizing the first COMSEC variety to generate unencrypted host commands;

a second communication security module on the vehicle to decrypt the encrypted hosted commands utilizing the second COMSEC variety to generate unencrypted hosted commands;

a payload on the vehicle reconfigured according to the unencrypted host commands and the unencrypted hosted commands;

a payload antenna on the vehicle to transmit payload data to a host receiving antenna and a hosted receiving antenna;

the first communication security module to encrypt unencrypted host telemetry and unencrypted hosted telemetry from the payload by utilizing the first COMSEC variety to generate encrypted host telemetry and encrypted hosted telemetry;

a telemetry transmitter on the vehicle to transmit the encrypted host telemetry and the encrypted hosted telemetry to the host SOC; and

the host SOC to transmit the encrypted hosted telemetry to the HOC.

22. A system for protected multi-operators payload operations, the system comprising:

a hosted payload (HoP) operation center (HOC) to transmit encrypted hosted commands to a host spacecraft operations center (SOC);

the host SOC to transmit encrypted host commands and the encrypted hosted commands to a vehicle, wherein the encrypted host commands are encrypted utilizing a first COMSEC variety and the encrypted hosted commands are encrypted utilizing a second COMSEC variety;

a first communication security module to decrypt the encrypted host commands utilizing the first COMSEC variety to generate unencrypted host commands;

a second communication security module to decrypt the encrypted hosted commands utilizing the second COMSEC variety to generate the unencrypted hosted commands;

a payload reconfigured according to the unencrypted host commands and the unencrypted hosted commands;

a payload antenna on the vehicle to transmit payload data to a host receiving antenna and a hosted receiving antenna;

the first communication security module to encrypt unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry;

a host telemetry transmitter to transmit the encrypted host telemetry to the host SOC;

the second communication security module to encrypt unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry;

a hosted telemetry transmitter to transmit the encrypted hosted telemetry to the host SOC; and

the host SOC to transmit the encrypted hosted telemetry to the HOC.

23. A system for protected multi-operators payload operations, the system comprising:

a hosted payload (HoP) operation center (HOC) to transmit encrypted hosted commands to a vehicle;

a host spacecraft operations center (SOC) to transmit encrypted host commands to the vehicle, wherein the encrypted host commands are encrypted utilizing a first communication security (COMSEC) variety and the encrypted hosted commands are encrypted utilizing a second COMSEC variety;

a first communication security module on the vehicle to decrypt the encrypted host commands utilizing the first COMSEC variety to generate unencrypted host commands;

a second communication security module on the vehicle to decrypt the encrypted hosted commands utilizing the second COMSEC variety to generate unencrypted hosted commands;

a payload reconfigured according to the unencrypted host commands and the unencrypted hosted commands;

a payload antenna on the vehicle to transmit payload data to a host receiving antenna and a hosted receiving antenna;

the first communication security module to encrypt unencrypted host telemetry utilizing the first COMSEC variety to generate encrypted host telemetry;

a host telemetry transmitter on the vehicle to transmit the encrypted host telemetry to the host SOC;

the second communication security module to encrypt unencrypted hosted telemetry utilizing the second COMSEC variety to generate encrypted hosted telemetry; and

a hosted telemetry transmitter to transmit the encrypted hosted telemetry to the HOC.

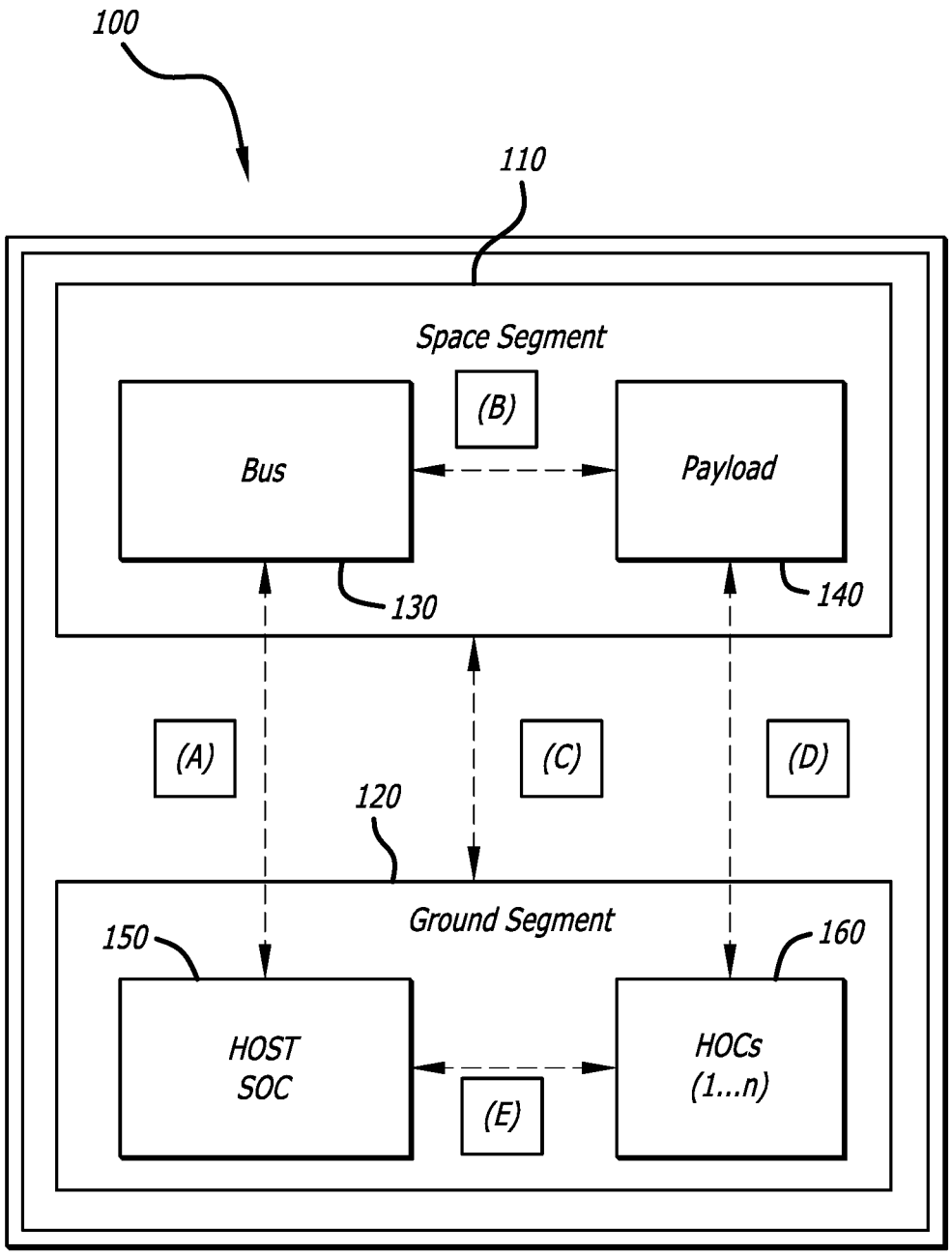

100
110
Space Segment
(B)
Bus
Payload
130
140
(A)
(C)
(D)
120
Ground Segment
150
160
HOST
SOC
HOCs
(1...n)
(E)

FIG. 1

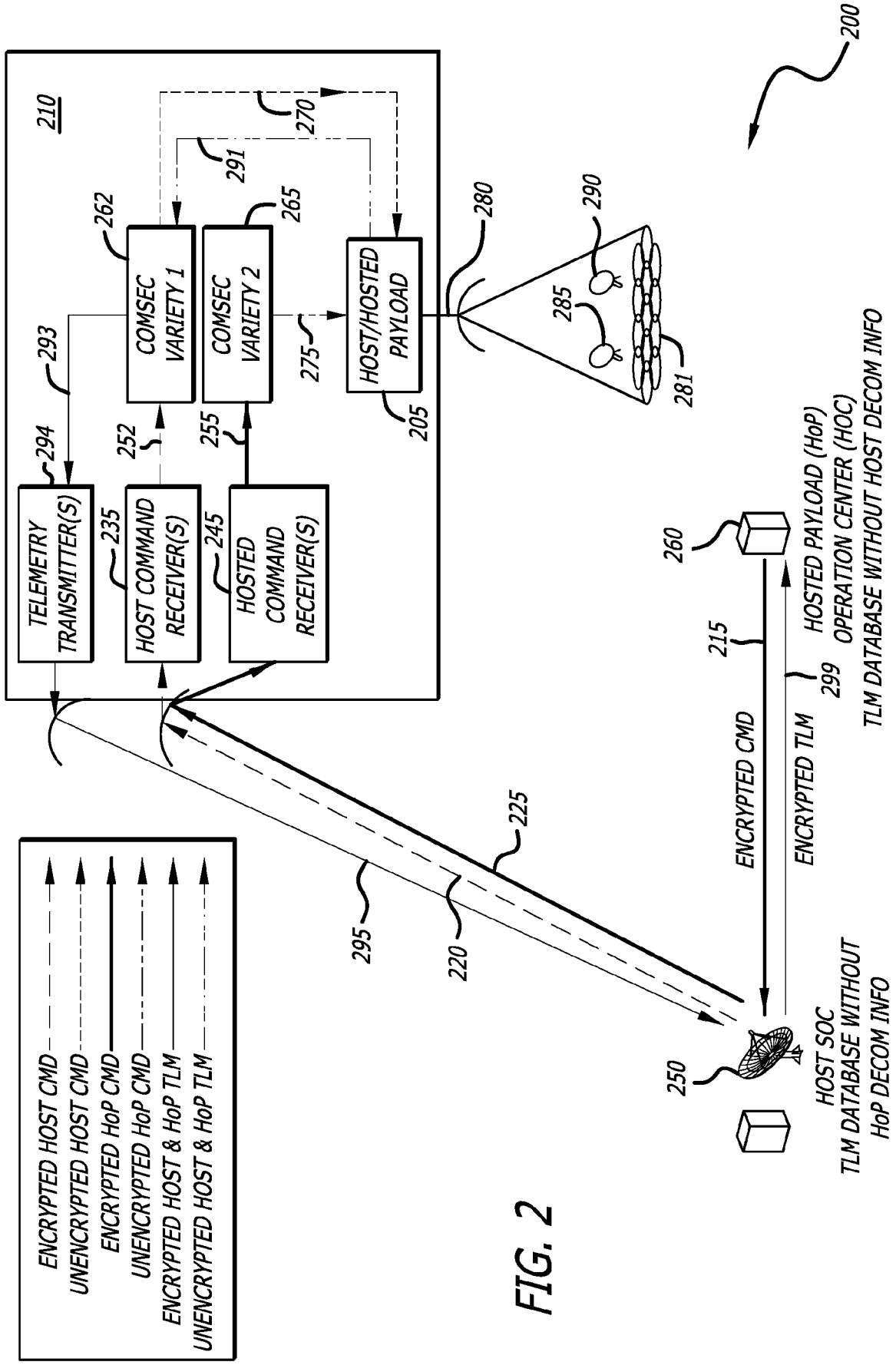

200
210
270
291
262
265
280
290
COMSEC VARIETY 1
COMSEC VARIETY 2
HOST/HOSTED PAYLOAD
285
281
293
275
205
294
252
255
TELEMETRY TRANSMITTER(S)
HOST COMMAND RECEIVER(S)
HOSTED COMMAND RECEIVER(S)
235
245
260
215
HOSTED PAYLOAD (HoP) OPERATION CENTER (HOC) TLM DATABASE WITHOUT HOST DECOM INFO
299
ENCRYPTED CMD
ENCRYPTED TLM
225
295
220
250
HOST SOC TLM DATABASE WITHOUT HoP DECOM INFO
ENCRYPTED HOST CMD
UNENCRYPTED HOST CMD
ENCRYPTED HoP CMD
UNENCRYPTED HoP CMD
ENCRYPTED HOST & HoP TLM
UNENCRYPTED HOST & HoP TLM

FIG. 2

FIG. 3A

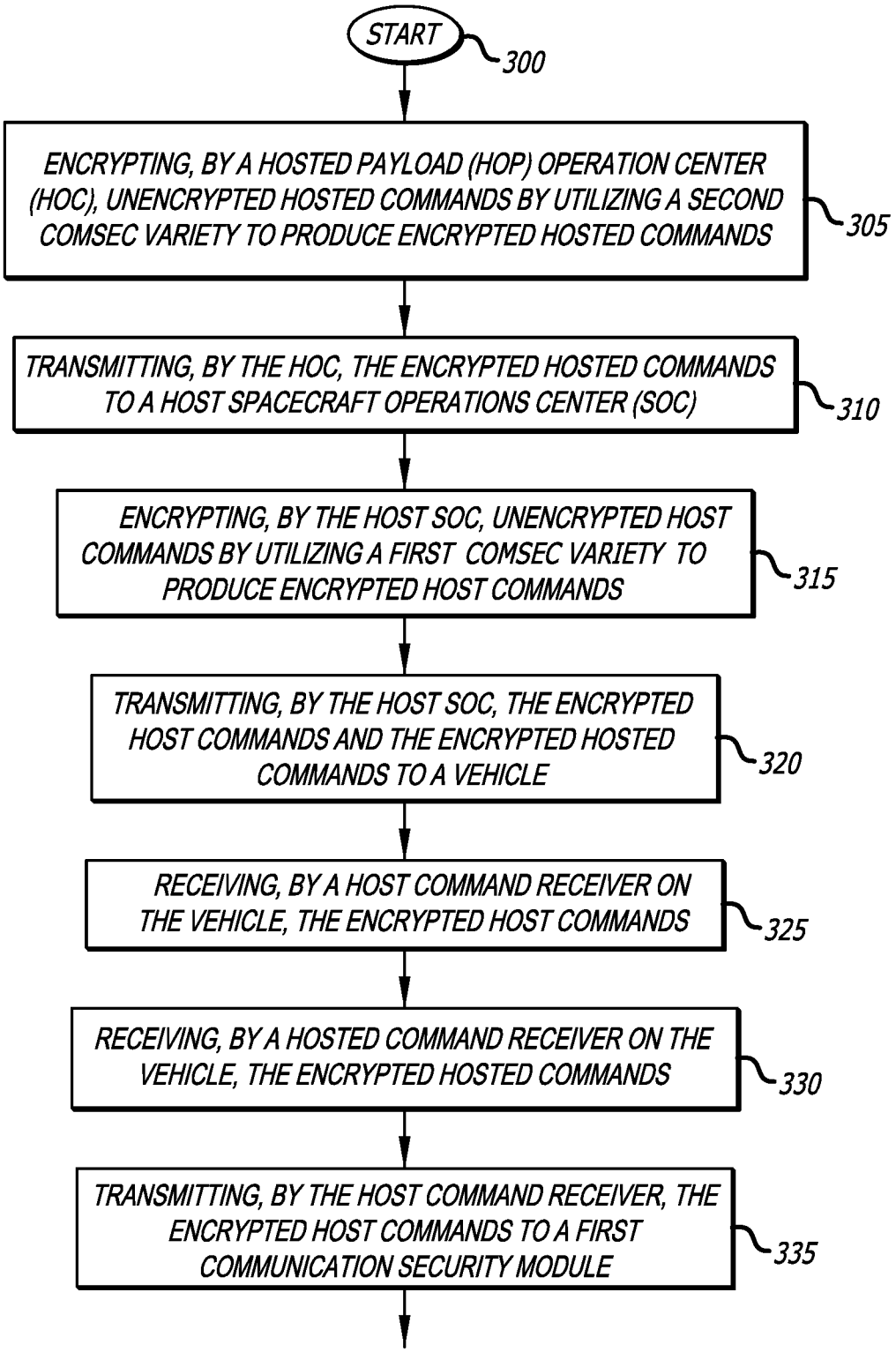

START
300
ENCRYPTING, BY A HOSTED PAYLOAD (HOP) OPERATION CENTER (HOC), UNENCRYPTED HOSTED COMMANDS BY UTILIZING A SECOND COMSEC VARIETY TO PRODUCE ENCRYPTED HOSTED COMMANDS
305
TRANSMITTING, BY THE HOC, THE ENCRYPTED HOSTED COMMANDS TO A HOST SPACECRAFT OPERATIONS CENTER (SOC)
310
ENCRYPTING, BY THE HOST SOC, UNENCRYPTED HOST COMMANDS BY UTILIZING A FIRST COMSEC VARIETY TO PRODUCE ENCRYPTED HOST COMMANDS
315
TRANSMITTING, BY THE HOST SOC, THE ENCRYPTED HOST COMMANDS AND THE ENCRYPTED HOSTED COMMANDS TO A VEHICLE
320
RECEIVING, BY A HOST COMMAND RECEIVER ON THE VEHICLE, THE ENCRYPTED HOST COMMANDS
325
RECEIVING, BY A HOSTED COMMAND RECEIVER ON THE VEHICLE, THE ENCRYPTED HOSTED COMMANDS
330
TRANSMITTING, BY THE HOST COMMAND RECEIVER, THE ENCRYPTED HOST COMMANDS TO A FIRST COMMUNICATION SECURITY MODULE
335

FIG. 3B

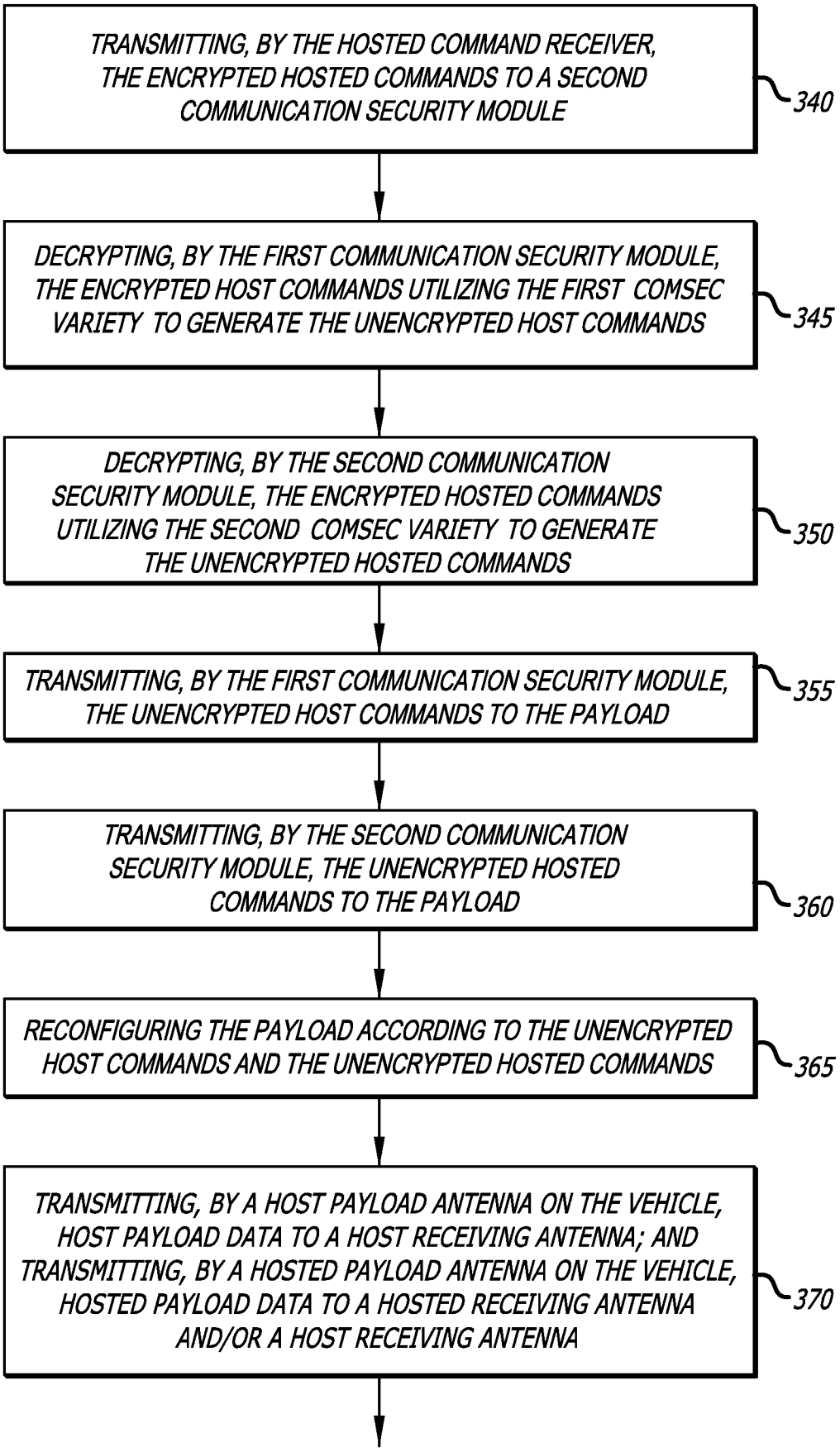
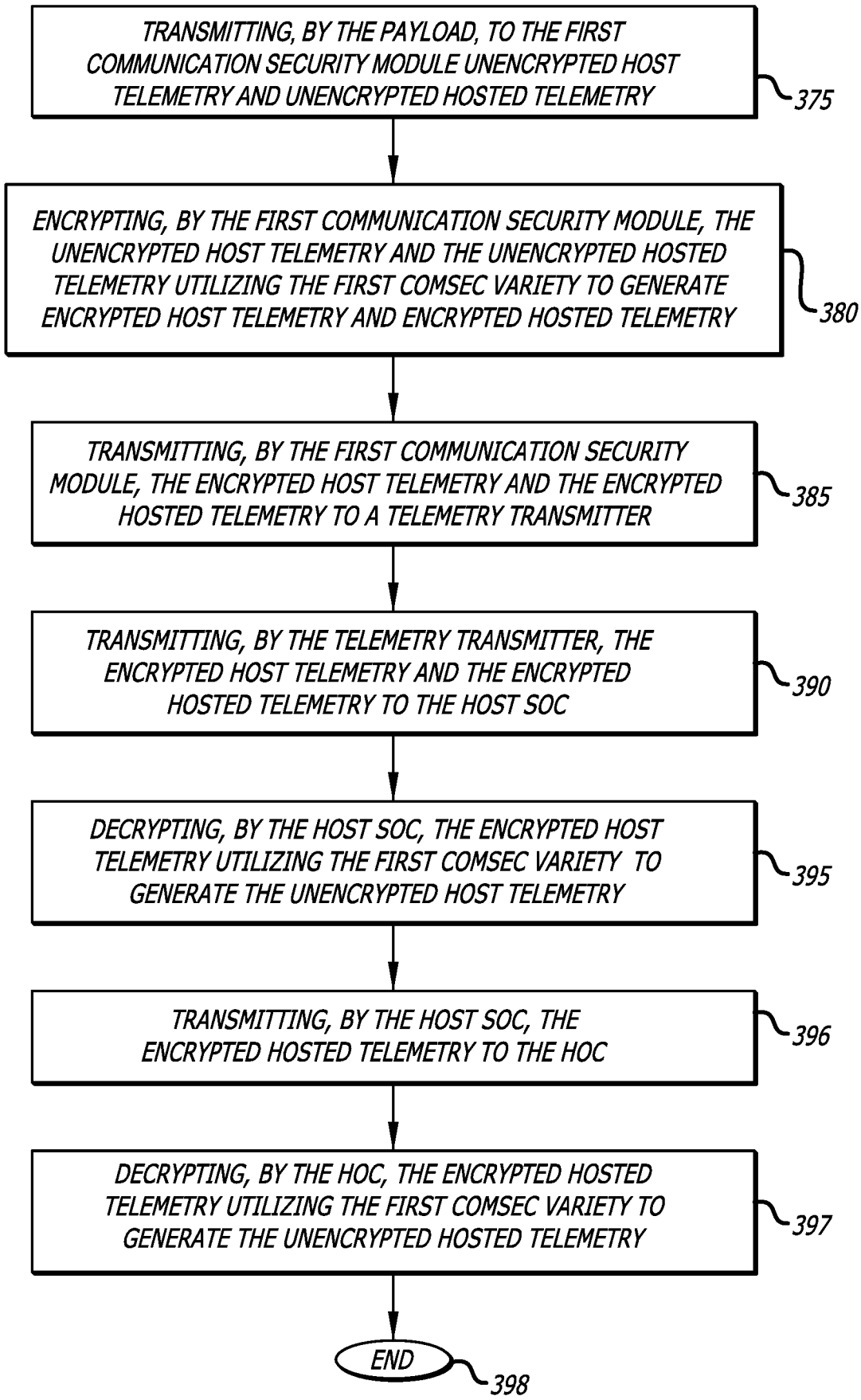

TRANSMITTING, BY THE HOSTED COMMAND RECEIVER, THE ENCRYPTED HOSTED COMMANDS TO A SECOND COMMUNICATION SECURITY MODULE
340
DECRYPTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOST COMMANDS UTILIZING THE FIRST COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOST COMMANDS
345
DECRYPTING, BY THE SECOND COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOSTED COMMANDS UTILIZING THE SECOND COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOSTED COMMANDS
350
TRANSMITTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE UNENCRYPTED HOST COMMANDS TO THE PAYLOAD
355
TRANSMITTING, BY THE SECOND COMMUNICATION SECURITY MODULE, THE UNENCRYPTED HOSTED COMMANDS TO THE PAYLOAD
360
RECONFIGURING THE PAYLOAD ACCORDING TO THE UNENCRYPTED HOST COMMANDS AND THE UNENCRYPTED HOSTED COMMANDS
365
TRANSMITTING, BY A HOST PAYLOAD ANTENNA ON THE VEHICLE, HOST PAYLOAD DATA TO A HOST RECEIVING ANTENNA; AND TRANSMITTING, BY A HOSTED PAYLOAD ANTENNA ON THE VEHICLE, HOSTED PAYLOAD DATA TO A HOSTED RECEIVING ANTENNA AND/OR A HOST RECEIVING ANTENNA
370

FIG. 3C


TRANSMITTING, BY THE PAYLOAD, TO THE FIRST COMMUNICATION SECURITY MODULE UNENCRYPTED HOST TELEMETRY AND UNENCRYPTED HOSTED TELEMETRY
375
ENCRYPTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE UNENCRYPTED HOST TELEMETRY AND THE UNENCRYPTED HOSTED TELEMETRY UTILIZING THE FIRST COMSEC VARIETY TO GENERATE ENCRYPTED HOST TELEMETRY AND ENCRYPTED HOSTED TELEMETRY
380
TRANSMITTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOST TELEMETRY AND THE ENCRYPTED HOSTED TELEMETRY TO A TELEMETRY TRANSMITTER
385
TRANSMITTING, BY THE TELEMETRY TRANSMITTER, THE ENCRYPTED HOST TELEMETRY AND THE ENCRYPTED HOSTED TELEMETRY TO THE HOST SOC
390
DECRYPTING, BY THE HOST SOC, THE ENCRYPTED HOST TELEMETRY UTILIZING THE FIRST COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOST TELEMETRY
395
TRANSMITTING, BY THE HOST SOC, THE ENCRYPTED HOSTED TELEMETRY TO THE HOC
396
DECRYPTING, BY THE HOC, THE ENCRYPTED HOSTED TELEMETRY UTILIZING THE FIRST COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOSTED TELEMETRY
397
END
398

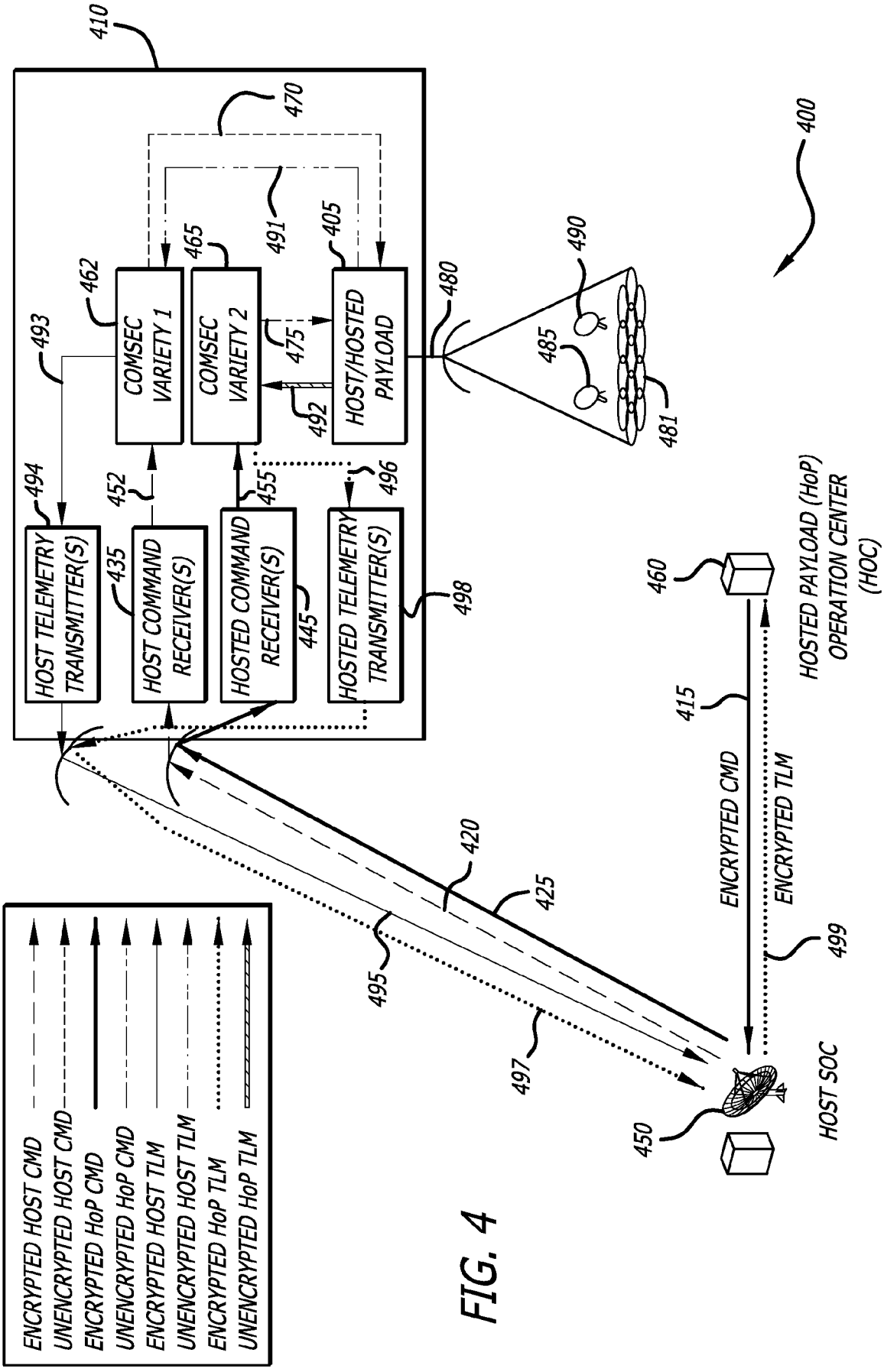

410
400
470
491
405
465
462
493
COMSEC VARIETY 1
COMSEC VARIETY 2
HOST/HOSTED PAYLOAD
475
480
490
485
492
481
494
452
455
496
HOST TELEMETRY TRANSMITTER(S)
HOST COMMAND RECEIVER(S)
HOSTED COMMAND RECEIVER(S)
HOSTED TELEMETRY TRANSMITTER(S)
435
445
498
460
415
HOSTED PAYLOAD (HoP) OPERATION CENTER (HOC)
ENCRYPTED CMD
ENCRYPTED TLM
420
425
495
497
499
450
HOST SOC
ENCRYPTED HOST CMD
UNENCRYPTED HOST CMD
ENCRYPTED HoP CMD
UNENCRYPTED HoP CMD
ENCRYPTED HOST TLM
UNENCRYPTED HOST TLM
ENCRYPTED HoP TLM
UNENCRYPTED HoP TLM

FIG. 4

FIG. 5A

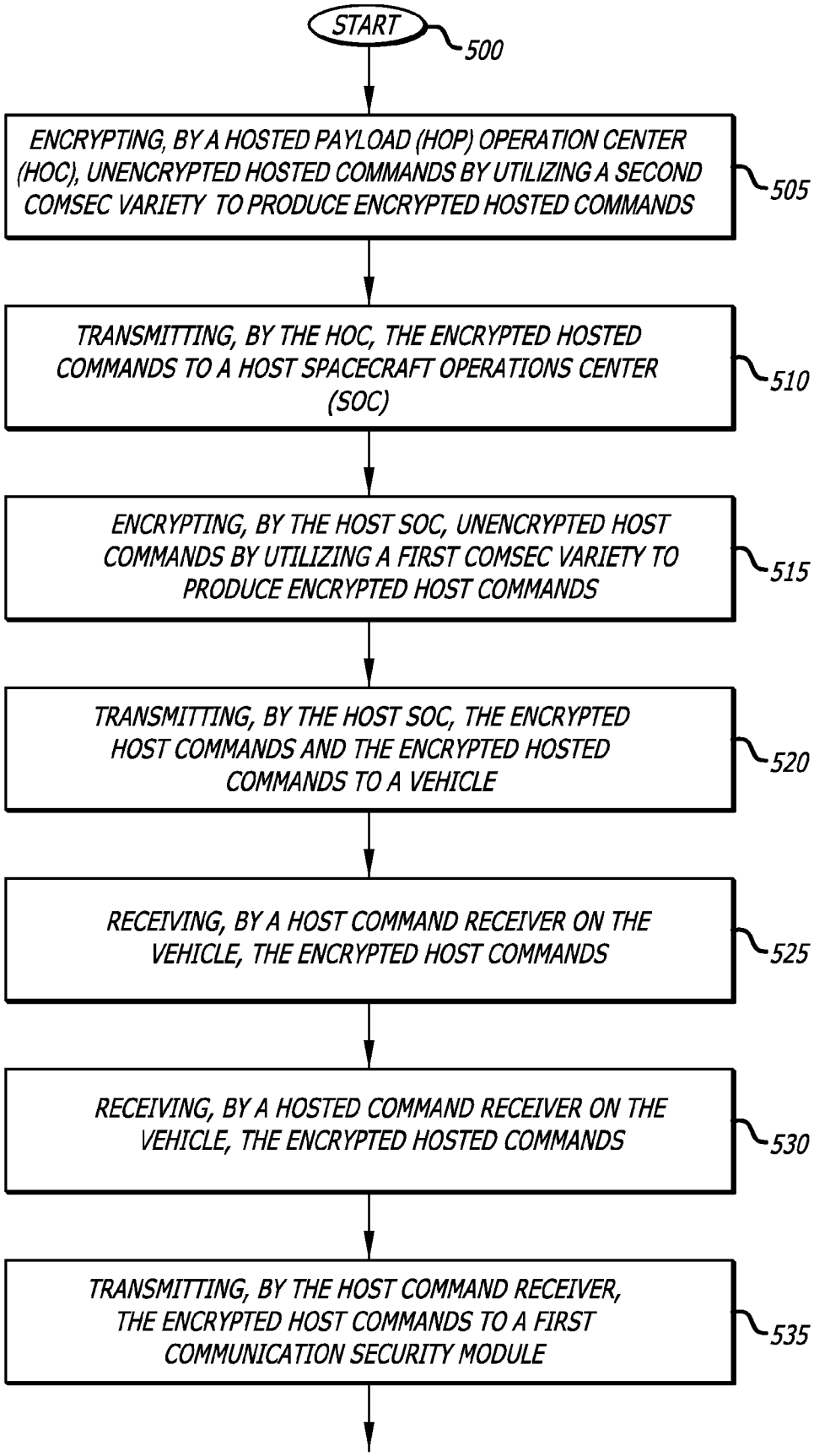

START
500
ENCRYPTING, BY A HOSTED PAYLOAD (HOP) OPERATION CENTER (HOC), UNENCRYPTED HOSTED COMMANDS BY UTILIZING A SECOND COMSEC VARIETY TO PRODUCE ENCRYPTED HOSTED COMMANDS
505
TRANSMITTING, BY THE HOC, THE ENCRYPTED HOSTED COMMANDS TO A HOST SPACECRAFT OPERATIONS CENTER (SOC)
510
ENCRYPTING, BY THE HOST SOC, UNENCRYPTED HOST COMMANDS BY UTILIZING A FIRST COMSEC VARIETY TO PRODUCE ENCRYPTED HOST COMMANDS
515
TRANSMITTING, BY THE HOST SOC, THE ENCRYPTED HOST COMMANDS AND THE ENCRYPTED HOSTED COMMANDS TO A VEHICLE
520
RECEIVING, BY A HOST COMMAND RECEIVER ON THE VEHICLE, THE ENCRYPTED HOST COMMANDS
525
RECEIVING, BY A HOSTED COMMAND RECEIVER ON THE VEHICLE, THE ENCRYPTED HOSTED COMMANDS
530
TRANSMITTING, BY THE HOST COMMAND RECEIVER, THE ENCRYPTED HOST COMMANDS TO A FIRST COMMUNICATION SECURITY MODULE
535

FIG. 5B

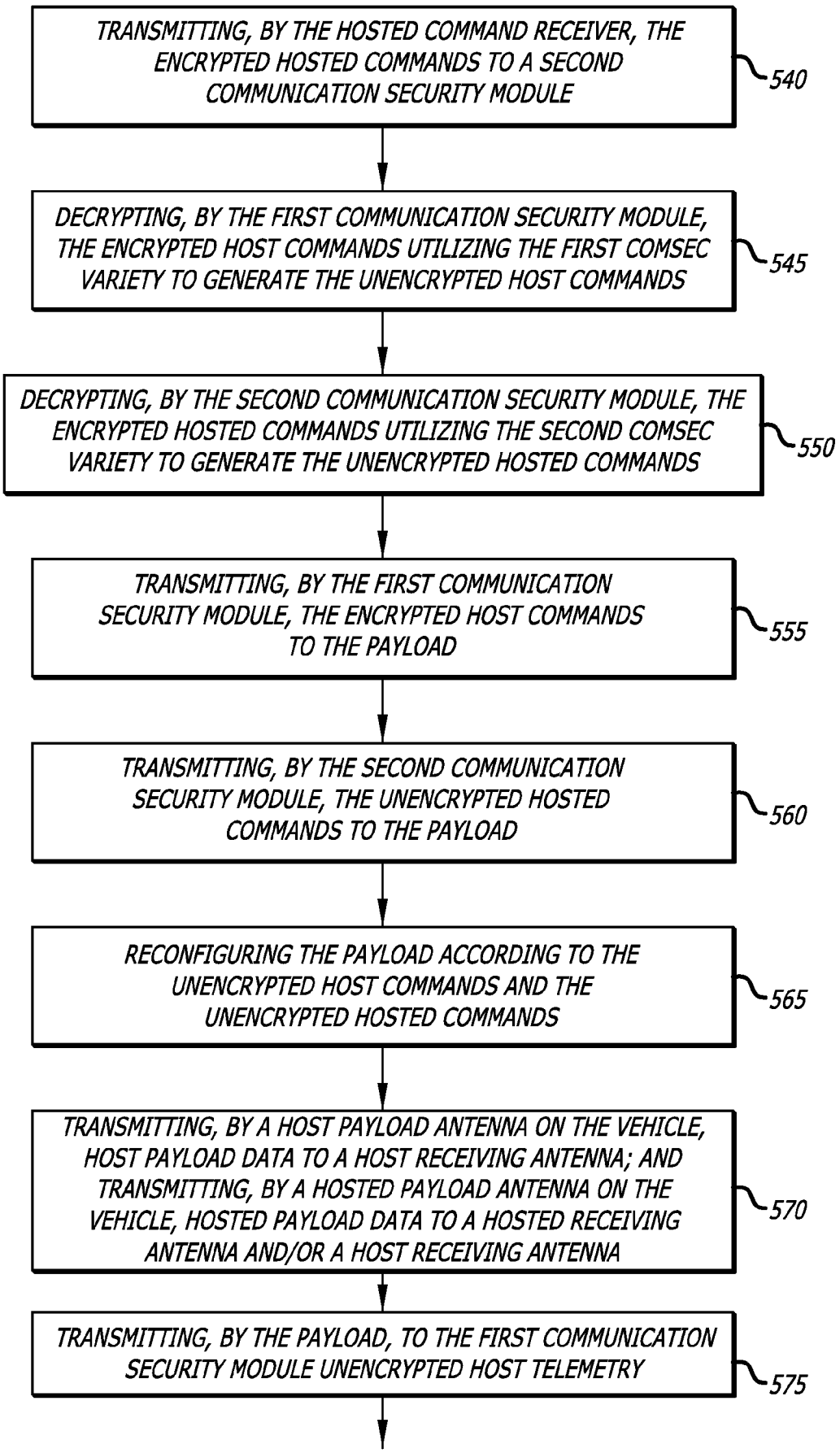

TRANSMITTING, BY THE HOSTED COMMAND RECEIVER, THE ENCRYPTED HOSTED COMMANDS TO A SECOND COMMUNICATION SECURITY MODULE
540
DECRYPTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOST COMMANDS UTILIZING THE FIRST COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOST COMMANDS
545
DECRYPTING, BY THE SECOND COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOSTED COMMANDS UTILIZING THE SECOND COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOSTED COMMANDS
550
TRANSMITTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOST COMMANDS TO THE PAYLOAD
555
TRANSMITTING, BY THE SECOND COMMUNICATION SECURITY MODULE, THE UNENCRYPTED HOSTED COMMANDS TO THE PAYLOAD
560
RECONFIGURING THE PAYLOAD ACCORDING TO THE UNENCRYPTED HOST COMMANDS AND THE UNENCRYPTED HOSTED COMMANDS
565
TRANSMITTING, BY A HOST PAYLOAD ANTENNA ON THE VEHICLE, HOST PAYLOAD DATA TO A HOST RECEIVING ANTENNA; AND TRANSMITTING, BY A HOSTED PAYLOAD ANTENNA ON THE VEHICLE, HOSTED PAYLOAD DATA TO A HOSTED RECEIVING ANTENNA AND/OR A HOST RECEIVING ANTENNA
570
TRANSMITTING, BY THE PAYLOAD, TO THE FIRST COMMUNICATION SECURITY MODULE UNENCRYPTED HOST TELEMETRY
575

FIG. 5C

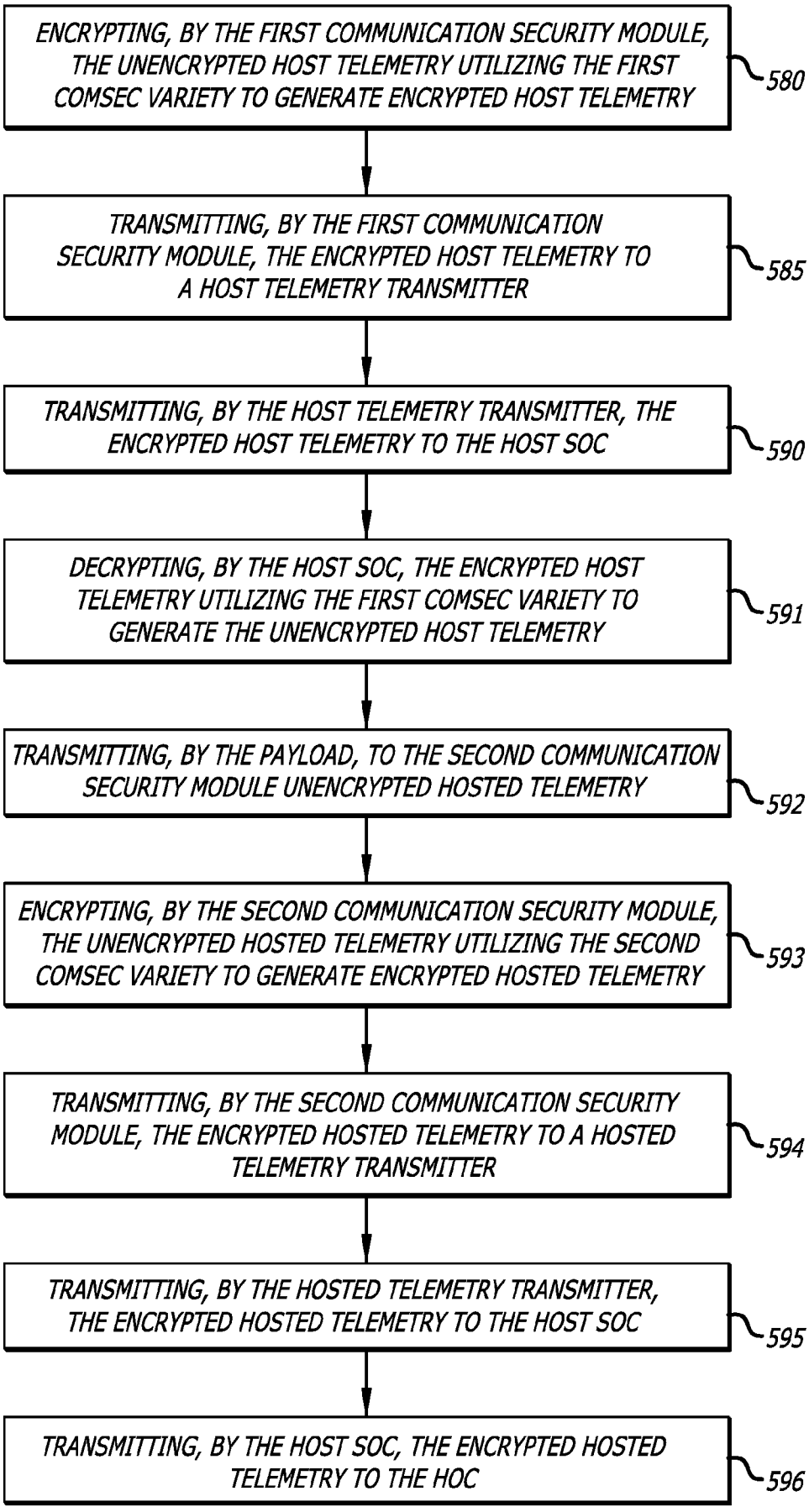
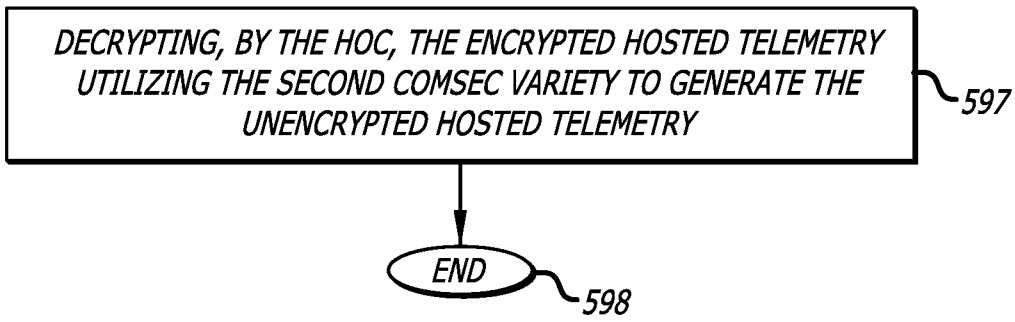

ENCRYPTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE UNENCRYPTED HOST TELEMETRY UTILIZING THE FIRST COMSEC VARIETY TO GENERATE ENCRYPTED HOST TELEMETRY
580
TRANSMITTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOST TELEMETRY TO A HOST TELEMETRY TRANSMITTER
585
TRANSMITTING, BY THE HOST TELEMETRY TRANSMITTER, THE ENCRYPTED HOST TELEMETRY TO THE HOST SOC
590
DECRYPTING, BY THE HOST SOC, THE ENCRYPTED HOST TELEMETRY UTILIZING THE FIRST COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOST TELEMETRY
591
TRANSMITTING, BY THE PAYLOAD, TO THE SECOND COMMUNICATION SECURITY MODULE UNENCRYPTED HOSTED TELEMETRY
592
ENCRYPTING, BY THE SECOND COMMUNICATION SECURITY MODULE, THE UNENCRYPTED HOSTED TELEMETRY UTILIZING THE SECOND COMSEC VARIETY TO GENERATE ENCRYPTED HOSTED TELEMETRY
593
TRANSMITTING, BY THE SECOND COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOSTED TELEMETRY TO A HOSTED TELEMETRY TRANSMITTER
594
TRANSMITTING, BY THE HOSTED TELEMETRY TRANSMITTER, THE ENCRYPTED HOSTED TELEMETRY TO THE HOST SOC
595
TRANSMITTING, BY THE HOST SOC, THE ENCRYPTED HOSTED TELEMETRY TO THE HOC
596

FIG. 5D


DECRYPTING, BY THE HOC, THE ENCRYPTED HOSTED TELEMETRY UTILIZING THE SECOND COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOSTED TELEMETRY
597
END
598

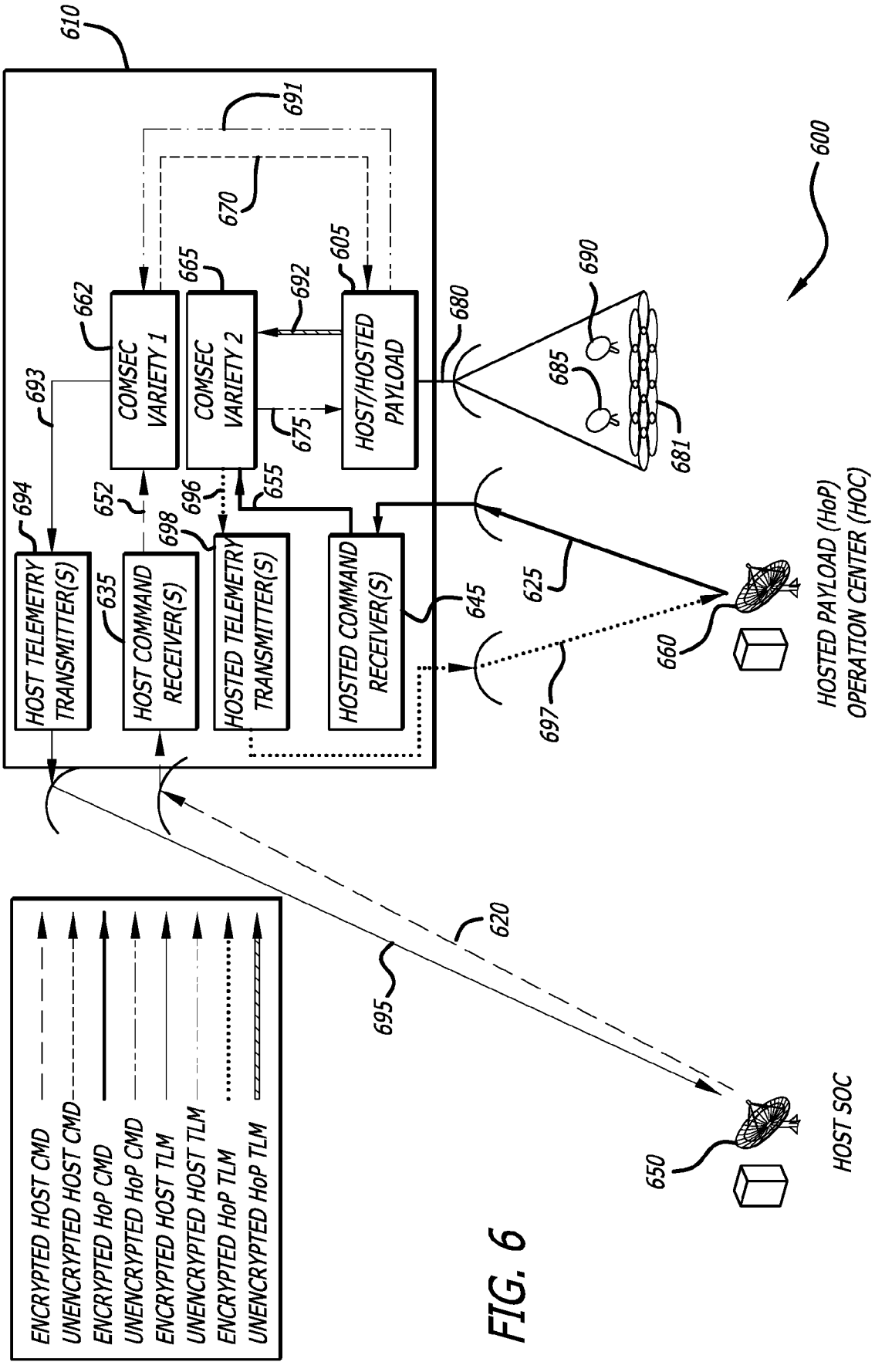

610
600
691
670
605
665
692
662
680
690
693
COMSEC VARIETY 1
COMSEC VARIETY 2
HOST/HOSTED PAYLOAD
685
675
681
694
652
696
655
698
HOST TELEMETRY TRANSMITTER(S)
HOST COMMAND RECEIVER(S)
HOSTED TELEMETRY TRANSMITTER(S)
HOSTED COMMAND RECEIVER(S)
635
645
625
660
697
HOSTED PAYLOAD (HoP) OPERATION CENTER (HOC)
620
695
650
HOST SOC
ENCRYPTED HOST CMD
UNENCRYPTED HOST CMD
ENCRYPTED HoP CMD
UNENCRYPTED HoP CMD
ENCRYPTED HOST TLM
UNENCRYPTED HOST TLM
ENCRYPTED HoP TLM
UNENCRYPTED HoP TLM

FIG. 6

FIG. 7A

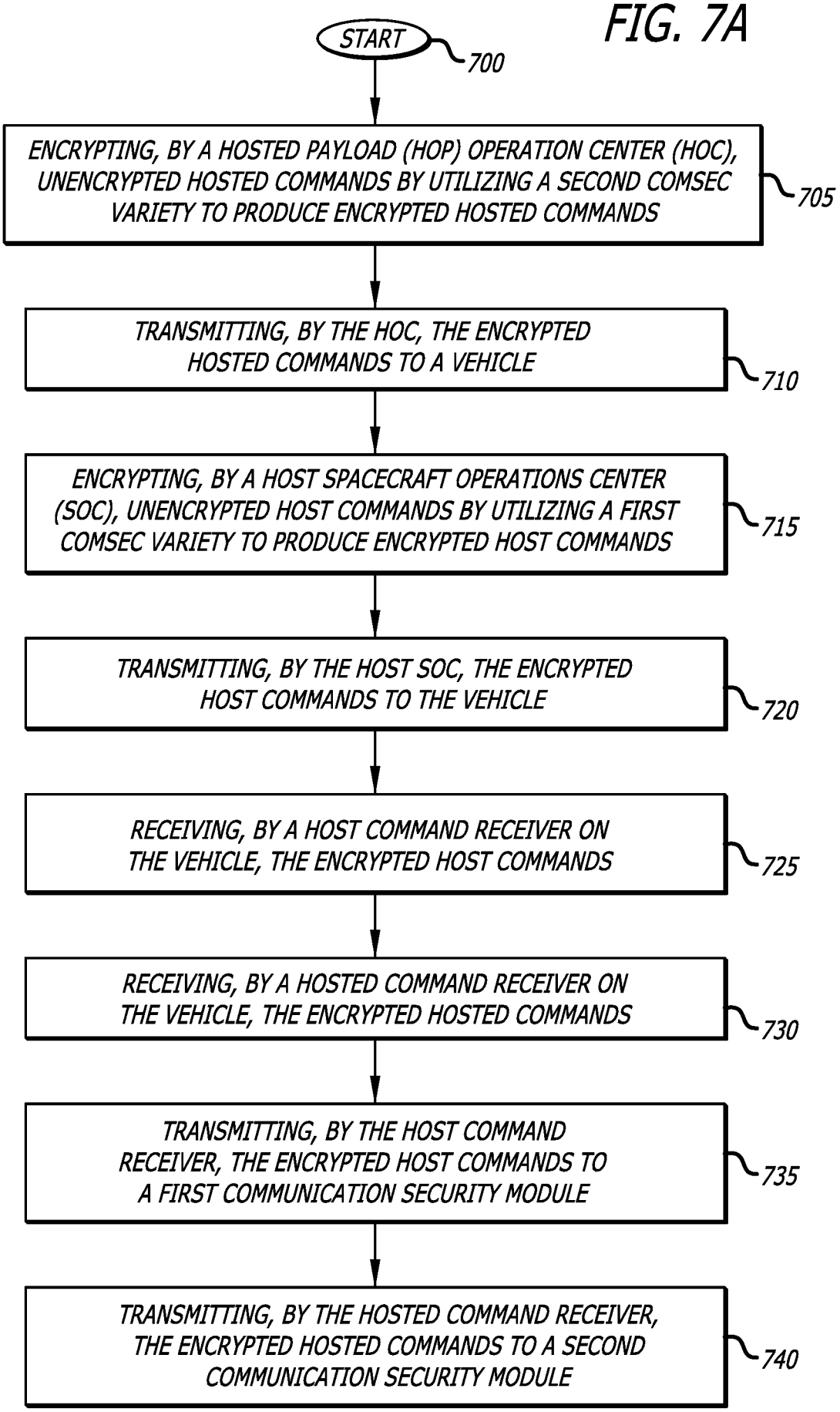

START
700
ENCRYPTING, BY A HOSTED PAYLOAD (HOP) OPERATION CENTER (HOC), UNENCRYPTED HOSTED COMMANDS BY UTILIZING A SECOND COMSEC VARIETY TO PRODUCE ENCRYPTED HOSTED COMMANDS
705
TRANSMITTING, BY THE HOC, THE ENCRYPTED HOSTED COMMANDS TO A VEHICLE
710
ENCRYPTING, BY A HOST SPACECRAFT OPERATIONS CENTER (SOC), UNENCRYPTED HOST COMMANDS BY UTILIZING A FIRST COMSEC VARIETY TO PRODUCE ENCRYPTED HOST COMMANDS
715
TRANSMITTING, BY THE HOST SOC, THE ENCRYPTED HOST COMMANDS TO THE VEHICLE
720
RECEIVING, BY A HOST COMMAND RECEIVER ON THE VEHICLE, THE ENCRYPTED HOST COMMANDS
725
RECEIVING, BY A HOSTED COMMAND RECEIVER ON THE VEHICLE, THE ENCRYPTED HOSTED COMMANDS
730
TRANSMITTING, BY THE HOST COMMAND RECEIVER, THE ENCRYPTED HOST COMMANDS TO A FIRST COMMUNICATION SECURITY MODULE
735
TRANSMITTING, BY THE HOSTED COMMAND RECEIVER, THE ENCRYPTED HOSTED COMMANDS TO A SECOND COMMUNICATION SECURITY MODULE
740

FIG. 7B

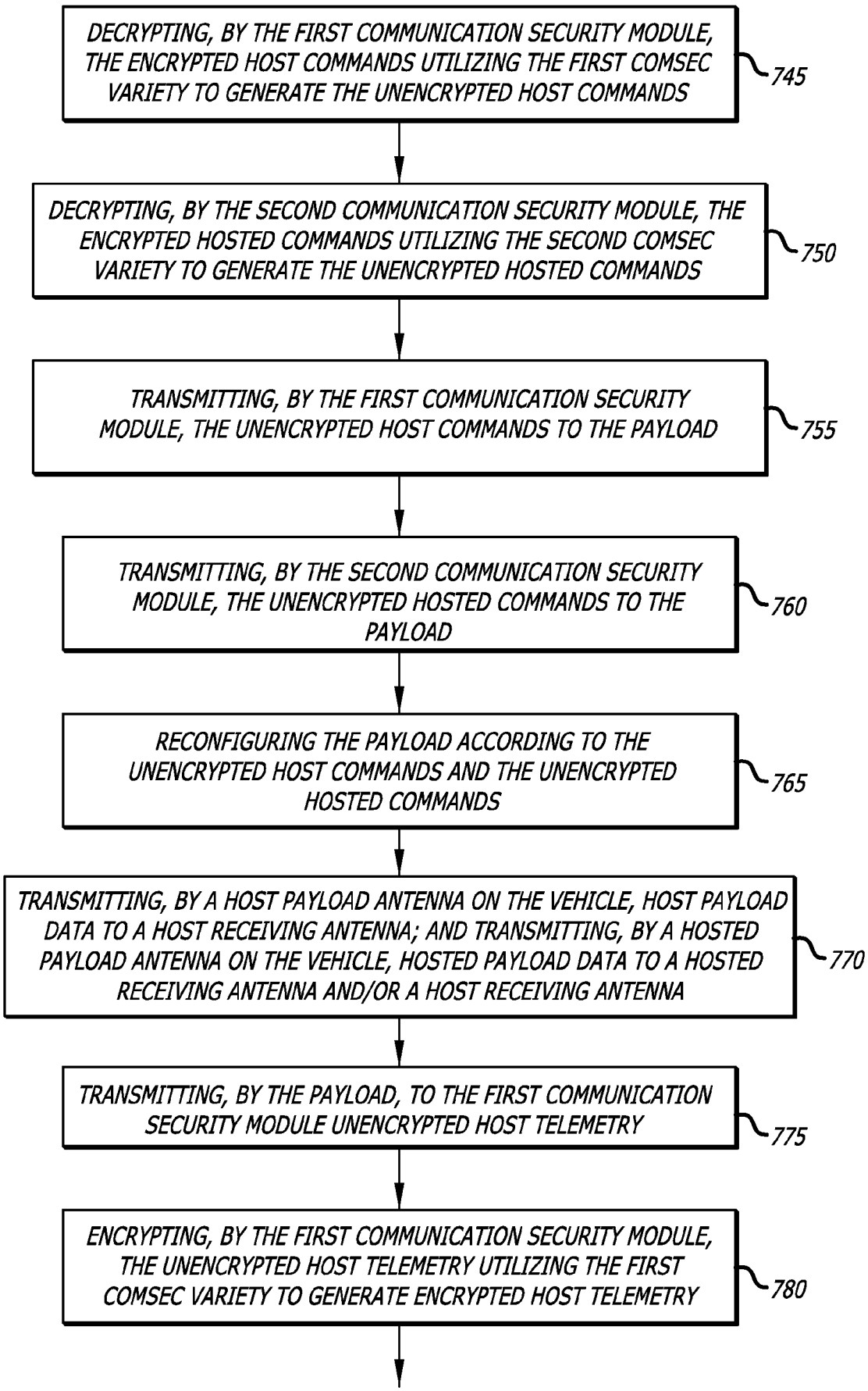
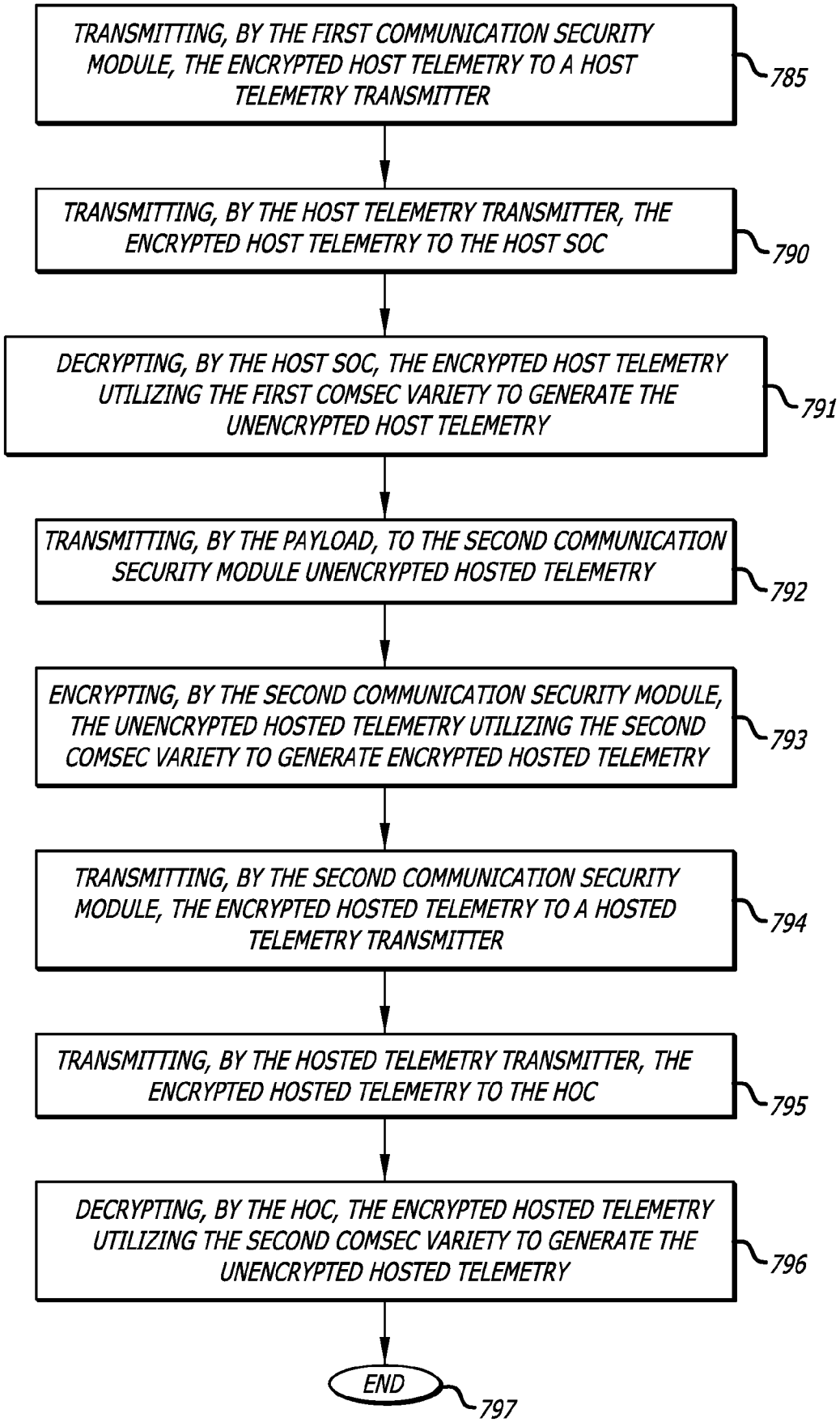

DECRYPTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOST COMMANDS UTILIZING THE FIRST COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOST COMMANDS
745
DECRYPTING, BY THE SECOND COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOSTED COMMANDS UTILIZING THE SECOND COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOSTED COMMANDS
750
TRANSMITTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE UNENCRYPTED HOST COMMANDS TO THE PAYLOAD
755
TRANSMITTING, BY THE SECOND COMMUNICATION SECURITY MODULE, THE UNENCRYPTED HOSTED COMMANDS TO THE PAYLOAD
760
RECONFIGURING THE PAYLOAD ACCORDING TO THE UNENCRYPTED HOST COMMANDS AND THE UNENCRYPTED HOSTED COMMANDS
765
TRANSMITTING, BY A HOST PAYLOAD ANTENNA ON THE VEHICLE, HOST PAYLOAD DATA TO A HOST RECEIVING ANTENNA; AND TRANSMITTING, BY A HOSTED PAYLOAD ANTENNA ON THE VEHICLE, HOSTED PAYLOAD DATA TO A HOSTED RECEIVING ANTENNA AND/OR A HOST RECEIVING ANTENNA
770
TRANSMITTING, BY THE PAYLOAD, TO THE FIRST COMMUNICATION SECURITY MODULE UNENCRYPTED HOST TELEMETRY
775
ENCRYPTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE UNENCRYPTED HOST TELEMETRY UTILIZING THE FIRST COMSEC VARIETY TO GENERATE ENCRYPTED HOST TELEMETRY
780

FIG. 7C


TRANSMITTING, BY THE FIRST COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOST TELEMETRY TO A HOST TELEMETRY TRANSMITTER
785
TRANSMITTING, BY THE HOST TELEMETRY TRANSMITTER, THE ENCRYPTED HOST TELEMETRY TO THE HOST SOC
790
DECRYPTING, BY THE HOST SOC, THE ENCRYPTED HOST TELEMETRY UTILIZING THE FIRST COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOST TELEMETRY
791
TRANSMITTING, BY THE PAYLOAD, TO THE SECOND COMMUNICATION SECURITY MODULE UNENCRYPTED HOSTED TELEMETRY
792
ENCRYPTING, BY THE SECOND COMMUNICATION SECURITY MODULE, THE UNENCRYPTED HOSTED TELEMETRY UTILIZING THE SECOND COMSEC VARIETY TO GENERATE ENCRYPTED HOSTED TELEMETRY
793
TRANSMITTING, BY THE SECOND COMMUNICATION SECURITY MODULE, THE ENCRYPTED HOSTED TELEMETRY TO A HOSTED TELEMETRY TRANSMITTER
794
TRANSMITTING, BY THE HOSTED TELEMETRY TRANSMITTER, THE ENCRYPTED HOSTED TELEMETRY TO THE HOC
795
DECRYPTING, BY THE HOC, THE ENCRYPTED HOSTED TELEMETRY UTILIZING THE SECOND COMSEC VARIETY TO GENERATE THE UNENCRYPTED HOSTED TELEMETRY
796
END
797

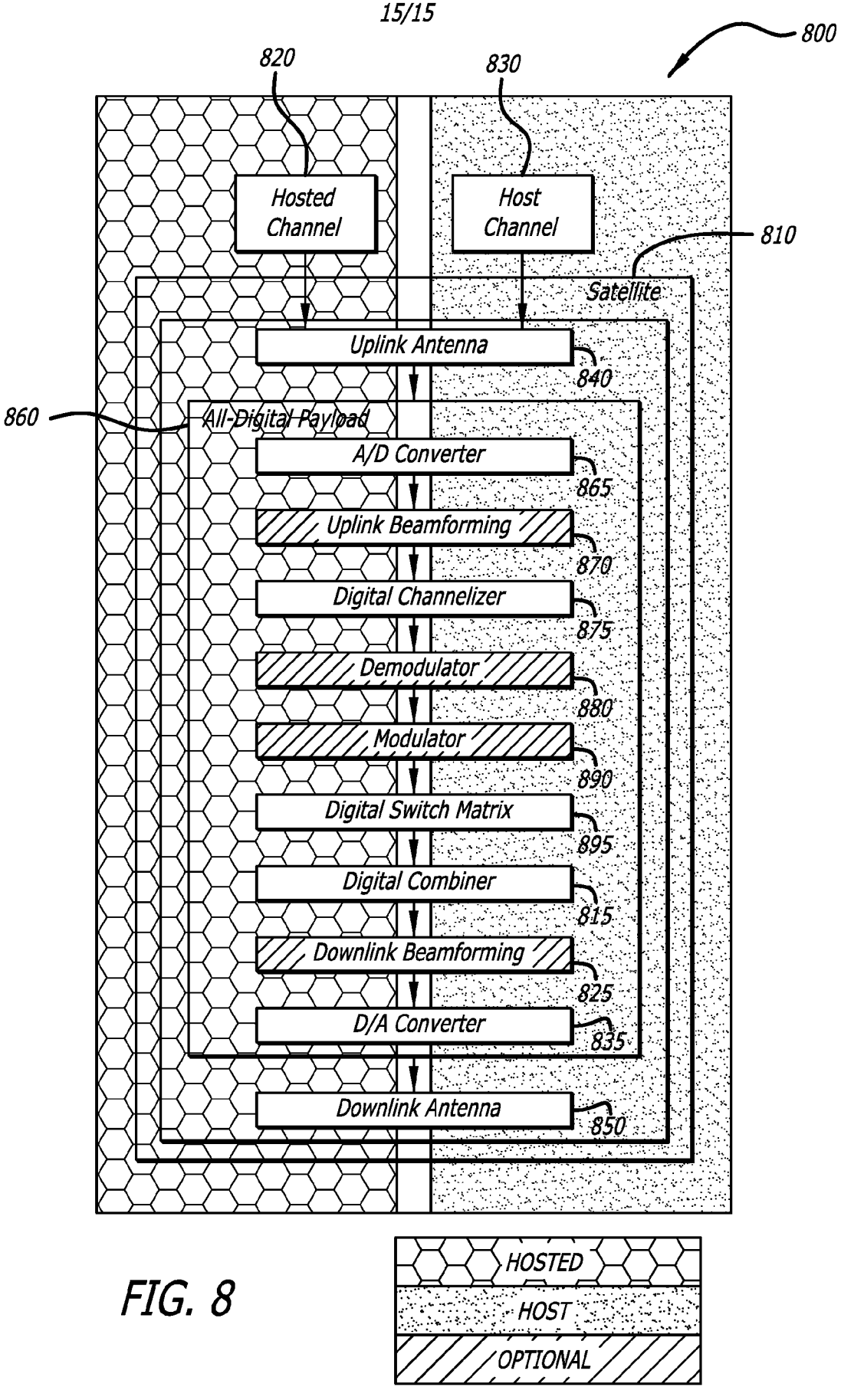

800
820
830
Hosted Channel
Host Channel
810
Satellite
Uplink Antenna
840
860
All-Digital Payload
A/D Converter
865
Uplink Beamforming
870
Digital Channelizer
875
Demodulator
880
Modulator
890
Digital Switch Matrix
895
Digital Combiner
815
Downlink Beamforming
825
D/A Converter
835
Downlink Antenna
850
HOSTED
HOST
OPTIONAL

FIG. 8

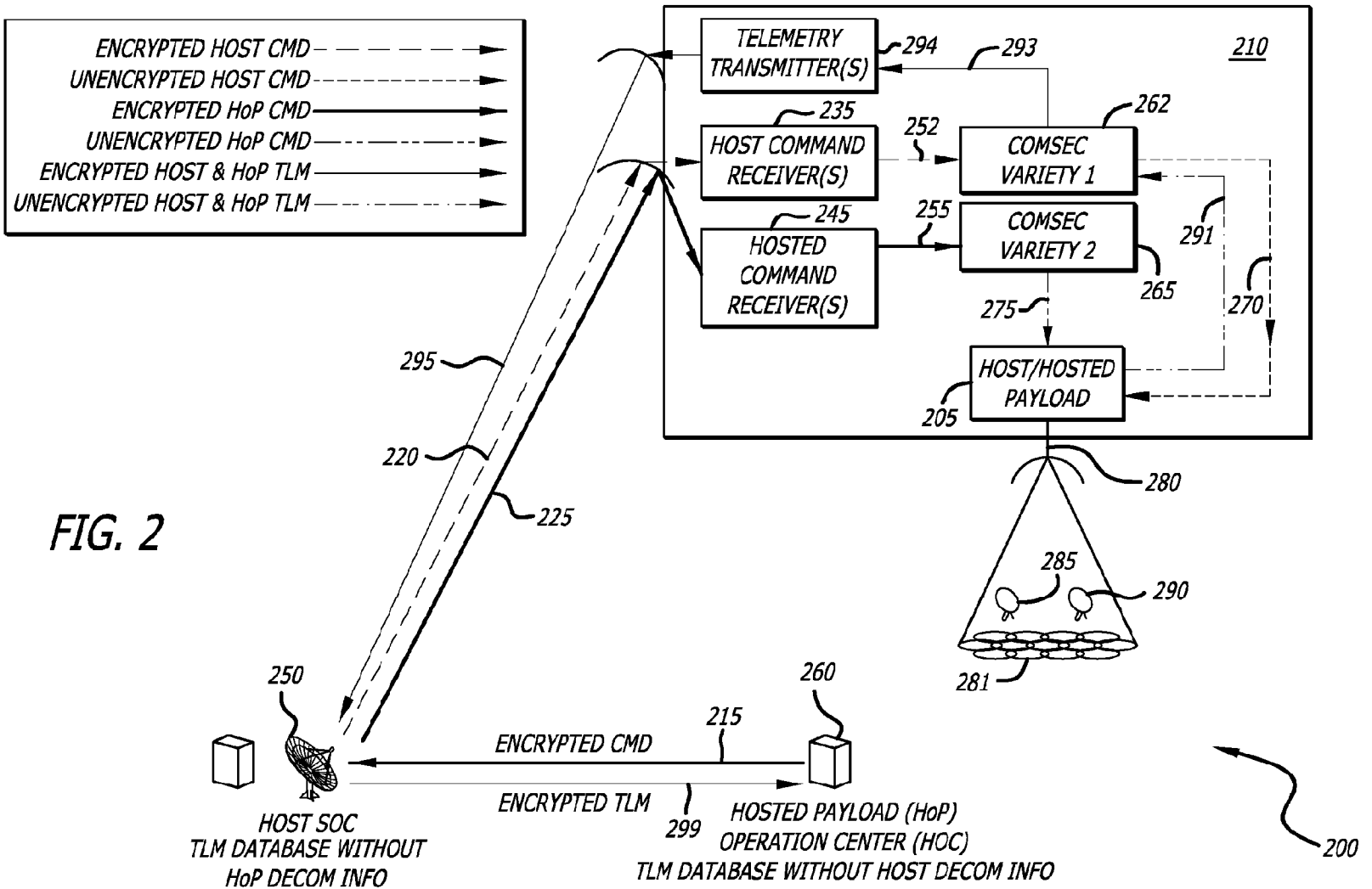

ENCRYPTED HOST CMD
UNENCRYPTED HOST CMD
ENCRYPTED HoP CMD
UNENCRYPTED HoP CMD
ENCRYPTED HOST & HoP TLM
UNENCRYPTED HOST & HoP TLM
TELEMETRY TRANSMITTER(S)
294
293
210
235
HOST COMMAND RECEIVER(S)
252
262
COMSEC VARIETY 1
245
HOSTED COMMAND RECEIVER(S)
255
COMSEC VARIETY 2
291
265
270
275
HOST/HOSTED PAYLOAD
205
295
220
225
280
285
290
281
250
260
215
ENCRYPTED CMD
ENCRYPTED TLM
299
HOST SOC
TLM DATABASE WITHOUT
HoP DECOM INFO
HOSTED PAYLOAD (HoP)
OPERATION CENTER (HOC)
TLM DATABASE WITHOUT HOST DECOM INFO
200

FIG. 2