	144	20060101507	A1	2006-05-11	Camenisch, Ja L.	
	145	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
	146	20060114821	A1	2006-06-01	Willey et al.	
	147	20060114832	A	2006-06-01	Hamilton et al.	
	148	20060126562	A1	2006-06-15	Liu, Huitao	
	149	20060135144	A	2006-06-22	Jothipragasam, Premkumar	
	150	20060136882	A1	2006-06-22	Noonan et al.	
	151	20060143066	A1	2006-06-29	Calabria	
	152	20060143098		2006-06-29	LAZARIDIS, Mihal	
	153	20060156398	A	2006-07-13	Ross et al.	
	154	20060160536	A	2006-07-20	Chou, Joey	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	155	20060165060		2006-07-27	DUA, Robin	
	156	20060168128	A	2006-07-27	Sistla et al.	
	157	20060173959	A	2006-08-03	Mckelvie et al.	
	158	20060174035	A	2006-08-03	Tufail, Mudassir	
	159	20060178917		2006-08-10	MERRIAM et al.	
	160	20060178918		2006-08-10	MIKURAK, Michael G.	
	161	20060182137	A1	2006-08-17	Zhou et al.	
	162	20060183462		2006-08-17	KOLEHMAINEN, Mikko	
	163	20060190314		2006-08-24	HERNANDEZ, Rick	
	164	20060190987	A1	2006-08-24	Ohta et al.	
	165	20060193280	A1	2006-08-31	Lee et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	166	20060199608		2006-09-07	DUNN et al.	
	167	20060200663	A1	2006-09-07	Thornton, Andrew J.	
	168	20060206709	A1	2006-09-14	Labrou et al.	
	169	20060206904		2006-09-14	WATKINS et al.	
	170	20060218395		2006-09-28	MAES, Stephane H.	
	171	20060233108		2006-10-19	KRISHNAN, Murali R.	
	172	20060233166		2006-10-19	BOU-DIAB et al.	
	173	20060236095		2006-10-19	SMITH et al.	
	174	20060242685		2006-10-26	HEARD et al.	
	175	20060258341		2006-11-16	MILLER et al.	
	176	20060274706	A1	2006-12-07	Chen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	177	20060277590	A1	2006-12-07	Limont et al.	
	178	20060291419	A1	2006-12-28	McConnell et al.	
	179	20060291477		2006-12-28	CROAK et al.	
	180	20070005795	A1	2007-01-04	Gonzalez, Ruben	
	181	20070019670		2007-01-25	FALARDEAU, Eric	
	182	20070022289		2007-01-25	ALT et al.	
	183	20070025301	A	2007-02-01	Petersson et al.	
	184	20070033194	A	2007-02-08	Srinivas et al.	
	185	20070033197	A	2007-02-08	Scherzer, Shimon et al.	
	186	20070035390	A1	2007-02-15	Thomas et al.	
	187	20070036312		2007-02-15	CAI et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	188	20070055694		2007-03-08	RUGE et al.	
	189	20070060200	A1	2007-03-15	Boris et al.	
	190	20070061243	A1	2007-03-15	Ramer et al.	
	191	20070061800	A1	2007-03-15	Cheng et al.	
	192	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	193	20070073899	A1	2007-03-29	Judge et al.	
	194	20070076616		2007-04-05	NGO et al.	
	195	20070093243		2007-04-26	KAPADEKAR et al.	
	196	20070100981		2007-05-03	ADAMCZYK et al.	
	197	20070101426		2007-05-03	LEE et al.	
	198	20070104126		2007-05-10	CALHOUN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	199	20070104169	A1	2007-05-10	Poison	
	200	20070109983	A	2007-05-17	Shankar, Rohit et al.	
	201	20070111740	A1	2007-05-17	Wandel	
	202	20070130283	A1	2007-06-07	Klein et al.	
	203	20070130315	A1	2007-06-07	Friend et al.	
	204	20070140113	A1	2007-06-21	Gemelos	
	205	20070140145	A	2007-06-21	Kumar et al.	
	206	20070140275		2007-06-21	BOWMAN et al.	
	207	20070143824	A1	2007-06-21	Shahbazi, Majid	
	208	20070147317	A	2007-06-28	Smith et al.	
	209	20070147324		2007-06-28	McGary, Faith	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	210	20070155365	A	2007-07-05	Kim, Sung-Jun et al.	
	211	20070165630	A1	2007-07-19	Rasanen et al.	
	212	20070168499	A	2007-07-19	Chu, Jing-Long	
	213	20070171856	A1	2007-07-26	Bruce et al.	
	214	20070174490	A1	2007-07-26	Choi et al.	
	215	20070191006	A1	2007-08-16	Carpenter	
	216	20070192460	A1	2007-08-16	Choi et al.	
	217	20070198656		2007-08-23	MAZZAFERRI et al.	
	218	20070201502	A1	2007-08-30	Abramson, Nathan	
	219	20070213054	A1	2007-09-13	Han, Seung-Wook	
	220	20070220251		2007-09-20	ROSENBERG et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	221	20070226225		2007-09-27	YIU et al.	
	222	20070226775	A	2007-09-27	Andreasen et al.	
	223	20070234402	A1	2007-10-04	Khosravi et al.	
	224	20070243862		2007-10-18	COSKUN et al.	
	225	20070248100	A1	2007-10-25	Zuberi et al.	
	226	20070254646	A1	2007-11-01	Sokondar	
	227	20070254675		2007-11-01	ZORLU OZER et al.	
	228	20070255769	A1	2007-11-01	Agrawal et al.	
	229	20070255797	A1	2007-11-01	Dunn et al.	
	230	20070255848		2007-11-01	SEWALL et al.	
	231	20070257767	A1	2007-11-08	Beeson, Curt	

	232	20070259656	A	2007-11-08	Jeong, Jong Woo	
	233	20070259673		2007-11-08	WILLARS et al.	
	234	20070263558		2007-11-15	SALOMONE, Leonardo	
	235	20070266422	A1	2007-11-15	Germano et al.	
	236	20070274327		2007-11-29	KAARELA et al.	
	237	20070280453		2007-12-06	Kelley, Sean S.	
	238	20070282896		2007-12-06	WYDROUG et al.	
	239	20070293191	A1	2007-12-20	Mir et al.	
	240	20070294395		2007-12-20	STRUB et al.	
	241	20070294410	A1	2007-12-20	Pandya et al.	
	242	20070297378	A1	2007-12-27	Poyhonen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	243	20070298764		2007-12-27	CLAYTON, Steve	
	244	20070299965	A1	2007-12-27	Nieh et al.	
	245	20070300252		2007-12-27	Acharya, Swarup et al.	
	246	20080005285		2008-01-03	ROBINSON et al.	
	247	20080005561		2008-01-03	BROWN et al.	
	248	20080010379	A	2008-01-10	Zhao, Hang	
	249	20080010452		2008-01-10	HOLTZMAN et al.	
	250	20080018494	A1	2008-01-24	Waite et al.	
	251	20080020738	A1	2008-01-24	Ho et al.	
	252	20080022354	A	2008-01-24	Grewal, Karanvir et al.	
	253	20080025230	A	2008-01-31	Patel et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	254	20080032715	A1	2008-02-07	Jia et al.	
	255	20080034063	A1	2008-02-07	Yee, Robert	
	256	20080034419	A	2008-02-07	Mullick et al.	
	257	20080039102		2008-02-14	SEWALL et al.	
	258	20080049630		2008-02-28	KOZISEK et al.	
	259	20080050715	A1	2008-02-28	Golczewski et al.	
	260	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	261	20080052387		2008-02-28	HEINZ et al.	
	262	20080056273	A	2008-03-06	Pelletier et al.	
	263	20080059474		2008-03-06	LIM, Keng	
	264	20080059743		2008-03-06	BYCHKOV et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	265	20080060066		2008-03-06	WYNN et al.	
	266	20080062900		2008-03-13	RAO, Bindu Rama	
	267	20080064367		2008-03-13	NATH et al.	
	268	20080066149		2008-03-13	LIM, Keng	
	269	20080066150		2008-03-13	LIM, Keng	
	270	20080066181	A1	2008-03-13	Haveson et al.	
	271	20080070550	A	2008-03-20	Hose, David Alan	
	272	20080077705	A1	2008-03-27	Li et al.	
	273	20080080457	A1	2008-04-03	Cole, Terry L.	
	274	20080081606		2008-04-03	COLE, Terry L.	
	275	20080082643		2008-04-03	STORRIE et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	276	20080083013		2008-04-03	SOLIMAN et al.	
	277	20080085707		2008-04-10	FADELL, Tony	
	278	20080089295	A	2008-04-17	Keeler, James D. et al.	
	279	20080089303	A1	2008-04-17	Wirtanen et al.	
	280	20080095339		2008-04-24	ELLIOTT et al.	
	281	20080096559	A1	2008-04-24	Phillips et al.	
	282	20080098062		2008-04-24	BALIA, Hinal K.	
	283	20080109679		2008-05-08	WRIGHT et al.	
	284	20080120129	A	2008-05-22	Seubert et al.	
	285	20080120174	A1	2008-05-22	Li	
	286	20080120668		2008-05-22	Yau, Frank Chuen-Foo	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	287	20080120688		2008-05-22	QIU et al.	
	288	20080125079	A1	2008-05-29	O'Neil et al.	
	289	20080126287	A1	2008-05-29	Cox et al.	
	290	20080127304	A1	2008-05-29	Ginter et al.	
	291	20080130534		2008-06-05	TOMIOKA, Tazuko	
	292	20080130656		2008-06-05	KIM et al.	
	293	20080132201		2008-06-05	KARLBERG, Johan	
	294	20080132268	A1	2008-06-05	Choi-Grogan et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		☐

EFS Web 2.1.18

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	2	101035308	CN	A	2006-03-09	Huawei Tech. Co. Ltd.		☐
	3	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		☐
	4	101115248	CN	A	2008-01-30	Lenovo Beijing Ltd.		☐
	5	101123553	CN	A	2007-09-11	SouTheast University		☐
	6	101127988	CN	A	2008-02-20	ZTE Corporation		☐
	7	101155343	CN	B	2006-09-29	Huawei Tech. Co. Ltd.		☐
	8	101183958	CN	A	2008-05-21	Huawei Tech. Co. Ltd.		☐
	9	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.		☐
	10	101341764	CN	A	2009-01-07	Telefonaktiebolaget LM Ericsson		☐
	11	101815275	CN	A	2010-08-25	Yang, Liu		☐
	12	1310401	CN	A	2001-08-29	Wang, Di Xing		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	13	1345154A	CN		2002-04-17	Datang Microelectronics Tech. Co.		☐
	14	1508734	CN	A	2004-06-30	Chinese Creative Corp.		☐
	15	1538730	CN	A	2004-10-20	Zhongxing Communication Co., Ltd.		☐
	16	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.		☐
	17	1801829	CN	A	2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		☐
	18	1802839	CN	A	2006-07-12	Motorola Inc.		☐
	19	1867024	CN	A	2006-11-22	Huawei Technologies Co., Ltd.		☐
	20	1878160	CN	A	2006-12-13	Huawei Technologies Co., Ltd.		☐
	21	1889777	CN	A	2006-07-19	Huawei Tech. Co. Ltd.		☐
	22	1937511	CN	A	2007-03-28	ZTE		☐
	23	1098490	EP	A2	2001-05-09	Nortel Networks Ltd.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	24	1289326	EP	A1	2003-03-05	Motorola, Inc.		☐
	25	1463238	EP		2004-09-29	Alcatel		☐
	26	1503548	EP	A1	2005-02-02	FG Microtec GmbH		☐
	27	1545114	EP	A1	2005-06-22	Alcatel		☐
	28	1739518	EP		2007-01-03	Research In Motion Limited		☐
	29	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		☐
	30	1850575	EP	A1	2007-10-31	Research In Motion		☐
	31	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		☐
	32	1942698	EP	A1	2008-07-09	Apple Inc.		☐
	33	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		☐
	34	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	35	2026514	EP	A1	2009-02-18	Nokia Siemens Networks		☐
	36	2005339247	JP	A	2005-12-08	Secured Communications		☐
	37	2006041989	JP		2006-02-09	Fujitsu Ltd.		☐
	38	2006155263	JP	A	2006-06-15	NEC Corporation		☐
	39	2006197137	JP		2006-07-27	NTT Docomo Inc.		☐
	40	2006344007	JP	A	2006-12-21	Hitachi Ltd.		☐
	41	2007318354	JP	A	2007-12-06	Fujitsu Ten Ltd.		☐
	42	2008301121	JP	A	2008-12-11	Kyocera Corp.		☐
	43	2009111919	JP		2009-05-21	Kyocera Communications Systems		☐
	44	2009212707	JP	A	2009-09-17	Fujitsu Ltd.		☐
	45	2009218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	46	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		☐
	47	3148713	JP	B2	2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		☐
	48	20040053858	KR	A	2004-06-25	Electronics and Telecommunications Research Instit		☐
	49	0208863	WO		2002-01-31	Telemac Corp.		☐
	50	1998058505	WO		1998-12-23	Sonera Oy		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[6]
	1	"Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	☐
	2	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐
	3	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐
	4	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	5	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	☐
	6	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐
	7	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	☐
	8	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	☐
	9	Accuris Networks, "The Business Value of Mobile Data Offload -- a White Paper", 2010	☐
	10	Ahmed et al., "A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and Its Performance," BenQ Mobile, Munich Germany; University of Klagenfurt, Klagenfurt, Austria; 2006	☐
	11	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	☐
	12	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	☐
	13	Android Cupcake excerpts, The Android Open Source Project, Feb. 10, 2009	☐
	14	ANTON, B. et al., "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming"; Release Date February 2003, Version 1.0; Wi-Fi Alliance -- Wireless ISP Roaming (WISPr)	☐
	15	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	16	BYRD, "Open Secure Wireless," May 5, 2010	☐
	17	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	☐
	18	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	☐
	19	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	☐
	20	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	☐
	21	DIKAIAKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	☐
	22	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	☐
	23	Droid Wall 1.3.7 description 20100428 obtained from https://www.freewarelovers.com/android/apps/droid-wall	☐
	24	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	☐
	25	European Commission, "Data Roaming Tariffs - Transparency Measures," obtained from EUROPA - Europe's Information Society Thematic Portal website, June 24, 2011: "http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm."	☐
	26	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	27	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	☐
	28	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	☐
	29	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	☐
	30	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	☐
	31	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	☐
	32	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	☐
	33	Kasper et al., "Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted Computing," Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany; ICACT 2008	☐
	34	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	☐
	35	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	☐
	36	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	☐
	37	Koutsopoulou et al., "Charging, Accounting and Billing Management Schemes in Mobile Telecommunication Networks and the Internet," IEEE Communications Surveys & Tutorials, First Quarter 2004, Vol. 6, No. 1	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	38	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	☐
	39	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	☐
	40	KYRIAKAKOS et al., "Ubiquitous Service Provision in Next Generation Mobile Networks," Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004	☐
	41	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	☐
	42	Loopt User Guide, metroPCS, 7/17/2008	☐
	43	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	☐
	44	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	☐
	45	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	☐
	46	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	☐
	47	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	☐
	48	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

	49	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	☐
	50	Richtel, "Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition]," National Post, Canada, Oct. 2, 2007	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17867585
	Filing Date	2022-07-18
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	NOT ASSIGNED YET
	Attorney Docket Number	P025C1C1C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2023-01-09
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	47342152
Application Number:	17867585
International Application Number:	
Confirmation Number:	5955
Title of Invention:	Security Techniques for Device Assisted Services
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Michael Farjami/Evan Gunderman
Filer Authorized By:	Michael Farjami
Attorney Docket Number:	RALEP025C1C1C1C1C1
Receipt Date:	09-JAN-2023
Filing Date:	18-JUL-2022
Time Stamp:	18:01:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P025C1C1C1C1C1_IDS1_Jan_9_23.pdf	215731 05e6a5371eecde2e821bc142378f9b2b36d32bac	no	40

Warnings:

Information:	
This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	215731

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/867,585	07/18/2022	Gregory G. Raleigh	RALEP025C1C1C1C1C1

CONFIRMATION NO. 5955

106963
Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

PUBLICATION NOTICE

OC000000136752648

Title: Security Techniques for Device Assisted Services

Publication No.US-2022-0353301-A1
Publication Date:11/03/2022

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/867,585	07/18/2022		830	RALEP025C1C1C1C1C1	1	1

CONFIRMATION NO. 5955

FILING RECEIPT

OC000000135457820

106963
Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

Date Mailed: 07/28/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Gregory G. Raleigh, Tyler, TX;

Applicant(s)

Headwater Research LLC, Tyler, TX;

Assignment For Published Patent Application

Headwater Research LLC, Tyler, TX

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 16/907,887 06/22/2020 PAT 11405429
which is a CON of 16/034,362 07/13/2018 PAT 10694385
which is a CON of 14/948,065 11/20/2015 PAT 10028144
which is a CON of 13/737,748 01/09/2013 PAT 9198042
which is a CON of 12/694,445 01/27/2010 PAT 8391834
which is a CIP of 12/380,780 03/02/2009 PAT 8839388
and claims benefit of 61/252,151 10/15/2009
and said 12/380,780 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 07/27/2022

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/867,585**

Projected Publication Date: 11/03/2022

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Security Techniques for Device Assisted Services

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 17/867,585

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	1 minus 20 =	*	x 50 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 240 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	830		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT A	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT A	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT A	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT B	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT B	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT B	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

Attorney Docket No.: RALEP025C1C1C1C1C1

PATENT APPLICATION COVER SHEET

MAIL STOP PATENT APPLICATION
COMMISSIONER FOR PATENTS
P.O. BOX 1450; ALEXANDRIA, VA 22313-1450

Transmitted herewith is the patent application of:

ASSIGNEE(S): **Headwater Research LLC**

Inventor(s): Gregory G. Raleigh

For: "Security Techniques for Device Assisted Services"

This application is a ☒ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: 16/907,887

Enclosed are:

☒ Eleven (11) Sheets of drawings

☐ Request for Non-Publication (Form PTO/SB/35 (11-00))

☐ Separate Payment Form PTO-2038 for $40.00 is Attached for Assignment of the invention to: _____

☐ The enclosed payment includes $_____ for the recording of the assignment

☒ Applicant Claims Small Entity Status

☐ Information Disclosure Statement

☒ Application Data Sheet PTO/AIA/14

☒ One (1) Declaration

☒ The filing fee has been calculated as shown below:

	(Col. 1)	(Col. 2)	SMALL ENTITY		OTHER THAN A SMALL ENTITY	
FOR:	No. Filed	No. Extra	RATE	FEE	RATE	FEE
BASIC FEE				$80.00		$320.00
SEARCH FEE				$350.00		$700.00
EXAMINATION FEE				$400.00		$800.00
APPLICATION SIZE FEE (Total Number of Sheets)	38/50=	0	x $210.00=	$	x $420.00=	$
TOTAL CLAIMS	1 -20 =	0	x $50.00=	$	x $100.00=	$
INDEPENDENT CLAIMS	1 -3 =	0	x $240.00=	$	x $480.00 =	$
SURCHARGE FOR LATE FILING OF DECLARATION			+ $80.00	$	+ $160.00 =	$
			TOTAL	$830.00	TOTAL	$

If the difference in Col. 1 is less than zero, enter "0" in Col. 2

☒ Enclosed is a payment in the amount of $830.00 by Credit Card.

☐ Please charge Deposit Account No. 50-0731 in the amount of $0.00.

☒ The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication, or credit any overpayment to Deposit Account No. 50-0731.

Date: July 18, 2022 /Farshad Farjami/

FARSHAD FARJAMI, ESQ.

Reg. No.: 41,014

Customer No.: 106963

Farshad Farjami, Esq.
FARJAMI & FARJAMI LLP

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being filed via EFS in United States Patent and Trademark Office, on the date stated below.

July 18, 2022
Date

Evan C. Gunderman /evan c. gunderman/
Name Signature

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP025C1C1C1C1C1
	Application Number	
Title of Invention	Security Techniques for Device Assisted Services	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Gregory	G.	Raleigh	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Incline Village	State/Province	NV	Country of Residence	US

Mailing Address of Inventor:

Address 1	110 North College Avenue		
Address 2	Suite 1116		
City	Tyler	State/Province	TX
Postal Code	75702	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	106963		
Email Address	patent@headwaterllc.com	Add Email	Remove Email

Application Information:

Title of the Invention	Security Techniques for Device Assisted Services		
Attorney Docket Number	RALEP025C1C1C1C1C1	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	11	Suggested Figure for Publication (if any)	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP025C1C1C1C1C1
	Application Number	

Title of Invention	Security Techniques for Device Assisted Services

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	106963		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
thisapplication	Continuation of	16907887	2020-06-22

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP025C1C1C1C1C1
	Application Number	

Title of Invention	Security Techniques for Device Assisted Services

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16907887	Continuation of	16034362	2018-07-13	10694385	2020-06-03
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16034362	Continuation of	14948065	2015-11-20	10028144	2018-07-17
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14948065	Continuation of	13737748	2013-01-09	9198042	2015-11-24
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13737748	Continuation of	12694445	2010-01-27	8391834	2013-03-05
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12694445	Continuation in part of	12380780	2009-03-02	8839388	2014-09-16

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12694445	Claims benefit of provisional	61252151	2009-10-15
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12380780	Claims benefit of provisional	61206354	2009-01-28
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12380780	Claims benefit of provisional	61206944	2009-02-04
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12380780	Claims benefit of provisional	61207393	2009-02-10

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP025C1C1C1C1C1
	Application Number	
Title of Invention	Security Techniques for Device Assisted Services	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12380780	Claims benefit of provisional	61207739	2009-02-13
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.			

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.			

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP025C1C1C1C1C1
	Application Number	
Title of Invention	Security Techniques for Device Assisted Services	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP025C1C1C1C1C1
	Application Number	

Title of Invention	Security Techniques for Device Assisted Services

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee ◯ Legal Representative under 35 U.S.C. 117 ◯ Joint Inventor

◯ Person to whom the inventor is obligated to assign. ◯ Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	Headwater Research LLC

Mailing Address Information For Applicant:

Address 1	110 North College Avenue		
Address 2	Suite 1116		
City	Tyler	**State/Province**	TX
Country	US	Postal Code	75702
Phone Number	903-201-6211	Fax Number	
Email Address	patent@headwaterllc.com		

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP025C1C1C1C1C1
	Application Number	

Title of Invention	Security Techniques for Device Assisted Services

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	Headwater Research LLC

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	110 North College Avenue		
Address 2	Suite 1116		
City	Tyler	**State/Province**	TX
Country i	US	Postal Code	75702
Phone Number	903-201-6211	Fax Number	
Email Address	patent@headwaterllc.com		

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Farshad Farjami/			Date (YYYY-MM-DD)	2022-07-18
First Name	Farshad	Last Name	Farjami	Registration Number	41014

Additional Signature may be generated within this form by selecting the Add button.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP025C1C1C1C1C1
	Application Number	
Title of Invention	Security Techniques for Device Assisted Services	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Gregory G. Raleigh Date (Optional) : _____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

BACKGROUND OF THE INVENTION

[0001] With the advent of mass market digital communications, applications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), DOCSIS, DSL, and Wi-Fi (Wireless Fidelity) becoming user capacity constrained. In the wireless case, although network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum and cell splitting being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0002] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user compared to wireless, wire line user service consumption habits are trending toward very high bandwidth applications and content that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0004] FIG. 1 illustrates a secure execution environment for device assisted services in accordance with some embodiments.

[0005] FIG. 2 illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0006] FIG. 3 illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0007] FIG. 4 illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0008] FIG. 5 illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0009] FIG. 6 illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0010] FIG. 7 illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0011] FIG. 8 illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0012] FIG. 9 illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0013] FIG. 10 illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0014] FIG. 11 illustrates another secure execution environment for device assisted services in accordance with some embodiments.

DETAILED DESCRIPTION

[0015] The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term 'processor' refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0016] A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

[0017] In some embodiments, security techniques for device assisted services are provided. In some embodiments, secure service measurement and/or control execution partition techniques for device assisted services are provided. In some embodiments, a secure execution environment for device assisted services is provided. In some embodiments, a secure stack for device assisted services is provided. In some embodiments, a secure memory for device assisted services is provided. In some embodiments, a secure modem for device assisted services is

provided (e.g., providing a secure communication link between the modem/modem driver and a service processor and/or agent on the device, such as a communications device or an intermediate networking device). In some embodiments, one or more secure monitoring points for device assisted services are provided. In some embodiments, one or more secure monitoring points with verification for device assisted services are provided (e.g., a secured monitoring point can be provided in a modem, which communicates securely to a secured execution environment in a CPU/processor, which can then verify such service usage measures). In some embodiments, a secure bus for device assisted services is provided. In some embodiments, a secure execution environment in the CPU/processor for device assisted services is provided. In some embodiments, secure access to a secure execution environment(s) for device assisted services is provided (e.g., securing communication from a bottom of the stack, such as modem drivers, which require credentials to access the bus as controlled by a service processor or secure agent on the device, and in which the traffic on the bus is encrypted). In some embodiments, various secure execution environments for device assisted services are provided using various hardware partition techniques (e.g., secure memory, secure modems, secure memory partition(s) in the CPU/processor), as described herein.

[0018] In some embodiments, device assisted services (DAS) provide for one or more of device based service usage measurements, service usage policy implementation, service usage accounting, service usage control, and any of the other functions described in various embodiments that assist, replace, and/or augment network based functions. For example, various DAS embodiments perform one or more of the following: facilitate and control activation to one or more access service networks; measure access and/or service usage on one or more access networks; control access and/or service usage on one or more access networks; account for different types of service usage on one or more access networks; implement quality of service (QOS) controls, collect and report QOS traffic demand, aggregate multiple device QOS demand reports to asses a measure of overall network QOS demand, and/or facilitate QOS resource allocation; and/or facilitate roaming between access networks. There are many more functions and embodiments for DAS as described with respect to various embodiments.

[0019] In some embodiments, various program/functional elements that perform the functions to implement various DAS embodiments are referred to herein as DAS agents or

device assisted service agents, or in some embodiments, more specific terms are used to be more descriptive in specific examples. In some embodiments, device assisted service agent functions include service measurements and/or service measure recording and/or service measure reporting (e.g., to the service controller, the device, the user, or other device agents) and/or service measure synchronization (e.g., between device and network). In some embodiments, device assisted service agent functions include service usage controls and/or service usage control policy settings. In some embodiments, service usage controls include one or more of network authorization, network authentication, network admission, access control, service usage activity classification, allowing or disallowing one or more service usage activity and traffic shaping for one or more service usage activity.

[0020] In some embodiments, device assisted service agent functions include one or more of the following: reporting service usage to QOS control elements in the network, receiving QOS assignment from the network, reporting QOS assignments to the network, and/or communicating with QOS service reservation elements in the network. In some embodiments, device assisted service agent functions include one or more of implementing QOS service controls on the device based on one or more of the following criteria: fair queuing of service usage activities, differentiated QOS based on an assigned QOS hierarchy of service usage activities, service usage activity QOS assignments from the network for one or more service usage activities, service usage activity policy directives from the network for one or more service usage activities.

[0021] In some embodiments, a service control link is used for communication between the device assisted service agents and the service controller. In some embodiments, the service control link is a secure link (e.g., an encrypted communication link).

[0022] In some embodiments, the device assisted service agent functions include device assisted service system communication, measuring and/or recording and/or reporting and/or synchronizing service measures, observing communicating information for service control integrity, communicating information for service control policy instructions and/or settings, or updating device assisted software and/or agent settings.

[0023] In some embodiments, device assisted service on the device includes the following: service measurements, service controls, user interface and usage reporting, user policy options, accept policy instructions, protected execution partition provided to prevent hacking, malware, errors, and other security techniques. In some embodiments, device assisted service on the server includes one or more of the following: set policy, set configurations, install/update agents, check usage versus policy, check proper operation of agents, synchronize usage from network to device, and other verification techniques. For example, when errors in policy enforcement are detected, servers can perform actions to either further observe, quarantine, or suspend the device.

[0024] In some embodiments, a control server/control service network element receives service measures from the device. In some embodiments, the control server/control service network element receives service measures from the network. In some embodiments, the control server/control service network element sets policies and manages service across multiple networks (e.g., while one modem is shown in various figures, multiple modems can be employed for multiple networks with consistent service usage measures, service controls, QOS controls, UI (User Interface), user preferences, user usage reporting, and/or other settings/controls across different networks).

[0025] In some embodiments, traffic type refers to one or more of the following: best effort network traffic, real-time traffic (e.g., live voice such as VOIP, live video, etc.), streaming traffic, multi-cast traffic, uni-cast traffic, point to point traffic, file types, traffic associated with an application, real time traffic, traffic with an assigned priority, traffic without an assigned priority, and traffic for a certain network.

[0026] In some embodiments, service usage activity refers to a usage of service by a device. In some embodiments, service usage activity can be one or more of connection to an access network, connection to certain destinations, URLs or addresses on a network, connection to the network by one or more applications, transmission of certain types of traffic, a type of transaction based service, a type of advertising based services, or a combination of one or more of the following: an application type, a network destination/address/URL, a traffic type, and a transaction type.

[0027] In some embodiments, protection of the device assisted service agents/functional elements to protect the functions that perform the device assisted functions is provided with a protected execution partition on the CPU (Central Processor Unit), APU (Auxiliary Processor Unit), or another hardware based processor. For example, such hardware protected execution capabilities in the CPU, APU, or other processor can be combined in some embodiments with either OS software functions or other native mode software functions to create secure program execution partitions as described herein. In some embodiments, the term host is used to refer to the hardware and firmware and/or software system that executes the device applications and networking stack. In some embodiments, some of the device assisted service agents/functions are implemented in a modem execution partition environment.

[0028] FIG. 1 illustrates a secure execution environment 100 (e.g., for a communications device) for device assisted services in accordance with some embodiments. As shown in FIG. 1, the device execution environments include program/functional elements for a communications (e.g., a communications device can be an intermediate networking device, such as 3G/4G WWAN to WLAN bridges/routers/gateways, femto cells, DOCSIS modems, DSL modems, remote access/backup routers, and other intermediate network devices, or a mobile communications device, such as a mobile phone, a PDA, an eBook reader, a music device, an entertainment/gaming device, a computer, laptop, a netbook, a tablet, a home networking system, and/or any other mobile communications device) device that utilizes the modem subsystems #1 (125) through #N (127) to connect to one or more of the access networks #1 (136) through #N (138). In some embodiments, a communications device includes multiple program execution partitions. As shown in FIG. 1, four execution partitions are provided: an application execution partition 102 in which, for example, application programs execute, a kernel execution partition 112 in which, for example, the lower level drivers and basic low level OS programs execute, a protected device assisted service (DAS) execution partition 114 (also referred to as protected DAS partition) in which, in some embodiments, some or all of the device assisted service agents and/or functions execute, and a modem execution partition 124 in which, for example, the modem program elements execute and, in some embodiments, some or all of the device assisted service agents and/or functions execute. In some embodiments, each of these execution partitions are optimized for different software functions, each providing programs with the basic physical memory, data memory, CPU or APU or modem processor execution resources, high

level and/or low level OS, memory management, file storage, I/O device resources (e.g., user interface (UI), peripherals, etc.), network communications stack, other device resources, and/or other resources that are required or used for operation of the programs. The collection of these hardware and software resources for the CPU or APU is sometimes referred to herein with the term host.

[0029] As shown, FIG. 1 illustrates an application execution partition 102 and a kernel execution partition 112, which are shown as separate partitions within the device execution environments. For example, this separation is based on the manner in which "kernel programs" (e.g., drivers and network stack, etc.) are commonly supported as compared to "application programs" (e.g., browsers, word processors, user interfaces, etc.) within the context of several different popular operating systems (OS) (e.g., Windows, UNIX, Linux, MAC OS, certain mobile device OSs, certain embedded device OSs, etc.). In some embodiments, this functional separation is not required, and, in some embodiments, other functional separations are supported.

[0030] As shown in FIG. 1, protected device assisted service agents, such as the protected DAS partition device assisted service agents 110, execute in the protected DAS partition 114 while unprotected device assisted service agents and/or OS networking stack elements and applications (e.g., applications 106A through 106C) execute outside of the secure device assisted service execution partition 114, such as the application partition device assisted service agents 104 and the OS networking stack and/or kernel partition device assisted service agents 108. For example, the protected DAS partition 114 can make it more difficult for a hacker, malware or system errors to compromise, attack or modify the device assisted service measurements, service policy implementation or service usage control operations on the device (e.g., communications device). In some embodiments, the protected DAS partition 114 need not support open access to all programs and OS elements so that it can be easier to protect. Also, as shown, a bus driver 116 in the application execution partition 102 provides for communication with a modem bus 120, which is in communication with a bus driver 121 in the modem execution partition 124. The protected DAS partition also includes a host service control link 118, which facilitates communication with a host secure channel 150 as shown.

[0031] In some embodiments, the protected DAS partition 114 is a protected execution partition on the main device that is supported by certain configurations in the host (e.g., a secure virtual execution environment or a separate hardware security function). For example, this protected execution partition can be used to provide added service measurement integrity and/or service control integrity for a device assisted service enabled device. In some embodiments, as described herein, the operating system (OS) also performs a role in establishing the protected execution partition for secure operation of device assisted services, and, in some embodiments, this role is performed by native software or firmware operating on secure hardware elements.

[0032] In some embodiments, the DAS agents responsible for maintaining service control integrity execute in the protected DAS partition 114. For example, the protected DAS partition device assisted service agents 110 can include one or more of the following: one or more service usage measurement functions; some or all of the device networking stack functions that are monitored and/or controlled by the device assisted services system; device drivers that interface to an OS networking stack to observe or manipulate stack traffic; access control integrity functions; service policy control functions; service UI functions; application identification functions, and/or functions to classify service usage activities by combinations of application, address/URL and/or traffic type; modem bus driver functions; and/or modem data encryption functions to prevent other unauthorized programs from bypassing the device assisted service measurements and/or controls by directly accessing the modem around the stack. In some embodiments, the system designer or a given set of design criteria determine which of the various described device assisted agent functions should be executed in protected DAS partition 114 to strengthen the service control integrity for the system.

[0033] In some embodiments, the device operating system provides for the protected DAS partition 114 in addition to conventional security features available in the operating system. In some embodiments, the protected DAS partition 114 provides an execution partition with increased program execution protection in which, for example, service measurement and/or service control programs (agents) can execute in a mode that provides for higher access control integrity (e.g., proper service usage reporting and/or service measurement and/or service control system operation with increased protection from attacks, errors, malware, etc.). In some

embodiments, a hardware assisted secure execution partition provides for increased program execution protection for device assisted service agent functions.

[0034] In some embodiments, a service control link (e.g., host service control link 118 via host secure channel 150 to network service control link 152) is used for communication between the device assisted service agents and a service controller 122. In some embodiments, the service control link is a secure link (e.g., an encrypted communications link). In some embodiments, an encrypted secure control link can be implemented over the higher layers of the network stack (e.g., TCP, HTTP, TLS, etc.), and, in some embodiments, the encrypted link can be implemented over lower layers in the network stack, such as the IP layer or the access network layers (e.g., the WWAN device management channels or signaling layers). In some embodiments, service control link security is provided at least in part by encrypting link traffic between the device and the service controller 122. In some embodiments, service control link security is provided at least in part by running the service control link device side program agents in the protected DAS partition 114. In some embodiments, service control link security is achieved at least in part by restricting access to the service control link to certain device assisted service agents that are allowed to communicate with the service controller 122. In some embodiments, the agents that are allowed to communicate with the service control link perform such communications using encrypted communications. In some embodiments, the encrypted communications is accomplished with a secure inter-agent communication bus on the device. In some embodiments, the only mechanism for modifying the configuration of the operation, execution code, execution instructions and/or settings of certain device assisted service processor agents executing in the protected DAS partition 114 is through the service control link. In some embodiments, the only mechanism for modifying any program elements executing inside the protected DAS partition 114 is through the service control link so that only the service controller 122 may modify the operation or service policy settings for the agents located in the service measurement and/or service control execution partition.

[0035] As shown in FIG. 1, various server functions within the service controller 122 are provided. In some embodiments, a service history server 158 collects service usage measures from one or more of the device DAS agents and/or from various sources of potential network based service usage databases, such as the access network service usage 142 (e.g., carrier

charging data record (CDR) systems), private network service usage 144 (e.g., MVNO or enterprise network service usage accounting system), and/or billing, mediation service usage log, reconciliation 148 (e.g., service provider billing or mediation system). In some embodiments, an access control integrity server 156 is used to compare various access control verification checks to ensure that the device assisted service agents have not been compromised. The various embodiments used in the access control integrity server 156 to perform these integrity checks are described with respect to various embodiments. Some embodiments include comparing device based service usage measures versus the service usage that should result if the desired service policy were properly implemented, comparing device based service usage measures versus the service usage that should result if the desired service policy were properly implemented with device based service usage measures that are executing in the protected DAS partition 114 and/or the modem execution partition 124, comparing network based service usage measures versus the service usage that should result if the desired service policy were properly implemented, and comparing network based service usage measures with device based service usage measures. In some embodiments, a policy control server 154 stores policy settings for the various service plans that can be implemented on the device, and communicates the appropriate policy settings to the appropriate device DAS agents.

[0036] In some embodiments, the service controller 122 has secure access to service measures, service control settings, software images, software security state(s), and/or other settings/functions, for example, by virtue of the hardware enhanced execution partition and the secure channel into the protected DAS partition 114. For example, the host secure channel 150 can be encrypted employing keys that are public/private or point to point private. Also, other link security, for example, can be implemented as described herein. For example, servers can ensure that the link remains authenticated and information is validated. For example, the service controller can perform one or more of the following verification techniques: compare the monitored service usage versus the policy, compare the monitored service usage versus other service usage measures and/or combined with various other network service usage measures.

[0037] In some embodiments, the protected DAS partition 114 includes a host service control link 118 as shown in FIG. 1 that works in combination, that is, in communication with a network service control link 152 to send and receive secure messages between the service

controller and the host via a host secure channel 150. In some embodiments, the protected DAS partition 114 only accepts new program images from the service controller 122 and not from local programs or disks. In some embodiments, the protected DAS partition 114 cannot communicate with other applications and/or kernel programs. In some embodiments, the protected DAS partition 114 can also communicate with other applications and/or kernel programs but only to gather information or to set settings. In some embodiments, the protected DAS partition 114 can also communicate with other applications and/or kernel programs but only through a restricted encrypted communication bus that restricts outside program access to protected programs or agent functions, and can also restrict the agents inside of the protected partition from accepting unauthorized information or code modifications from programs outside the protected partition. Various other security techniques can be provided for the DAS execution environments as will be apparent to one of ordinary skill in the art in view of the embodiments described herein.

[0038] In some embodiments, the protected DAS partition 114 is created by employing CPU or APU hardware security features in addition to or in alternative to other software security features (e.g., virtual execution partitions) that can be provided by the operating system and/or other software. In some embodiments, the host hardware security features are provided with the operating system secure kernel operating modes. In some embodiments, the host hardware security features used for secure device assisted service execution partition operation are independent of the operating system kernel (e.g., implemented in secure program partitions in a separate secure program area not directly controlled by the OS and/or software that does not have access to the partitions).

[0039] In some embodiments, the hardware security features that support the protected DAS partition 114 include preventing other elements on the device from writing and/or reading certain memory areas reserved for device assisted service agents and/or control link functions. In some embodiments, this memory protection function is accomplished by locating the memory in a secure hardware partition that cannot be accessed by unauthorized device program elements (e.g., a separate bank of isolated memory space within the host CPU). In some embodiments, this memory protection function includes encrypting traffic to and from memory so that only authorized device program elements posses the counterpart encryption capability to access the

memory. In some embodiments, the mechanism to access device assisted service agent memory and/or certain data elements is restricted to authorized device assisted service agents and/or the service controller via the service control link so that unauthorized program elements on the device cannot alter the device assisted service agent code and/or operation.

[0040] In some embodiments, the hardware security features that support the protected DAS partition 114 includes preventing unauthorized elements on the device from accessing the protected storage and/or file storage (e.g., "protected storage," such as disk storage, non-volatile memory, embedded non-volatile memory, such as NVRAM, flash or NVROM, securely embedded non-volatile memory, and/or other types of storage) that is used to store the device assisted service agent programs. In some embodiments, this protected storage is maintained within the secure hardware partitions that also execute one or more of the device assisted service agents so that only authorized device assisted service agents have access to the storage locations. In some embodiments, the images that are stored in such protected file storage must be properly encrypted and signed for a boot loader to authorize loading the device assisted service agent programs into execution memory, and in some embodiments, if the images are not properly signed then an access control integrity error is generated and/or the program is not loaded. In some embodiments, such properly signed DAS images can only be obtained from the service controller. In some embodiments, such DAS images can only be loaded into protected file storage by the service controller. In some embodiments, the hardware security features that prevent unauthorized elements on the device from accessing the protected file storage include encrypting all traffic to and from the secure storage so that only authorized device program elements possess the counterpart encryption capability to access the storage. In some embodiments, access or access rights to re-program a device assisted service agent program store is restricted to the service controller via the service control link so that unauthorized program elements on the device are not authorized to alter the device assisted service agent code and/or operation.

[0041] In some embodiments, the hardware security features that protect device assisted service agent storage include a protected DAS partition in which an access control integrity agent function is isolated from other device program elements, and a secure service control link is also isolated in a similar manner, and the access control integrity agent scans the execution memory,

data memory and/or file storage used by one or more device assisted services agents to measure and/or control services. In some embodiments, the purpose of the scan is to detect changes to the device assisted service agent code and/or data. In some embodiments, the purpose of the scan is to detect other unauthorized program elements or data that may be present in reserved or protected areas used for device assisted service agent execution. In some embodiments, reports of such scan audits are reported over the service control link to the service controller for further processing by use of cloud based resources to identify access control integrity violations. In some embodiments, the access control integrity agent functions include one or more of hashing other device assisted security agents, querying other device assisted security agents, observing the operation of other device assisted security agents or monitoring service measures and then either evaluating the results locally on the device to determine if they are within pre-defined allowable parameters or sending at least some of the results to the service controller for further analysis via the service control link. In some embodiments, the scan audits are compared with earlier versions of the scans to compare code configuration or operational characteristics. In some embodiments, the scan audits are compared against known databases for the code or operational characteristics that should be present in the DAS agents.

[0042] In some embodiments, an access control integrity agent, or a new version of the access control integrity agent can be downloaded by the service controller over the secure service control link. For example, this technique provides for a real time assessment of device service control security state as described above in the event that corruption or compromise of the secure device assisted service agent(s) has occurred. In some embodiments, the access control integrity agent that is downloaded can have a different configuration and/or operation than any agent previously loaded onto the device so that it is difficult or impossible for a hacker or malware to spoof the operation of the agent in a short period of time. For example, by requiring the agent to report security assessments back to the server in a period of time that is typically less than what is required to spoof the agent, the agent will either report back an accurate assessment of device status or will be blocked by a hacker or malware, and both of these conditions can provide the information required to take action if the device assisted services system has been corrupted or compromised.

[0043] In some embodiments, the protected DAS partition and/or the modem execution partition can be used to securely store some or all of the device credentials that are used for one or more of device group association, activation, authorization to the access network and/or the DAS network, service level, and service usage accounting and/or billing.

[0044] In some embodiments, the modem subsystem also includes DAS elements that strengthen the access control integrity of the DAS system. As shown in FIG. 1, one or more modems can include, in some embodiments, DAS agent functions labeled modem partition DAS agents 126. The modem execution partition 124 of the modem sub system #1 (125) of the modem execution partition 124 includes modem partition DAS agents 126 in communication (e.g., secure communication, such as using encrypted communications) with a modem 128 and a modem service control link 130, which is in communication with the network service control link 152 via the modem secure channel #1 (132), as shown. Also, the modem 128 is in communication (e.g., secure communication, such as using encrypted communications) with the access network #1 (136), which is in communication with the access network service usage 142 and the Internet 140, which is in communication with a private network 146, which is in communication with the private network service usage 144, as shown.

[0045] Example embodiments for DAS agent functions that execute in the modem execution partition include modem encryption and modem service usage measures. In other embodiments, the modem execution partition can also include higher level DAS agent functions, such as stack traffic classification, stack manipulation, access control, and/or traffic control. For example, the modem execution partition can also include a full service processor that is fully capable of managing all aspects of service usage measurement and/or service control. It will now be apparent to one of ordinary skill in the art that the modem execution partition can employ a number of the service security embodiments described in the context of the protected DAS partition, for example, to enhance the service integrity of the DAS system. For example, the DAS agents on the modem can be stored in an encrypted and signed format on non-volatile (NV) memory on the modem that is only accessible by the network service control link or by a local secure control link from the protected DAS partition to the modem execution partition. As shown in FIG. 1, a separate secure modem control channel (e.g., modem secure channel #1 (132) through modem secure channel #N (134)) that is distinct from the host secure control channel

150 is provided. This separate modem control channel can either be implemented over the higher network layers of the device or over the lower access network layer so that special access to access network resources is required to even connect to the modem DAS agents 126 thereby further enhancing service control related security.

[0046] In some embodiments, the protected DAS partition provides for performing the DAS agent functions required for parental controls, enterprise WWAN management controls or roaming controls, and/or usage reporting in the protected execution space. In view of the DAS embodiments described herein, it will now be apparent to one of ordinary skill in the art how to implement such protected controls for these various and other application scenarios.

[0047] In some embodiments, a protected DAS partition provides for performing a virtual machine (VM) on top of a secure machine. The device application OS that is accessible by software that can be installed without special permissions can be isolated from the secure hardware and/or OS that is running under the VM. Using these techniques, malware can be "cocooned in" on the VM OS rather than "walled out" as discussed with respect to various embodiments described herein.

[0048] In some embodiments, communication between program/functional elements outside of the protected DAS partition to DAS agents inside the protected DAS partition is controlled by a secure encrypted channel. In some embodiments, only programs/functions that have access to communicate with DAS agents are allowed to do so, and, in some embodiments, even these outside programs are not allowed to modify the DAS agent configuration, only to report information and/or receive information.

[0049] For example, various embodiments can be used to connect to multiple access networks through multiple modems, with each modem potentially being associated with a different set of DAS service policies corresponding to the different types of access networks supported. In some embodiments, such as for 3G/4G modems, WWAN/WLAN modems, and various other multiple modem embodiments, the multiple modems can also be provided on the same multi-mode modem subsystem rather than on different modem subsystems.

[0050] In some embodiments, the various techniques and embodiments described herein can be readily applied to intermediate networking devices as will now be apparent to one of ordinary skill in the art. For example, an intermediate networking device can includes some or all of the DAS agents for managing, controlling, and/or measuring service usage for one or more devices in communication with a wireless network via the intermediate networking device, in which the DAS agents can be executed in secure execution environments or secure execution partitions using the various techniques described herein. In some embodiments, intermediate networking devices include, for example, WWAN/WLAN bridges, routers and gateways, cell phones with WWAN/WLAN or WWAN/Bluetooth, WWAN/LAN or WWAN/WPAN capabilities, femto cells, back up cards for wired access routers, and other forms/types of intermediate networking devices.

[0051] FIG. 2 illustrates another secure execution environment 200 for device assisted services in accordance with some embodiments. In particular, FIG. 2 illustrates an embodiment in which DAS agents do not actually replace the OS network stack elements, but instead one or more DAS agents include device driver programs that interface into the network stack and pass (e.g., securely communicate) traffic information or actual traffic back and forth with the stack. These device driver interface constructs are labeled OS driver framework and interface 208 as shown in FIG. 2. Example OS system constructs that provide for this type of architecture for DAS agents include Windows NDIS and/or TDI drivers, Windows Filter Platform (WFP), Berkeley Packet Filter, ipfw (e.g., a BSD packet filter that can be used for various OSs, such as Unix, Linux, MAC OS), and/or other platforms/programs performing these or similar functions. While these OS stack options are not secure in themselves, if the drivers that interface with them are secured as illustrated in FIG. 2 by executing the drivers in the protected DAS partition 214, then higher overall access control integrity/security levels can be achieved.

[0052] As shown in FIG. 2, the service measurement and/or policy control drivers 210 executed in the protected DAS partition 214 represent the DAS drivers that interface to the OS stack device driver interface constructs labeled OS driver framework and interface 208 executed in the kernel execution partition 212, which are in communication with/interface with OS Stack API(s) 207. As also shown, applications, such as applications 106A through 106C execute in the application execution partition 202. In some embodiments, service access control integrity is

further enhanced by placing additional measurement points outside of the network stack, so that, for example, if the network stack service usage reporting is hacked, corrupted, and/or compromised, there is a secure additional or back-up service measure located on the device and/or in the network (e.g., modem agent 226 as shown in FIG. 2, which provides a service measurement point in the modem for measuring service usage by the device, and as shown also provides for secure communication with the modem agent 226 using modem encryption 225). For example, the service measure provided by the modem agent 226, modem encryption 225, and/or modem bus 120 functions shown in FIG. 2 can be executed in a protected partition (e.g., modem execution partition 124 as shown in FIG. 2 can be implemented as a secure or protected partition using the various techniques described herein).

[0053] FIG. 3 illustrates another secure execution environment 300 for device assisted services in accordance with some embodiments. As shown, some stack elements are executed in the kernel execution partition 312 and some stack elements are executed in the protected DAS execution partition 314. In some embodiments, the DAS agents 104 executed in the application execution partition 302 are directly monitoring and/or controlling stack traffic by intercepting it and imposing additional traffic measurement and/or filtering. Examples of such techniques are described herein with respect to various embodiments. As shown in FIG. 3, the network stack elements 308 are the OS stack elements that reside in the kernel execution partition 312 and the protected DAS network stack elements 310 are the stack elements that reside in protected DAS execution partition 314. For example, as some or potentially all of the stack network traffic processing resides in the protected DAS execution partition 314, a high level of service control integrity can be maintained using these techniques. For example, the modem bus driver 121 can be executed in a secure execution partition, such as modem execution partition 324, which can be implemented as a secure execution partition using the various techniques described herein, or the modem bus driver 121 can be executed in the protected DAS execution partition 314, so that unauthorized programs can be blocked from accessing the access network through the modem.

[0054] In some embodiments, the entire stack is executed in the protected DAS execution partition 314 with only a stack API executing in kernel execution partition 312. Various other embodiments involve implementing a minimum (e.g., in terms of a number of agents and/or functionality) in the protected DAS execution partition 314 required to secure a service measure

that can be used to confirm the integrity of the service policy implementation (e.g., as described with respect to various other embodiments disclosed herein). As will now be apparent to one of ordinary skill in the art, various combinations of stack processing functions can be implemented in a secure host execution partition to strengthen the service measurement and/or service control integrity of the DAS system using the techniques and/or similar techniques to the various techniques described herein.

[0055] In some embodiments, the stack elements implemented in the protected DAS execution partition can include stack API, sockets layer, TCP, UDP, service measurements at one or more points in the stack, IP layer processing, VPN/IPSEC, PPP, access control, traffic classification, traffic queuing, traffic routing, traffic QOS, traffic demand reporting to QOS allocation servers, traffic statistics reporting to the QOS servers, traffic QOS reservation requests including by traffic type or app type or service priority to the servers, traffic throttling, traffic statistics gathering, traffic QOS priority identification, modem drivers, modem data encryption, and/or other stack element functionality or features.

[0056] In some embodiments, the above discussed service control mechanisms are controlled by policy commands received over the service control link from the servers or other authorized network elements. In some embodiments, the device also reports usage measures to servers or other authorized network elements. In some embodiments, the device also reports QOS demand to the servers or other authorized network elements and/or accepts QOS instructions from the servers or other authorized network elements. In some embodiments, the device reports traffic statistics, projected traffic demand, application usage, projected QOS demand can all be reported to the servers or other authorized network elements for the purpose of provisioning the right amount of data bandwidth and traffic priority to the device, and the servers or other authorized network elements aggregate such reports from many different devices to project needed allocations across the entire network and make global bearer channel level or base station level decisions bearer channel allocation and bearer channel QOS allocation decisions, which can also be tied into a bearer channel provisioning, or bearer channel QOS provisioning apparatus or other authorized network elements located in the access network.

[0057] For example, as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein, additional security measures, can be added in some embodiments to augment the secure service partitioning, including, for example, access control integrity checks. For example, in addition to the service control policy instructions that can be received from the servers or other authorized network elements, an intermediate policy control agent can be present to make additional higher level decisions on how instantaneous policy should be implemented.

[0058] As shown in FIG. 3, the modem control link, shown as modem local channel 330, provides a link from local connection to the host service control link 118, which in turn connects through the host secure channel 150 to the service controller 152. This communication channel can also be implemented or configured to provide for encrypted communication and, in some embodiments, can be used as an alternative to the direct connection from the modem service control link to the network service control link as disclosed with respect to other figures and various embodiments as described herein.

[0059] As shown in FIG. 3, the final stack elements that feed or communicate with the modem bus driver 121 are the protected DAS network stack elements 310 located in the protected DAS execution partition 314 (illustrated as a solid line in FIG. 3), or, in some embodiments, can be the network stack elements 308 located in the kernel execution partition 312 (illustrated as a dashed line in FIG. 3). In some embodiments, these final stack elements feed or communicate with the modem subsystem 125. In some embodiments, the modem subsystem 125 includes an encrypted link so that the stack elements 310 in the protected DAS execution partition 314 can communicate with the modem 128 but other software programs or hardware elements cannot, for example, thereby preventing the service measures and/or controls from being inappropriately bypassed or otherwise comprised. For example and as similarly discussed above, the modem subsystem 125, for example, can include its own the protected execution partition using various techniques described herein. The modem protected execution partition, for example, can also include a service measure (e.g., modem agent 226 can provide such a service measurement point in the modem subsystem 125, as similarly described above with respect to FIG. 2) to increase service control integrity verification as depicted by service measure. The modem service measure can be included in protected execution partition that can

only be accessed by the service controller 122 by way of the modem local channel 330, or the modem service measure can only be accessed by another DAS agent 310 in protected execution partition 314. In some embodiments, the modem local channel 330 is implemented as a secure channel (e.g., an encrypted communication channel between the modem service control link 130 and the host service control link 118). As described herein, the modem driver can reside in protected service execution environment, or the modem traffic can be encrypted within service execution environment. For example, the encryption settings can be controlled by various secure control servers.

[0060] FIG. 4 illustrates another secure execution environment 400 for device assisted services in accordance with some embodiments. In particular, FIG. 4 illustrates a direct stack manipulation option performed by the DAS agents executed in the protected DAS execution partition 414, including, as shown, an app(lication) identify agent 420, an access control integrity agent 422, a policy control agent 424, a policy implementation agent 426, a service measure/service monitoring agent 428, a modem encryption agent 430, and a bus driver 432. For example, the policy implementation agent 426 performs access control and/or traffic shaping according a set of service control policies. The service control policies, for example, can be set by the service controller 122 or by the service controller 122 in coordination with the policy control agent 422. As shown the app identify agent 420 is in communication with the various applications 106A through 106C executed in the application execution partition 402. As also shown, the various applications 106A through 106C executed in the application execution partition 402 are in communication with the OS stack and/or stack API(s) 408 executed in the kernel execution partition 412.

[0061] In some embodiments, the protected service measure agent 428, the modem encryption agent 430, the modem driver agent 432, the application identifier agent 420, the access control integrity agent 422, and the policy control agent 424 are all implemented in protected DAS partition 414, as shown. In some embodiments, as will now be apparent to one of ordinary skill in the art, a subset of these functions can be implemented in a protected execution partition, such as the protected DAS partition, in various circumstances.

[0062] FIG. 4 also similarly shows various embodiments that are available for network based service usage measures and interfacing to the mediation and billing systems, and it should be understood that any or all of the embodiments and figures can be employed in the context of carrier networks, MVNOs, private networks, or open networks supporting enterprise IT manger controls, parental controls, multi-network controls, and/or roaming controls.

[0063] FIG. 5 illustrates another secure execution environment 500 for device assisted services in accordance with some embodiments. In particular, FIG. 5 is similar to that FIG. 4 except that FIG. 5 illustrates a modem service control link 132 that is connected directly to the service controller 122 via the network service control link 152 (e.g., via a modem secure channel). In some embodiments, a modem control link for DAS is established locally on the device or through an entirely different control channel, which, in some embodiments, provides enhanced security as discussed herein (e.g., it is very difficult to hack a service usage measure or service control that cannot be accessed on the device).

[0064] FIG. 6 illustrates another secure execution environment 600 for device assisted services in accordance with some embodiments. In particular, FIG. 6 illustrates a policy implementation agent 616 that includes the entire networking stack running in protected execution partition 614 and an OS stack API 608 that includes an application identifying function 620 in the kernel execution partition 612.

[0065] FIG. 7 illustrates another secure execution environment 700 for device assisted services in accordance with some embodiments. In particular, FIG. 7 illustrates DAS agents that do not replace the OS network stack elements, but instead one or more DAS agents are comprised of device driver programs that interface into the network stack and pass traffic information or actual traffic back and forth with the stack. These device driver interface constructs are labeled OS driver framework and interface 722 in FIG. 7 as similarly shown in and described with respect to FIG. 2, along with OS stack API 708, which includes application identifier function 720 as similarly discussed above with respect to FIG. 6, and are executed in kernel execution partition 712. Also, as shown, application partition DAS agents 104 are executed in application execution partition 702. The main difference between the embodiment in FIG. 7 and that shown in and described with respect to FIG. 2 is that the service measure agent

428, modem encryption agent 430, and modem driver agent 432 are executed in the protected DAS partition 714, as shown in FIG. 7. For example, this provides for enhanced service control security as described herein with respect to various embodiments.

[0066] FIG. 8 illustrates another secure execution environment 800 for device assisted services in accordance with some embodiments. In particular, FIG. 8 illustrates a more simplified embodiment that is similar to that of FIG. 7. In FIG. 8, only an access control integrity agent 422 and a service measure 428 are executed in protected DAS partition 814, and the bus driver 432 and the service measurement and/or policy control drivers 210 are executed in the kernel execution partition 712. This embodiment illustrates that provided that at least one protected service measure is provided on the device, then the DAS service control integrity can be very high. For example, if it is not possible to access the program code or control traffic for the service measure agent 428, and the host service control link 118 except through the encrypted control channel from the service controller 122, then this simplified configuration can be almost as secure as that possible with network based service measures. It will now be apparent to one of ordinary skill in the art that this technique similarly applies to a service measure and control link similarly implemented in a protected modem execution partition 324. In some embodiments, the access control integrity agent 422 provides additional security, for example, in the event that the protected DAS partition 814 is breached or compromised.

[0067] FIG. 9 illustrates another secure execution environment 900 for device assisted services in accordance with some embodiments. In particular, FIG. 9 illustrates an embodiment similar to that of FIG. 8 except that, in particular, in addition to the service measure being executed in protected DAS partition 914, the modem encryption agent 430 is also implemented in/executed in the protected DAS partition 914. For example, this prevents unauthorized software from defeating the service measurements and/or service controls by going around the network stack directly to the modem.

[0068] FIG. 10 illustrates another secure execution environment 1000 for device assisted services in accordance with some embodiments. In particular, FIG. 10 illustrates an embodiment similar to that of FIG. 9 except that, in particular, there are additional app partition DAS agents 104 executing in the application execution partition 702. For example, this illustrates that some

DAS agents can be implemented in application space (e.g., UI agent, policy control agent, and various other DAS agents as described herein) while still maintaining a high level of service measurement and/or control security as long as there are a few key measures and/or controls implemented in protected execution partitions using the various techniques described herein.

[0069] FIG. 11 illustrates another secure execution environment 1100 for device assisted services in accordance with some embodiments. In particular, FIG. 11 illustrates how the server cloud can be assisted by the on board access control integrity agent to detect tampering with other service measurement(s) and/or control agent(s), or to protect the service measurement and/or control system from being attacked by malware and/or otherwise comprised. As shown, the access control integrity agent 422 executes inside the protected DAS partition 1114 and is in communication with file storage 1130 (e.g., for persistently maintaining device status and/or other settings or status or monitoring information). The access control integrity agent 422 performs the various access control integrity check functions as, for example, described herein with respect to various embodiments, and, in some embodiments, in coordination with the servers over the secure control channel (e.g., host secure channel 150). In some embodiments, the access control integrity agent 422 can send the service controller 122 information about the other service measurements and/or control agents so that the service controller 122 can determine if the agents are working properly or have been tampered with or otherwise compromised. For example, such information can include sections of code, hashes, code segments, code variations from a previous image, code variations from a historical image, responses to queries, checksums, observations of operating behavior or patterns, service usage, policy implementation behavior, and/or other information that may be indicative of tampering, corruption, and/or a compromise of any of the device agents/measures. In some embodiments, the access control integrity agent 422 checks the operating environment for signs of malware signatures, or sends application and/or driver information or other information about the operating environments to the servers for further processing to detect malware. In some embodiments, the access control integrity agent 422 performs basic operations on protected DAS partition memory, kernel execution partition memory areas, application execution partition memory areas, on disk storage areas or on other file storage areas to detect known malware hashes or signatures, etc., or the access control integrity agent 422 can send the hashes to the

servers for comparison against malware databases (e.g., to compare against signatures for known malware or for further behavioral based or other security/malware detection techniques).

[0070] In some embodiments, the DAS system is implemented in a manner that is robust to losses in service control link (e.g., coverage outages on a WWAN link or loss of connection on a wired link). In some embodiments, the DAS system to be implemented in a manner that is robust to one or more server elements in the service controller going offline or failing for any reason. The following embodiments facilitate these techniques, as described below.

[0071] In some embodiments, it is advantageous for one or more of the device assisted service agents to maintain a record of the service usage reports and/or other reporting that is provided to the service controller regarding device service control state (e.g., present service plan settings, current service usage policy settings, current user preference settings, current DAS settings, current encrypted control channel and/or local encrypted communication channel key information, current DAS agent status reports, current DAS agent security state reports, current ambient service usage and/or transaction records, current service control integrity threat reports, user status information, device status information, application status information, device location, device QOS state, and/or other state and/or settings information). In addition to such information that exists on the device and is reported to the service controller, additional service information can be derived and recorded in the service controller, such as information received from outside the device and/or analysis of the device reported information (e.g., network based service usage measures, analysis of device service usage, comparison of device reports with other information, analysis of access control integrity agent reports, information received from roaming networks, information input to the service controller from parental control terminals, enterprise control terminals, virtual service provider control terminals, access network authorization information, service integrity violation level, and many other types of information used to properly measure and/or control the device services). For example, the information reported from the device and received or derived outside the device that is required to adequately define the actions needed from the service controller to maintain proper DAS system operation is sometimes referred to herein as the "device service state."

[0072] In some embodiments, the service controller functions are highly scalable and can be executed on a number of hardware and software platforms (e.g., different virtual machines in a server, different servers in a data center, or different servers located in different data centers). For example, in such embodiments the service controller can be designed so that the programs that execute the various service controller server functions can derive all of the information necessary to properly manage the device at any moment in time by knowing past device service state and current service state that adequately define the next set of actions the service controller needs to implement to properly maintain the DAS system operation. By designing the system in this way, if the server that is running the service controller server functions for any given device in question were to go down or become disconnected from the device, then another server could later resume proper operation of the DAS system by assigning another service controller server function to the device and recovering or restoring the necessary past device service state and the necessary current device service state.

[0073] For example, this can be accomplished in some embodiments as described below. The service controller saves the current device service state into a common database (e.g., which can be centralized or distributed) that is available to all service controller server functions. The device service state is saved each time the device communicates with the service controller, or at regular time intervals, or a combination of both. The device retains its current and past service state reports even after they are reported at least until the service controller sends the device a message confirming that the service controller has saved a given device service state. Once the device receives this save confirmation for a given device state report then it is no longer required to retain that particular device state report once the device has no further use for it. In this manner, if a service controller server function goes down then a save confirmation for one or more reported device states is not transmitted to the device by the service controller, and the device can retain that report. A server load balancer detects that a given service controller server function has gone down, looks up the devices that were being controlled by that service controller server function, finds that the device in question was one of those devices and re-assigns a new service controller server function (either in the same data center or in another data center) to control the device in question. The newly assigned service controller server function then recovers all past device states that were recorded in the service controller database and are required to properly manage the DAS system, and then asks the device to transmit or re-transmit

all device state reports that were not saved in the service controller database. Once the device transmits or re-transmits the requested information, the newly assigned service controller function then has the information it needs to properly manage the DAS system, it saves all the reported device state information, and then sends save confirmations to the device so that the device need no longer retain the older service state reports. The newly assigned service controller server function can then resume the DAS system operation with a set of actions that are identical or very similar to the actions that would have been taken by the original service controller server function if it had not gone down. One of ordinary skill in the art will now appreciate that the above techniques can also be used to accommodate temporary losses in the connection between the device and the service controller. For example, such techniques provide for a highly scalable and robust approach to implement a distributed service controller across multiple data centers for reliable service redundancy. In some embodiments, the past device service state information is saved in the protected DAS execution partition and/or the modem execution partition, for example, so that it is protected from corruption.

[0074] Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

INCORPORATION BY REFERENCE

[0075] This application incorporates the following provisional and nonprovisional U.S. patent applications by reference: Application No. 12/694,445, filed January 27, 2010, entitled SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES; Application No. 12/380,780, filed March 2, 2009, entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION; Application No. 61/206,354, filed January 28, 2009, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD; provisional Application No. 61/206,944, filed February 4, 2009, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD; provisional Application No. 61/207,393, filed February 10, 2009, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD; provisional Application No. 61/207,739, filed February 13, 2009, entitled SERVICES POLICY

COMMUNICATION SYSTEM AND METHOD; and provisional Application No. 61/252,151, filed on October 15, 2009, entitled SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES.

[0076] WHAT IS CLAIMED IS:

CLAIMS

1. A system, comprising:

a processor of a communications device configured to:

implement a service profile executed at least in part in a secure execution environment for assisting control of the communications device use of a service on a wireless network, wherein the service profile includes a plurality of service policy settings, and wherein the service profile is associated with a service plan that provides for access to the service on the wireless network;

monitor use of the service based on the service profile; and

verify the use of the service based on the monitored use of the service;

a memory of the communications device coupled to the processor and configured to provide the processor with instructions.

ABSTRACT

Security techniques for device assisted services are provided. In some embodiments, secure service measurement and/or control execution partition is provided. In some embodiments, implementing a service profile executed at least in part in a secure execution environment of a processor of a communications device for assisting control of the communications device use of a service on a wireless network, in which the service profile includes a plurality of service policy settings, and wherein the service profile is associated with a service plan that provides for access to the service on the wireless network; monitoring use of the service based on the service profile; and verifying the use of the service based on the monitored use of the service.

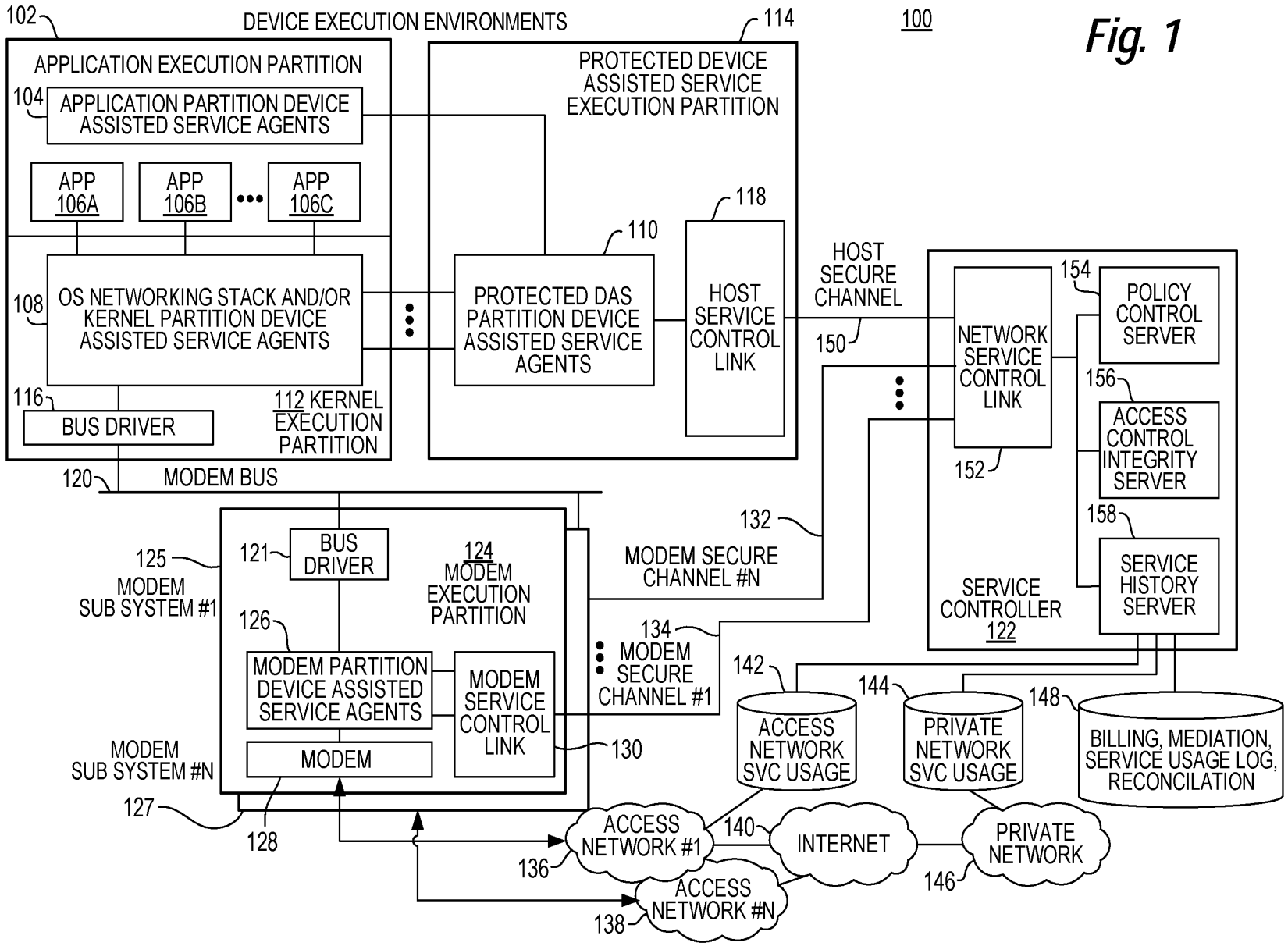
100
DEVICE EXECUTION ENVIRONMENTS
102
APPLICATION EXECUTION PARTITION
104
APPLICATION PARTITION DEVICE ASSISTED SERVICE AGENTS
APP 106A
APP 106B
APP 106C
108
OS NETWORKING STACK AND/OR KERNEL PARTITION DEVICE ASSISTED SERVICE AGENTS
116
BUS DRIVER
112 KERNEL EXECUTION PARTITION
114
PROTECTED DEVICE ASSISTED SERVICE EXECUTION PARTITION
110
PROTECTED DAS PARTITION DEVICE ASSISTED SERVICE AGENTS
118
HOST SERVICE CONTROL LINK
HOST SECURE CHANNEL
150
154
POLICY CONTROL SERVER
156
ACCESS CONTROL INTEGRITY SERVER
158
SERVICE HISTORY SERVER
NETWORK SERVICE CONTROL LINK
152
SERVICE CONTROLLER 122
120
MODEM BUS
125
MODEM SUB SYSTEM #1
121
BUS DRIVER
124 MODEM EXECUTION PARTITION
126
MODEM PARTITION DEVICE ASSISTED SERVICE AGENTS
MODEM SERVICE CONTROL LINK
MODEM
MODEM SUB SYSTEM #N
127
128
130
132
MODEM SECURE CHANNEL #N
134
MODEM SECURE CHANNEL #1
142
ACCESS NETWORK SVC USAGE
144
PRIVATE NETWORK SVC USAGE
148
BILLING, MEDIATION, SERVICE USAGE LOG, RECONCILATION
ACCESS NETWORK #1
136
140
INTERNET
PRIVATE NETWORK
146
ACCESS NETWORK #N
138

Fig. 1

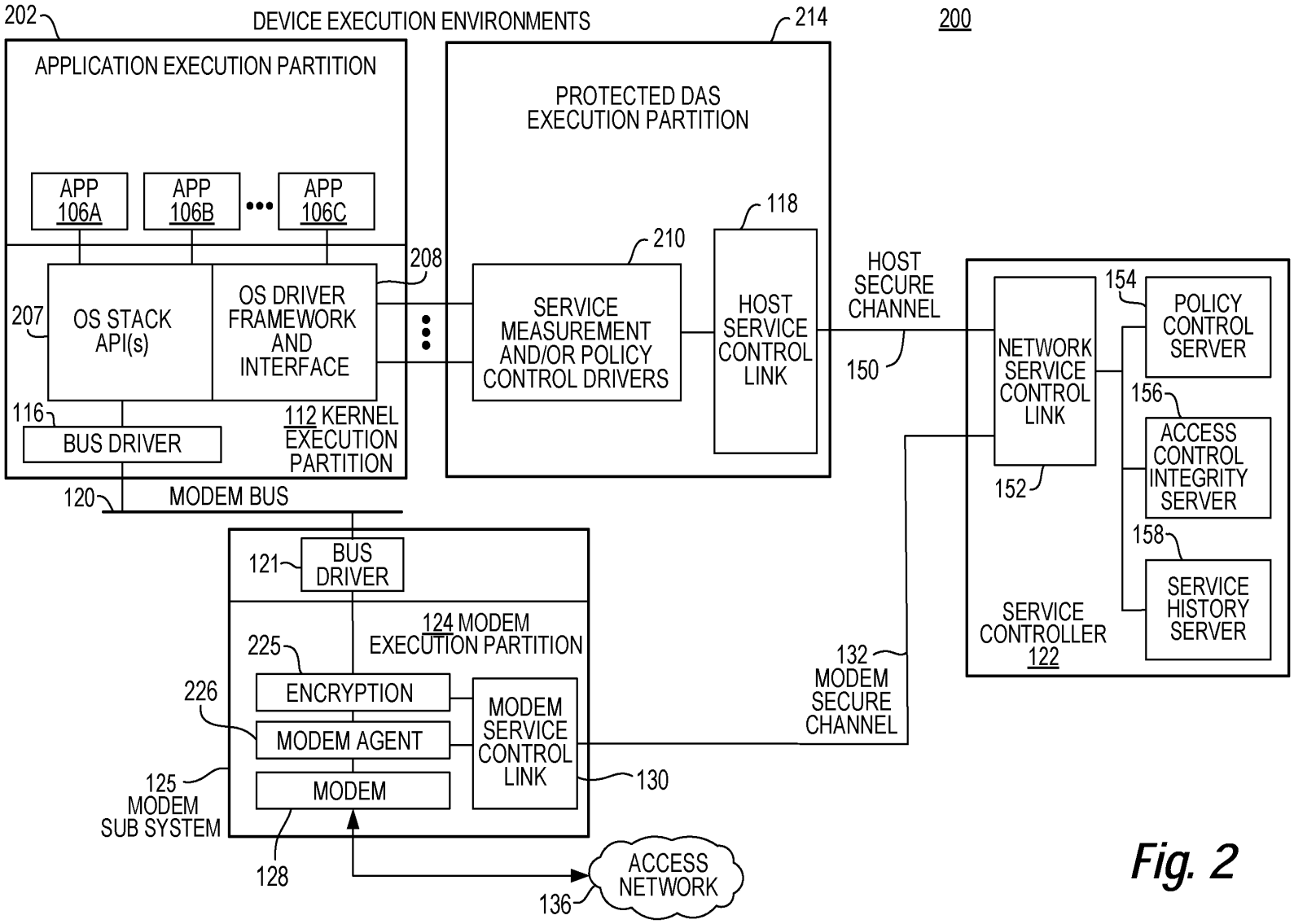
200
DEVICE EXECUTION ENVIRONMENTS
202
APPLICATION EXECUTION PARTITION
APP 106A
APP 106B
APP 106C
207
OS STACK API(s)
OS DRIVER FRAMEWORK AND INTERFACE
208
116
BUS DRIVER
112 KERNEL EXECUTION PARTITION
120
MODEM BUS
214
PROTECTED DAS EXECUTION PARTITION
210
SERVICE MEASUREMENT AND/OR POLICY CONTROL DRIVERS
118
HOST SERVICE CONTROL LINK
HOST SECURE CHANNEL
150
NETWORK SERVICE CONTROL LINK
152
154
POLICY CONTROL SERVER
156
ACCESS CONTROL INTEGRITY SERVER
158
SERVICE HISTORY SERVER
SERVICE CONTROLLER 122
121
BUS DRIVER
124 MODEM EXECUTION PARTITION
225
ENCRYPTION
226
MODEM AGENT
MODEM
MODEM SERVICE CONTROL LINK
130
125 MODEM SUB SYSTEM
128
132 MODEM SECURE CHANNEL
ACCESS NETWORK
136

Fig. 2

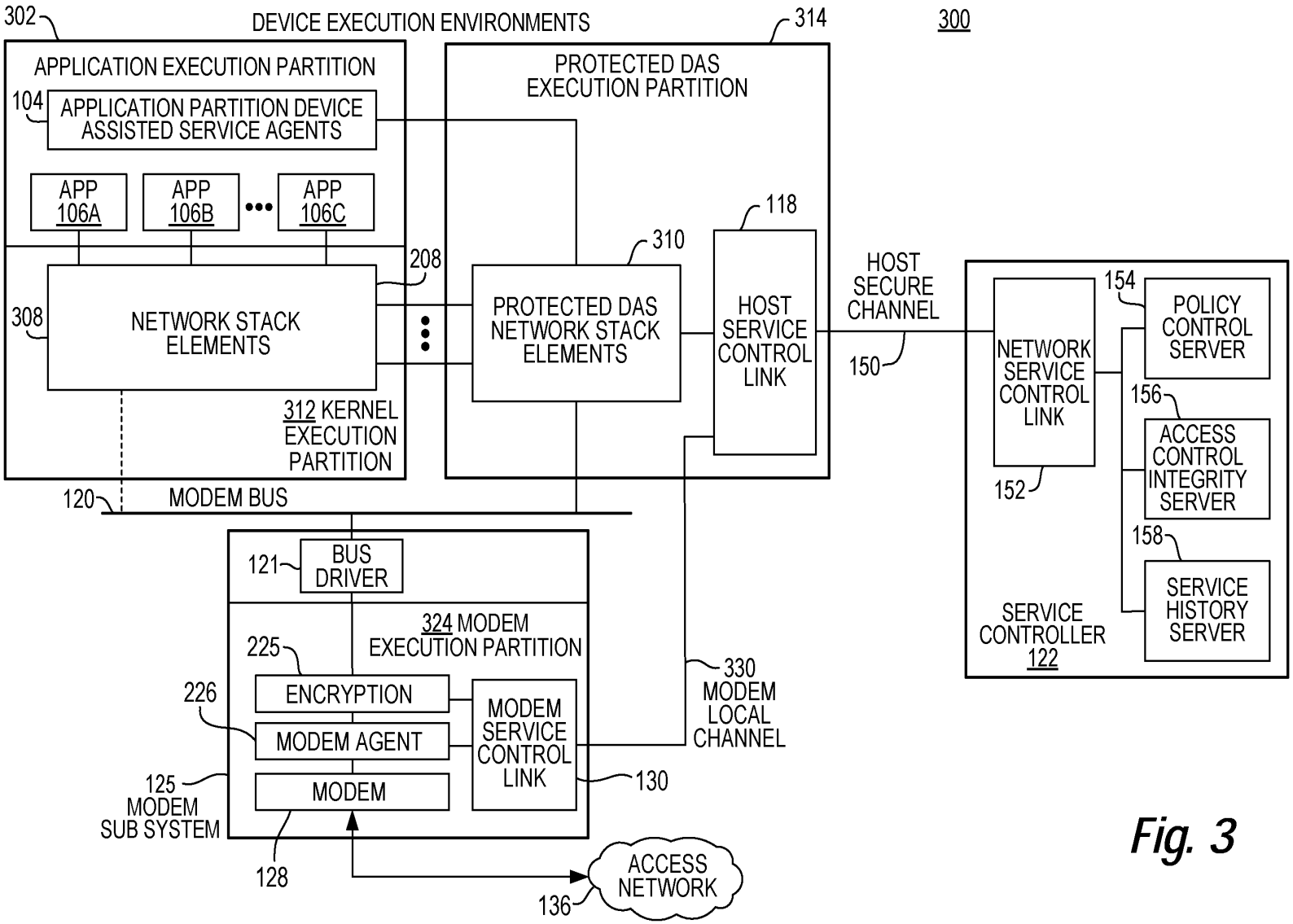
300
302
DEVICE EXECUTION ENVIRONMENTS
314
APPLICATION EXECUTION PARTITION
104
APPLICATION PARTITION DEVICE ASSISTED SERVICE AGENTS
APP 106A
APP 106B
APP 106C
308
NETWORK STACK ELEMENTS
208
312 KERNEL EXECUTION PARTITION
PROTECTED DAS EXECUTION PARTITION
310
PROTECTED DAS NETWORK STACK ELEMENTS
118
HOST SERVICE CONTROL LINK
HOST SECURE CHANNEL
150
NETWORK SERVICE CONTROL LINK
152
154
POLICY CONTROL SERVER
156
ACCESS CONTROL INTEGRITY SERVER
158
SERVICE HISTORY SERVER
SERVICE CONTROLLER 122
120
MODEM BUS
121
BUS DRIVER
324 MODEM EXECUTION PARTITION
225
ENCRYPTION
226
MODEM AGENT
MODEM
MODEM SERVICE CONTROL LINK
130
330 MODEM LOCAL CHANNEL
125 MODEM SUB SYSTEM
128
ACCESS NETWORK
136

Fig. 3

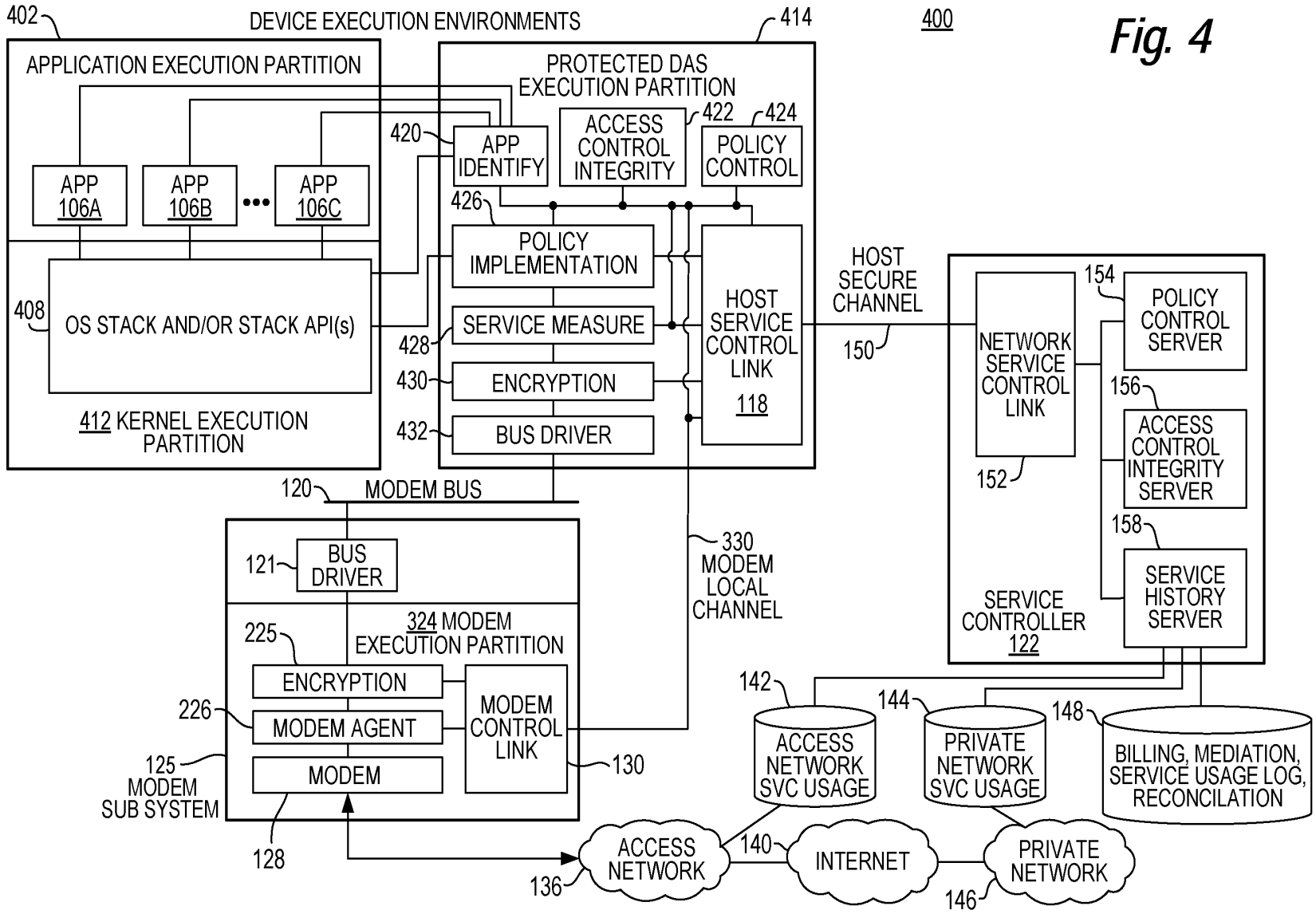
402
DEVICE EXECUTION ENVIRONMENTS
414
400
APPLICATION EXECUTION PARTITION
PROTECTED DAS EXECUTION PARTITION
420
APP IDENTIFY
ACCESS CONTROL INTEGRITY
422
424
POLICY CONTROL
APP 106A
APP 106B
APP 106C
426
POLICY IMPLEMENTATION
408
OS STACK AND/OR STACK API(s)
428
SERVICE MEASURE
430
ENCRYPTION
432
BUS DRIVER
HOST SERVICE CONTROL LINK
118
412 KERNEL EXECUTION PARTITION
HOST SECURE CHANNEL
150
154
POLICY CONTROL SERVER
NETWORK SERVICE CONTROL LINK
156
ACCESS CONTROL INTEGRITY SERVER
152
158
SERVICE HISTORY SERVER
SERVICE CONTROLLER 122
120
MODEM BUS
121
BUS DRIVER
330 MODEM LOCAL CHANNEL
324 MODEM EXECUTION PARTITION
225
ENCRYPTION
226
MODEM AGENT
MODEM CONTROL LINK
130
125 MODEM SUB SYSTEM
MODEM
128
142
ACCESS NETWORK SVC USAGE
144
PRIVATE NETWORK SVC USAGE
148
BILLING, MEDIATION, SERVICE USAGE LOG, RECONCILATION
ACCESS NETWORK
136
140
INTERNET
PRIVATE NETWORK
146

Fig. 4

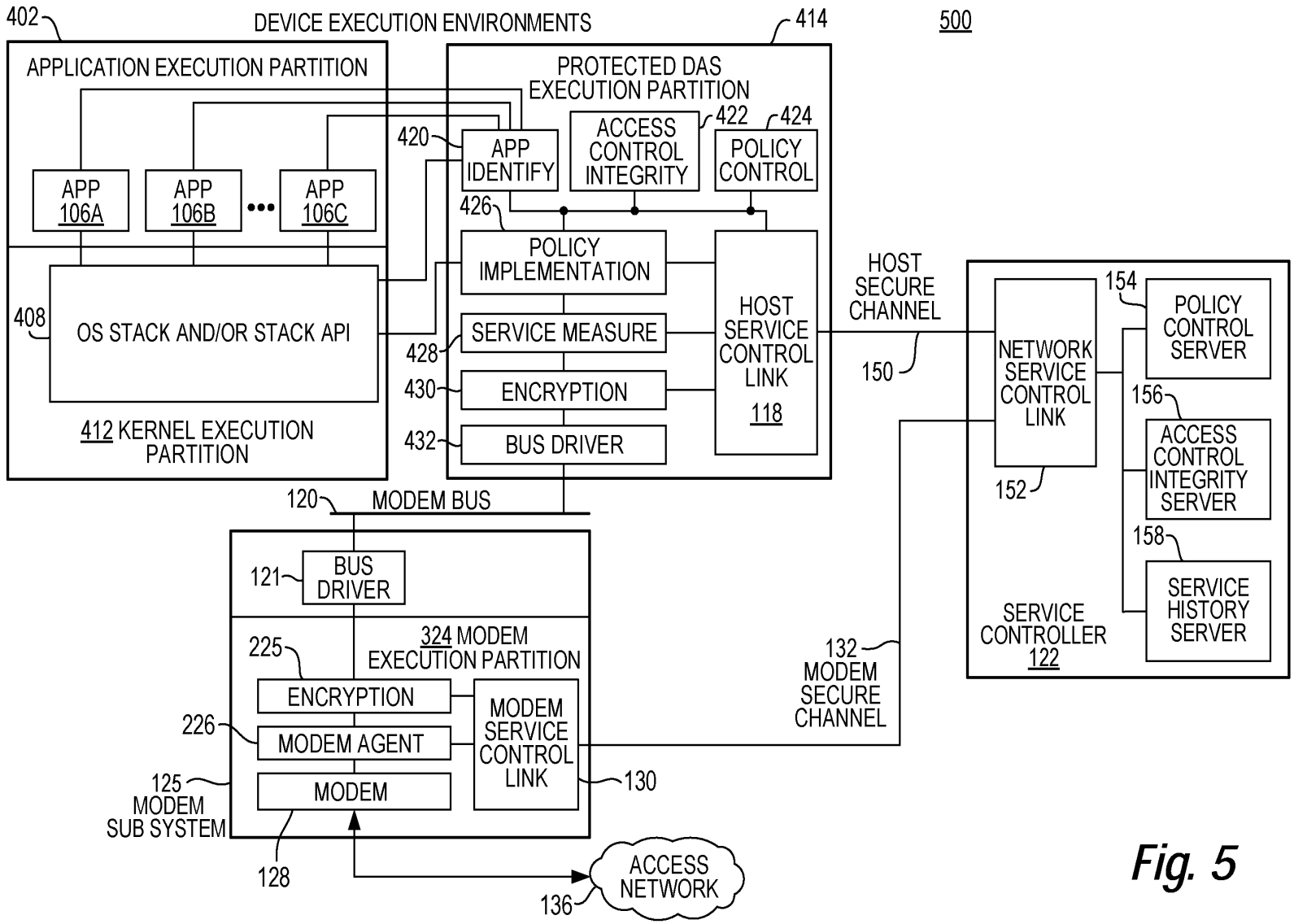
402
DEVICE EXECUTION ENVIRONMENTS
414
500
APPLICATION EXECUTION PARTITION
PROTECTED DAS EXECUTION PARTITION
APP 106A
APP 106B
APP 106C
420
APP IDENTIFY
ACCESS CONTROL INTEGRITY
422
424
POLICY CONTROL
426
POLICY IMPLEMENTATION
408
OS STACK AND/OR STACK API
428
SERVICE MEASURE
430
ENCRYPTION
432
BUS DRIVER
HOST SERVICE CONTROL LINK
118
412 KERNEL EXECUTION PARTITION
HOST SECURE CHANNEL
150
154
POLICY CONTROL SERVER
NETWORK SERVICE CONTROL LINK
156
ACCESS CONTROL INTEGRITY SERVER
152
158
SERVICE HISTORY SERVER
SERVICE CONTROLLER
122
120
MODEM BUS
121
BUS DRIVER
225
324 MODEM EXECUTION PARTITION
ENCRYPTION
226
MODEM AGENT
MODEM SERVICE CONTROL LINK
130
125
MODEM SUB SYSTEM
MODEM
128
132
MODEM SECURE CHANNEL
ACCESS NETWORK
136

Fig. 5

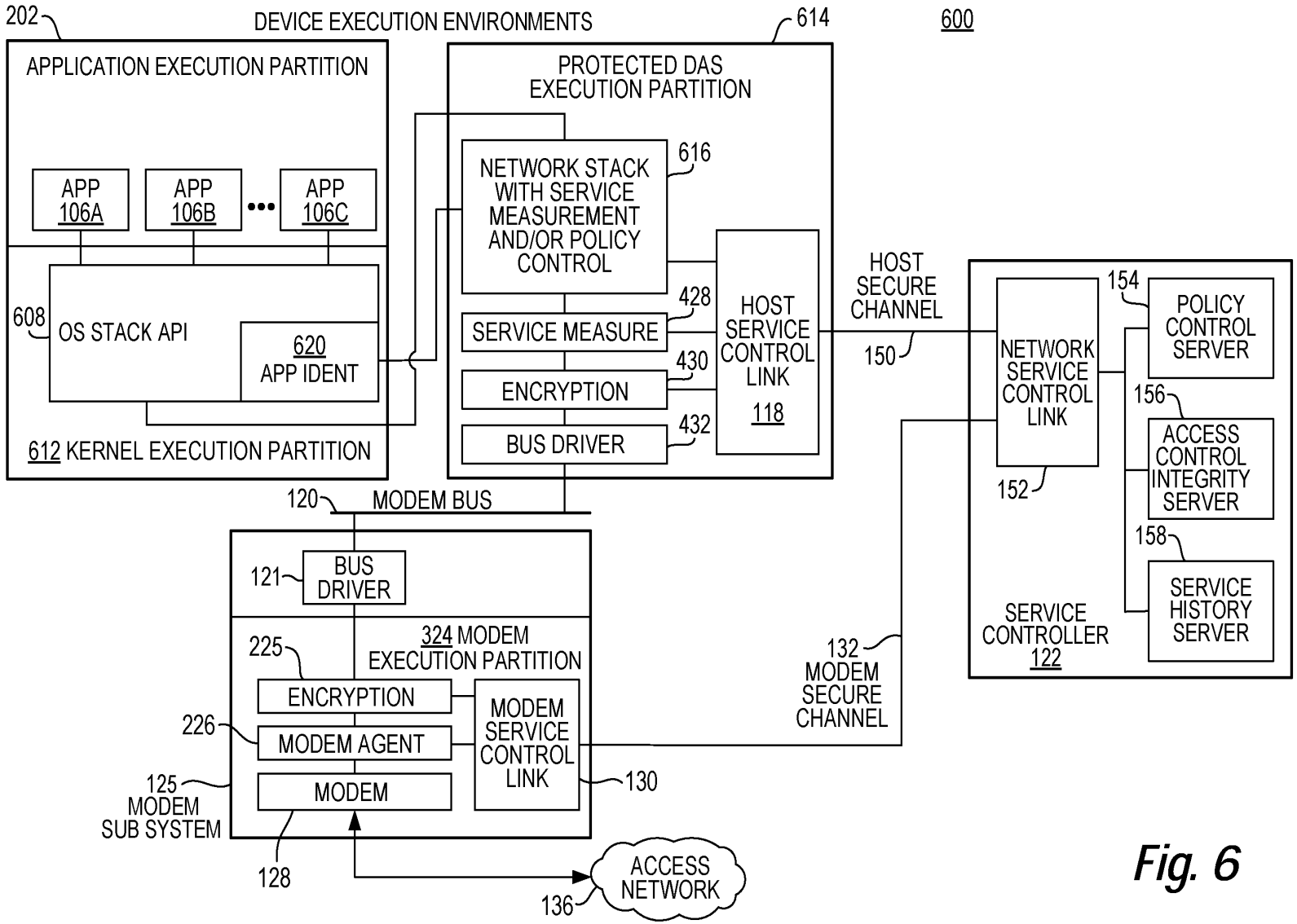
600
DEVICE EXECUTION ENVIRONMENTS
202
APPLICATION EXECUTION PARTITION
APP 106A
APP 106B
APP 106C
608
OS STACK API
620 APP IDENT
612 KERNEL EXECUTION PARTITION
614
PROTECTED DAS EXECUTION PARTITION
NETWORK STACK WITH SERVICE MEASUREMENT AND/OR POLICY CONTROL
616
SERVICE MEASURE
428
ENCRYPTION
430
BUS DRIVER
432
HOST SERVICE CONTROL LINK 118
HOST SECURE CHANNEL
150
NETWORK SERVICE CONTROL LINK
152
154
POLICY CONTROL SERVER
156
ACCESS CONTROL INTEGRITY SERVER
158
SERVICE HISTORY SERVER
SERVICE CONTROLLER 122
120
MODEM BUS
121
BUS DRIVER
324 MODEM EXECUTION PARTITION
225
ENCRYPTION
226
MODEM AGENT
MODEM SERVICE CONTROL LINK
130
125 MODEM SUB SYSTEM
MODEM
128
132 MODEM SECURE CHANNEL
ACCESS NETWORK
136

Fig. 6

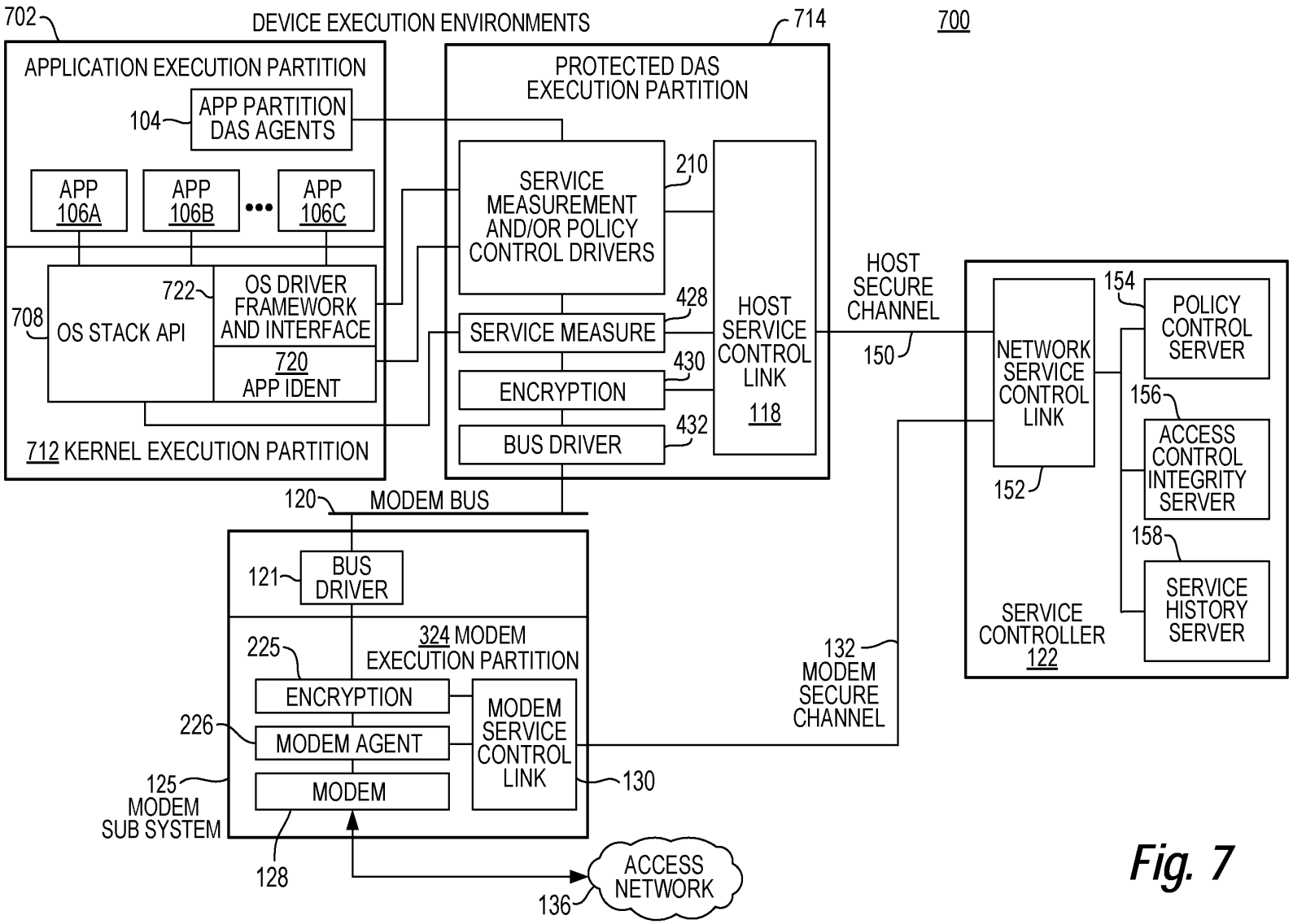
700
DEVICE EXECUTION ENVIRONMENTS
702
APPLICATION EXECUTION PARTITION
104
APP PARTITION DAS AGENTS
APP 106A
APP 106B
APP 106C
708
OS STACK API
722
OS DRIVER FRAMEWORK AND INTERFACE
720 APP IDENT
712 KERNEL EXECUTION PARTITION
714
PROTECTED DAS EXECUTION PARTITION
SERVICE MEASUREMENT AND/OR POLICY CONTROL DRIVERS
210
SERVICE MEASURE
428
ENCRYPTION
430
BUS DRIVER
432
HOST SERVICE CONTROL LINK 118
HOST SECURE CHANNEL
150
NETWORK SERVICE CONTROL LINK
152
154
POLICY CONTROL SERVER
156
ACCESS CONTROL INTEGRITY SERVER
158
SERVICE HISTORY SERVER
SERVICE CONTROLLER 122
120
MODEM BUS
121
BUS DRIVER
324 MODEM EXECUTION PARTITION
225
ENCRYPTION
226
MODEM AGENT
MODEM
MODEM SERVICE CONTROL LINK
130
125 MODEM SUB SYSTEM
128
132 MODEM SECURE CHANNEL
ACCESS NETWORK
136

Fig. 7

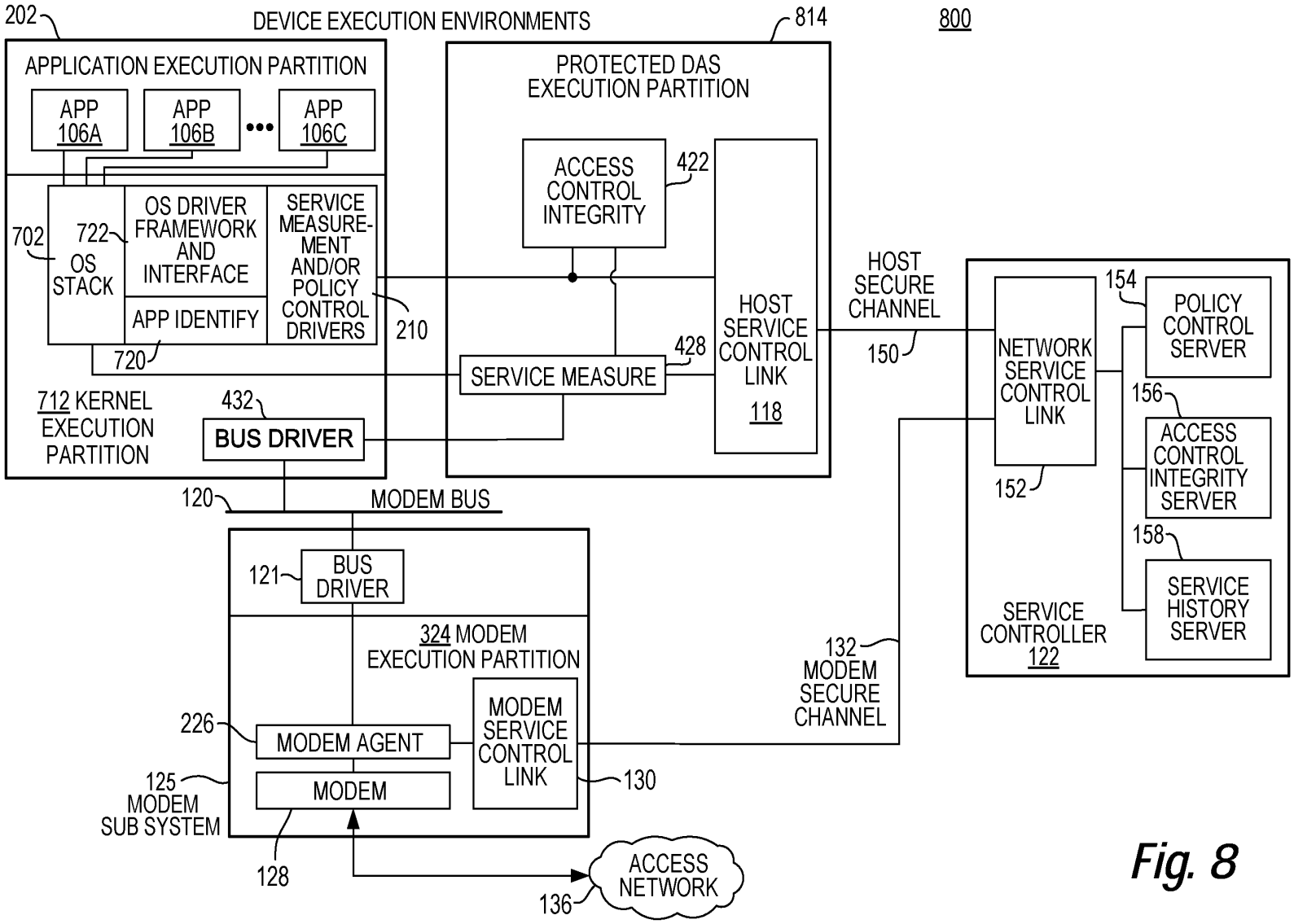
202
DEVICE EXECUTION ENVIRONMENTS
814
800
APPLICATION EXECUTION PARTITION
APP 106A
APP 106B
APP 106C
702
722
OS STACK
OS DRIVER FRAMEWORK AND INTERFACE
APP IDENTIFY
SERVICE MEASURE-MENT AND/OR POLICY CONTROL DRIVERS
210
720
712 KERNEL EXECUTION PARTITION
432
BUS DRIVER
PROTECTED DAS EXECUTION PARTITION
ACCESS CONTROL INTEGRITY
422
SERVICE MEASURE
428
HOST SERVICE CONTROL LINK
118
HOST SECURE CHANNEL
150
NETWORK SERVICE CONTROL LINK
152
154
POLICY CONTROL SERVER
156
ACCESS CONTROL INTEGRITY SERVER
158
SERVICE HISTORY SERVER
SERVICE CONTROLLER 122
120
MODEM BUS
121
BUS DRIVER
324 MODEM EXECUTION PARTITION
226
MODEM AGENT
MODEM SERVICE CONTROL LINK
130
125 MODEM SUB SYSTEM
MODEM
128
132 MODEM SECURE CHANNEL
ACCESS NETWORK
136

Fig. 8

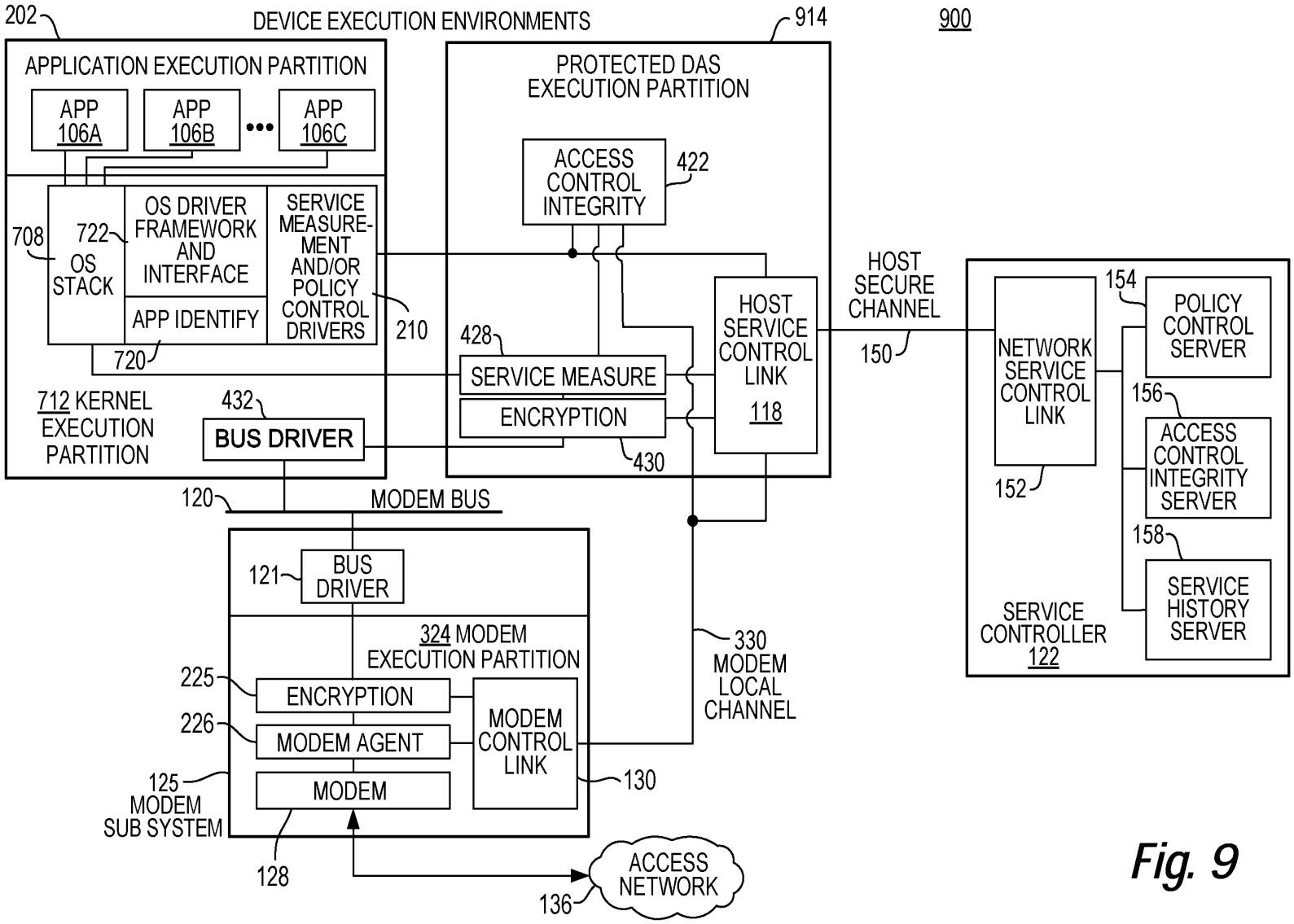
900
DEVICE EXECUTION ENVIRONMENTS
202
APPLICATION EXECUTION PARTITION
APP 106A
APP 106B
APP 106C
708
722
OS STACK
OS DRIVER FRAMEWORK AND INTERFACE
APP IDENTIFY
720
SERVICE MEASURE-MENT AND/OR POLICY CONTROL DRIVERS
210
712 KERNEL EXECUTION PARTITION
432
BUS DRIVER
914
PROTECTED DAS EXECUTION PARTITION
ACCESS CONTROL INTEGRITY
422
428
SERVICE MEASURE
ENCRYPTION
430
HOST SERVICE CONTROL LINK
118
HOST SECURE CHANNEL
150
NETWORK SERVICE CONTROL LINK
152
154
POLICY CONTROL SERVER
156
ACCESS CONTROL INTEGRITY SERVER
158
SERVICE HISTORY SERVER
SERVICE CONTROLLER 122
120
MODEM BUS
121
BUS DRIVER
324 MODEM EXECUTION PARTITION
225
ENCRYPTION
226
MODEM AGENT
MODEM
MODEM CONTROL LINK
130
125 MODEM SUB SYSTEM
128
330 MODEM LOCAL CHANNEL
ACCESS NETWORK
136

Fig. 9

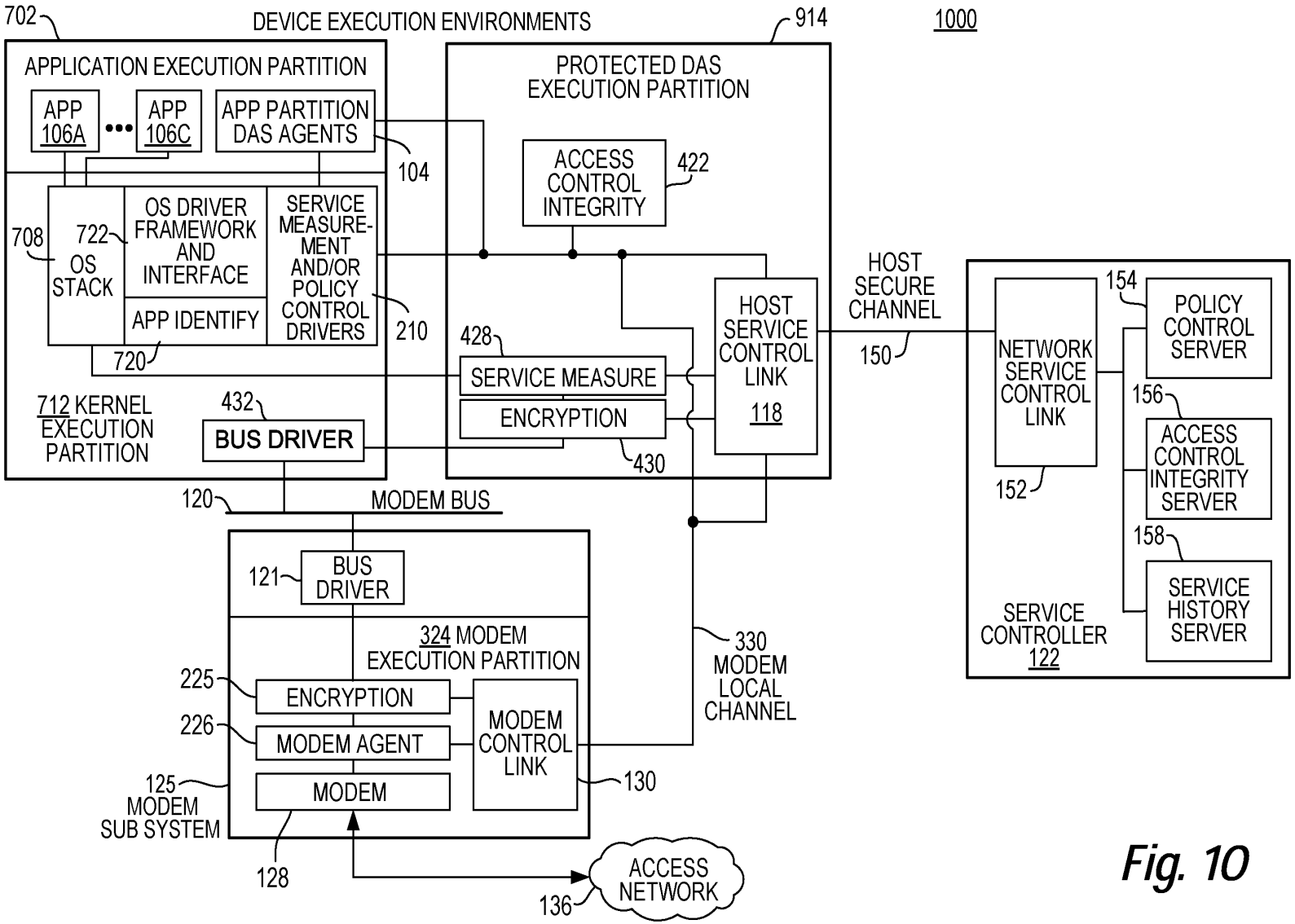
1000
DEVICE EXECUTION ENVIRONMENTS
702
APPLICATION EXECUTION PARTITION
APP 106A
APP 106C
APP PARTITION DAS AGENTS
104
708
722
OS STACK
OS DRIVER FRAMEWORK AND INTERFACE
APP IDENTIFY
SERVICE MEASUREMENT AND/OR POLICY CONTROL DRIVERS
210
720
712 KERNEL EXECUTION PARTITION
432
BUS DRIVER
914
PROTECTED DAS EXECUTION PARTITION
ACCESS CONTROL INTEGRITY
422
428
SERVICE MEASURE
ENCRYPTION
430
HOST SERVICE CONTROL LINK
118
HOST SECURE CHANNEL
150
NETWORK SERVICE CONTROL LINK
152
154
POLICY CONTROL SERVER
156
ACCESS CONTROL INTEGRITY SERVER
158
SERVICE HISTORY SERVER
SERVICE CONTROLLER
122
120
MODEM BUS
121
BUS DRIVER
324 MODEM EXECUTION PARTITION
225
ENCRYPTION
226
MODEM AGENT
MODEM
MODEM CONTROL LINK
130
125
MODEM SUB SYSTEM
128
330
MODEM LOCAL CHANNEL
ACCESS NETWORK
136

Fig. 10

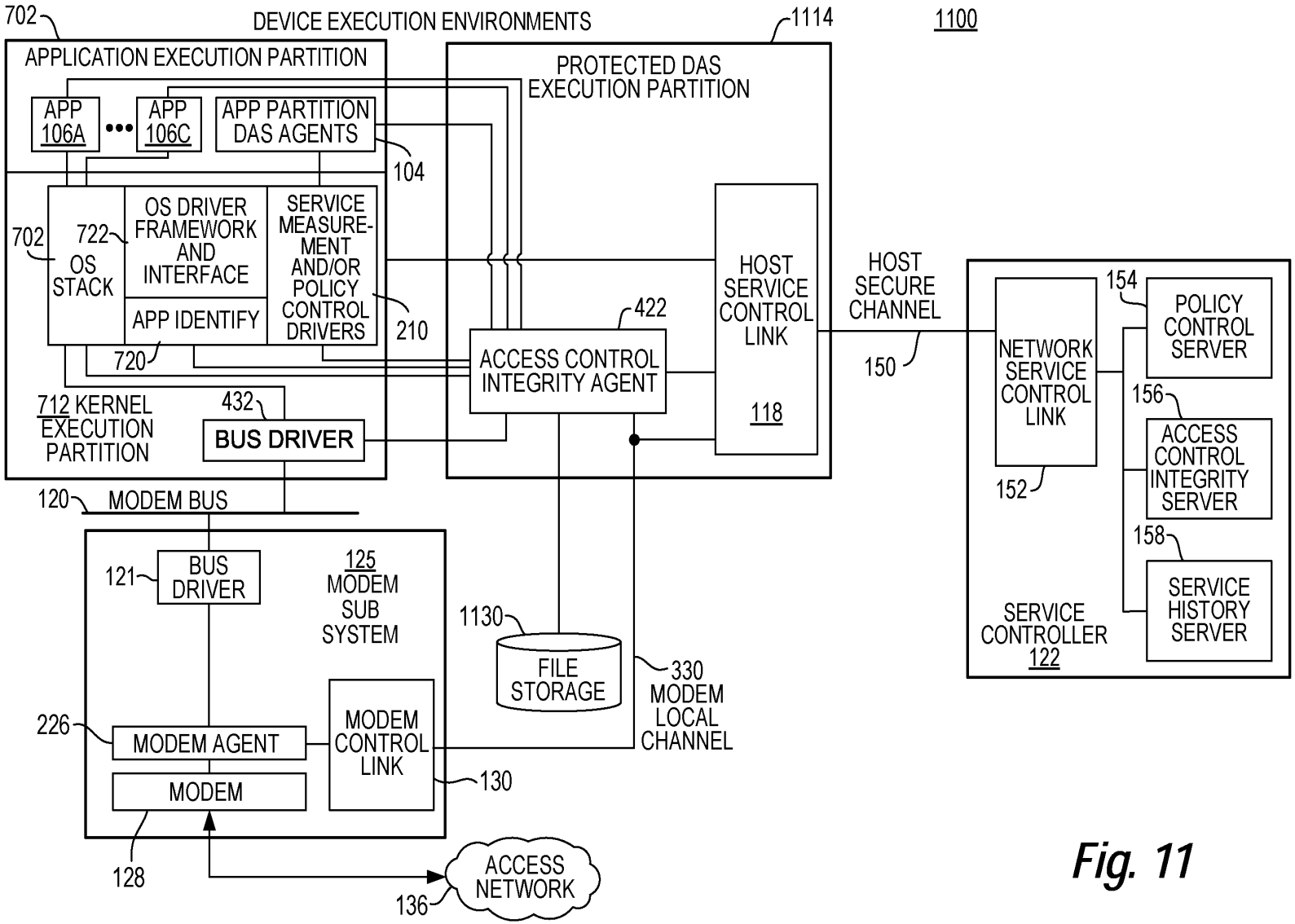
1100
DEVICE EXECUTION ENVIRONMENTS
702
APPLICATION EXECUTION PARTITION
APP 106A
APP 106C
APP PARTITION DAS AGENTS
104
702
722
OS STACK
OS DRIVER FRAMEWORK AND INTERFACE
APP IDENTIFY
720
SERVICE MEASURE-MENT AND/OR POLICY CONTROL DRIVERS
210
712 KERNEL EXECUTION PARTITION
432
BUS DRIVER
1114
PROTECTED DAS EXECUTION PARTITION
422
ACCESS CONTROL INTEGRITY AGENT
HOST SERVICE CONTROL LINK
118
HOST SECURE CHANNEL
150
NETWORK SERVICE CONTROL LINK
152
154
POLICY CONTROL SERVER
156
ACCESS CONTROL INTEGRITY SERVER
158
SERVICE HISTORY SERVER
SERVICE CONTROLLER 122
120
MODEM BUS
121
BUS DRIVER
125 MODEM SUB SYSTEM
226
MODEM AGENT
MODEM
128
MODEM CONTROL LINK
130
1130
FILE STORAGE
330 MODEM LOCAL CHANNEL
ACCESS NETWORK
136

Fig. 11

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Security Techniques for Device Assisted Services
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	Michael Farjami/Evan Gunderman
Attorney Docket Number:	RALEP025C1C1C1C1C1

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	80	80
UTILITY SEARCH FEE	2111	1	350	350
UTILITY EXAMINATION FEE	2311	1	400	400
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**830**

Electronic Acknowledgement Receipt	
EFS ID:	46217129
Application Number:	17867585
International Application Number:	
Confirmation Number:	5955
Title of Invention:	Security Techniques for Device Assisted Services
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Michael Farjami/Evan Gunderman
Filer Authorized By:	Michael Farjami
Attorney Docket Number:	RALEP025C1C1C1C1C1
Receipt Date:	18-JUL-2022
Filing Date:	
Time Stamp:	20:12:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$830
RAM confirmation Number	E20227HK13462103
Deposit Account	500731
Authorized User	Evan Gunderman
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		RALEP025C1C1C1C1C1_CON_App_July_18_22.pdf	606973 393d9a14d142ebf7e127a2364fcf8a914ad572bd	yes	53

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal of New Application	1	2
Application Data Sheet	3	10
Oath or Declaration filed	11	11
Specification	12	40
Claims	41	41
Abstract	42	42
Drawings-only black and white line drawings	43	53

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	44152 e4207ab46de4cdbc95759c48a4d32cad53971df6	no	2

Warnings:

Information:

Total Files Size (in bytes):	651125

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.