República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) **PI0707072-1 A2**

BRPI0707072A2

(22) Data de Depósito: 28/02/2007
(43) Data da Publicação: 19/04/2011
(RPI 2102)

(51) Int.Cl.:
H04Q 7/38

(54) Título: **PROCESSO DE DETECÇÃO DE TENTATIVAS DE INTRUSÃO EM UMA LINHA DE COMUNICAÇÃO, DISPOSITIVO DE VIGILÂNCIA DE COMUNICAÇÃO E AERONAVE**

(30) Prioridade Unionista: 08/03/2006 FR 0602043

(73) Titular(es): AIRBUS FRANCE

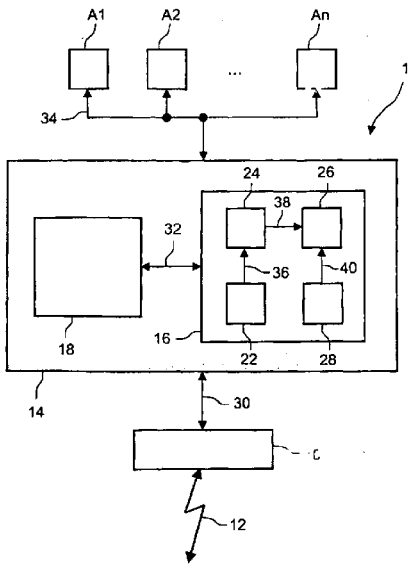
(72) Inventor(es): AGNÈS LECLERCQ

(74) Procurador(es): Antonio Mauricio Pedras Arnaud

(86) Pedido Internacional: PCT EP2007001713 de 28/02/2007

(87) Publicação Internacional: WO 2007/101588de 13/09/2007

(57) Resumo: PROCESSO DE DETECÇÃO DE TENTATIVAS DE INTRUSÃO EM UMA LINHA DE COMUNICAÇÃO, DISPOSITIVO DE VIGILÂNCIA DE COMUNICAÇÃO E AERONAVE. A invenção tem por objeto um processo de detecção de tentativas de intrusão em uma linha de comunicação entre uma aeronave e uma estação no solo, podendo a comunicação ser configurada de acordo com uma pluralidade de níveis de segurança, que compreende as seguintes etapas: a) analisa-se uma mensagem recebida para determinar um nível de segurança correspondente a esta mensaqem; b) compara-se o dito nível de segurança com um nível de segurança associado à comunicação; c) se os níveis de segurança comparados na etapa b) são diferentes, efetua-se uma ação relativa à rejeição da mensagem recebida e ao aviso de uma tentativa de intrusão. A invenção também se refere a um dispositivo para executar este processo.



"PROCESSO DE DETECÇÃO DE TENTATIVAS DE INTRUSÃO EM UMA LINHA DE COMUNICAÇÃO, DISPOSITIVO DE VIGILÂNCIA DE COMUNICAÇÃO E AERONAVE".

A invenção tem por objeto um processo de detecção de tentativas de intrusão em uma linha segura de comunicação entre uma aeronave e uma estação no solo, bem como uma aeronave compreendendo um dispositivo capaz de executar este processo. A invenção também se refere a um dispositivo de detecção de tentativas de intrusão em uma linha segura de comunicação entre uma aeronave e uma estação ao solo, bem como uma aeronave compreendendo tal dispositivo.

As aeronaves modernas, especialmente os aviões de transporte civil, trocam informações com estações baseadas no solo, particularmente estações de controle aéreo ou estações que permitem comunicar com as companhias aéreas que exploram estas aeronaves. As informações trocadas podem especialmente ser relativas a meteorologia, manutenção da aeronave, autorizações do controle aéreo, etc. Esta troca de informações é geralmente realizada por meio de linhas de dados digitais ("datalink" em inglês), correspondendo particularmente aos padrões ACARS ("Aircraft Communications Addressing and Reporting System" em inglês) ou ATN ("Aeronautical Telecommunication Network"em inglês). Após a abertura de uma seção de comunicação, uma aeronave e uma estação no solo trocam mensagens contendo as ditas informações. As linhas de dados consideradas são geralmente do tipo por radiocomunicação ou por satélite. Conseqüentemente, podem ser interceptadas por um pirata: este pode tentar decodificar mensagens transmitidas pela aeronave ou pela estação no solo, mas também enviar mensagens falsas aparentando proceder de uma aeronave ou de uma estação no solo. A fim de proteger as ditas linhas de comunicação contra pirataria, estas linhas podem ser seguras: assim, é possível prever uma autenticação do emissor de uma mensagem e/ou uma codificação das mensagens. Isto pode,

por exemplo, ser realizado por meio de chaves de autenticação e/ou de codificação. Todavia, um pirata pode tentar quebrar estas proteções, especialmente enviando várias mensagens falsas até que uma delas seja eventualmente aceita por uma aeronave ou uma estação no solo. Quanto menor for o número de mensagens falsas recebidas, menor será o risco de aceitação de uma mensagem falsa por uma aeronave ou uma estação no solo. Conseqüentemente, para minimizar este risco de aceitação de uma mensagem emitida por um pirata, é importante detectar as tentativas de intrusão em tal linha de comunicação, a fim de poder informar estas tentativas ao piloto da aeronave e/ou ao pessoal da estação no solo (da companhia aérea ou do controle aéreo) que podem então tomar medidas de vigilância apropriadas.

Estes problemas são resolvidos, pelo menos parcialmente, de acordo com a invenção, por um processo de detecção de tentativas de intrusão em uma linha de comunicação entre uma aeronave e uma estação no solo. Este processo é notável pelo fato de a comunicação poder ser configurada segundo uma pluralidade de níveis de segurança e de compreender as seguintes etapas:

a) quando uma mensagem é recebida por um meio de recepção associado à dita linha, analisa-se esta mensagem para determinar o nível de segurança correspondente a esta mensagem;

b) compara-se o dito nível de segurança correspondente a esta mensagem recebida com um nível de segurança associado à comunicação;

c) se os níveis de segurança comparados na etapa b) forem diferentes, efetua-se uma ação relativa à rejeição da mensagem recebida e ao aviso de uma tentativa de intrusão.

Desta maneira, durante a troca de mensagens em uma linha de comunicação na qual foi previamente estabelecida uma sessão de comunicação entre uma aeronave e uma estação no solo, por um lado, detectam-se as mensagens recebidas

cujo nível de segurança não corresponde ao nível de segurança esperado e, por outro lado, aceitam-se ou rejeitam-se as ditas mensagens recebidas e informam-se supostas tentativas de intrusão na dita linha. O processo de acordo com a invenção apresenta então as vantagens de permitir a rejeição de mensagens enviadas por um pirata além de informar as tentativas de intrusão correspondentes para que um operador humano (piloto, funcionários do controle aéreo ou das companhias aéreas, etc.) possa tomar as providências adequadas.

Em um modo preferido de realização, na etapa c), a dita ação relativa à rejeição da mensagem recebida e ao aviso de uma tentativa de intrusão é escolhida entre as seguintes:

A1) rejeita-se a mensagem recebida e informa-se uma tentativa de intrusão; ou

A2) rejeita-se a mensagem recebida; ou

A3) aceita-se a mensagem recebida.

De um modo preferido, quando se rejeita a mensagem recebida na etapa c), envia-se na dita linha de comunicação uma mensagem informando o emissor da dita mensagem que esta foi rejeitada. Isto apresenta a vantagem que, quando esta mensagem recebida provier de um emissor autorizado, porém com um nível de segurança inapropriado, este emissor é informado da rejeição da dita mensagem.

Vantajosamente, na etapa c), verifica-se, além disso, o valor de um estado de comunicação associado à dita linha e efetua-se a dita ação relativa à rejeição da mensagem recebida e ao aviso de uma tentativa de intrusão em função do dito valor deste estado de comunicação. Este estado de comunicação, em particular, pode corresponder a um estado "estável" ou a um estado "em fase de modificação" do nível de segurança associado à linha de comunicação. Neste caso, quando este estado de comunicação corresponde a um estado "estável", rejeita-se a mensagem recebida e informa-se uma tentativa de

intrusão. Quando este estado de comunicação corresponde a um estado "em fase de modificação", rejeita-se a mensagem recebida sem informar uma tentativa de intrusão, uma vez que esta mensagem pôde ser emitida pelo emissor autorizado (aeronave ou estação no solo) antes que este emissor tenha levado em conta a modificação do nível de segurança.

Ainda de maneira preferida, na etapa b), o nível de segurança associado à comunicação corresponde a um nível de segurança pré-selecionado em meios de gestão de comunicação. Em particular, este nível de segurança pode ser selecionado por um operador humano (piloto, etc.) em função das circunstâncias. Este operador pode especialmente escolher aumentar o dito nível de segurança se ele for informado de uma tentativa de intrusão pelo processo de acordo com a invenção. Geralmente, a fim de modificar o nível de segurança da linha de comunicação, estes meios de gestão de comunicação (de uma aeronave ou de uma estação no solo) enviam uma solicitação endereçada aos meios de gestão de comunicação localizados na outra extremidade da dita linha (respectivamente uma estação no solo ou uma aeronave) para que seja selecionado o mesmo nível de segurança para esta linha.

Em um modo preferido de realização, se os níveis de segurança comparados na etapa b) são diferentes, envia-se na dita linha de comunicação uma mensagem pedindo que o emissor da dita mensagem recebida modifique o nível de segurança da comunicação para igualá-la ao nível de segurança pré-selecionado nos ditos meios de gestão de comunicação. Assim, isto apresenta a vantagem que, quando esta mensagem recebida provier de um emissor autorizado, porém com um nível de segurança inapropriado, será possível efetuar automaticamente uma nova sincronização dos níveis de segurança correspondentes à aeronave e à estação no solo. As mensagens seguintes podem então ser transmitidas com o nível de segurança apropriado.

Em um modo particular de realização da invenção, o nível

de segurança da comunicação é função do tipo de mensagem transmitido. Isto permite adaptar este nível de segurança à importância e à criticidade das mensagens a fim de enviar com um nível de segurança elevado (com custo de envio muitas vezes maior do que um nível de segurança mais baixo) apenas mensagens para as quais isso apresenta uma importância.

De maneira vantajosa, quando, na etapa c), realiza-se a ação A1), além disso, acrescenta-se uma unidade a um contador. Assim, é possível contar as tentativas de intrusão na dita linha de comunicação. Este contador pode, em particular, ser consultado para fins de manutenção ou estatísticas.

Em outro modo particular de realização da invenção, quando na etapa c) realiza-se a ação A2), além disso, acrescenta-se uma unidade a um contador, que é zerado com uma periodicidade predeterminada, e informa-se uma tentativa de intrusão quando o valor do dito contador ultrapassar um valor limite predeterminado. Isto permite detectar as situações nas quais se recebe, em um período predeterminado, um número suficientemente elevado de mensagens cujo nível de segurança é inapropriado, mas cuja recepção isolada não teria sido considerada uma tentativa de intrusão.

Ainda de maneira preferida, na etapa c) realiza-se a ação A1) ou a ação A2) conforme o valor do dito estado de comunicação corresponde respectivamente a um nível de segurança estável ou a um nível de segurança em fase de modificação. Assim, quando se recebe uma mensagem cujo nível de segurança não é apropriado enquanto o nível de segurança associado à linha de comunicação é considerado um estado estável, considera-se que se trata de uma tentativa de intrusão uma vez que o emissor da dita mensagem deveria tê-la enviada com o nível de segurança apropriado. Por outro lado, quando se recebe tal mensagem enquanto o nível de segurança associado à linha de comunicação é considerado em fase de modificação,

considera-se que não se trata de uma tentativa de intrusão. De fato, neste caso é possível que o emissor da mensagem ainda não tenha levado em conta a modificação de nível de segurança associado a esta linha.

A invenção também se refere a um dispositivo de vigilância de comunicação em uma linha de comunicação entre uma aeronave e uma estação ao solo compreendendo:

- meios de emissão/recepção de mensagens nesta linha de comunicação;
- meios de gestão de comunicação ligados aos ditos meios de emissão/recepção.

Este dispositivo é notável pelo fato de, podendo a comunicação ser configurada segundo uma pluralidade de níveis de segurança, ele compreender, além disso, meios de vigilância de comunicação compreendendo:

- primeiros meios capazes de analisar uma mensagem recebida pelos ditos meios de emissão/recepção para determinar um nível de segurança correspondente a esta mensagem;
- segundos meios capazes de comparar o dito nível de segurança correspondente a esta mensagem recebida com um nível de segurança associado à comunicação e de fornecer um resultado de comparação;
- terceiros meios capazes de determinar uma ação associada a esta mensagem recebida em função do resultado de comparação fornecido pelos segundos meios.

Vantajosamente, os terceiros meios são, além disso, capazes de verificar o valor de um estado de comunicação associado à dita linha, e de determinar a dita ação associada à mensagem recebida em função do valor deste estado de comunicação.

Mais vantajosamente, os ditos meios de gestão de comunicação compreendem os ditos meios de vigilância de comunicação.

Mais vantajosamente, os meios de gestão de comunicação compreendem, além disso, meios capazes de gerenciar o valor do dito estado de comunicação associado à dita

linha.

Os ditos meios de emissão/recepção de mensagens são meios de emissão/recepção instalados a bordo da dita aeronave ou na dita estação no solo, conforme se deseja detectar as tentativas de intrusão relativas às mensagens recebidas por esta aeronave ou por esta estação no solo. De maneira preferida, o conjunto do dispositivo de acordo com a invenção é instalado respectivamente nesta aeronave ou nesta estação no solo.

A invenção também se refere a uma aeronave compreendendo um dispositivo de vigilância de comunicação entre uma aeronave e uma estação no solo, tal como precitado.

A invenção será melhor compreendida através da descrição a seguir e do exame da figura anexa.

A figura 1 é um esquema sinóptico de um dispositivo de vigilância de comunicação entre uma aeronave e uma estação no solo de acordo coma invenção.

Para fins de clareza, a descrição a seguir refere-se a um exemplo de aplicação da invenção no caso em que se procura detectar tentativas de intrusão relativas a mensagens recebidas por uma aeronave. Evidentemente, isso não deve ser interpretado de maneira limitativa, uma vez que a invenção se aplica de maneira similar à detecção de tentativas de intrusão relativas a mensagens recebidas por uma estação no solo.

O dispositivo 1 de acordo com a invenção é representado esquematicamente na figura 1. Ele é embarcado a bordo de uma aeronave, particularmente um avião de transporte civil, comunicando com uma estação no solo por meio de uma linha de comunicação 12, em particular uma linha de dados digital ("datalink" em inglês) capaz de ser configurada de acordo com uma pluralidade de níveis de segurança relativamente aos riscos de intrusão nesta linha por um pirata.

Este dispositivo destina-se a vigiar as comunicações nesta linha 12 a fim de detectar as tentativas de intrusão nesta linha 12 por um pirata. Para tal,

dispositivo 1 de acordo com a invenção compreende:

- meios de emissão/recepção 10 de mensagens em uma linha de comunicação 12 entre a dita aeronave e a dita estação no solo, por exemplo, meios de comunicação usuais instalados a bordo desta aeronave (meios de radiocomunicação VHF, HF, meios de comunicação por satélite, etc.);
- meios de gestão de comunicação 14 ligados a estes meios de emissão/recepção 10 por meio de uma ligação 30. Estes meios de gestão de comunicação, em particular, podem fazer parte de um processador que gerencia as comunicações da aeronave, por exemplo, um processador de tipo ATSU ("Air Traffic Services Unit" em inglês);
- meios de vigilância de comunicação 16 compreendendo:
- primeiros meios 22 capazes de analisar uma mensagem recebida pelos meios de emissão/recepção 10 para determinar um nível de segurança associado a esta mensagem;
- segundos meios 24 capazes de comparar este nível de segurança correspondente a esta mensagem recebida com um nível de segurança associado à comunicação e de fornecer um resultado de comparação;
- terceiros meios 26 capazes de verificar o valor de um estado de comunicação associado à linha 12 e de determinar uma ação associada a esta mensagem recebida em função, por um lado, do resultado da comparação fornecido pelos segundos meios 24 e, por outro lado, do valor do dito estado de comunicação.

De maneira preferida, os meios de gestão de comunicação 14 compreendem um roteador 18 que recebe dos meios de emissão/recepção 10, por meio da ligação 30, as mensagens recebidas através da linha de comunicação 12 e que envia cada mensagem para pelo menos uma aplicação de destino A1, A2,..., An por meio de um conjunto de ligações 34. Cada uma das ditas aplicações, em particular, pode ser um aplicativo de informática instalada em um processador da aeronave. Reciprocamente, este roteador coleta as

mensagens provenientes das ditas aplicações, por meio do conjunto de ligações 34, e as transmite, por meio da ligação 30, aos meios de emissão/recepção 10 que as enviam através da linha de comunicação 12.

De maneira preferida, ainda, como representado na figura 1, os meios de vigilância de comunicação 16 são integrados aos meios de gestão de comunicação 14. Eles são ligados ao roteador 18 por meio de uma ligação 32.

Os meios de gestão de comunicação 14 compreendem, além disso, meios 28 capazes de gerenciar um estado de comunicação associado à linha de comunicação 12. Estes meios 28 podem especialmente ser integrados aos meios de vigilância de comunicação 16. Estes meios 28 podem corresponder a uma máquina de estado que pode especialmente compreender pelo menos dois estados: um primeiro estado correspondente a um nível de segurança de comunicação estável e um segundo estado correspondente a um nível de segurança de comunicação em fase de modificação. Este segundo estado corresponde especialmente a uma situação na qual os meios de gestão de comunicação 14 da aeronave transmitiram uma mensagem de solicitação endereçada à estação no solo com o fim de modificar o nível de segurança da comunicação (por exemplo, após um pedido do piloto da aeronave), e na qual os ditos meios de gestão de comunicação 14 da aeronave ainda não receberam um consentimento da estação no solo relativamente a esta modificação de nível. O primeiro estado corresponde especialmente a uma situação na qual os meios de gestão de comunicação 14 da aeronave, após transmitir uma mensagem de solicitação endereçada à estação no solo com o fim de modificar o nível de segurança da comunicação (por exemplo, após um pedido do piloto da aeronave) receberam um consentimento da estação no solo relativamente a esta modificação de nível. Também corresponde a uma situação na qual os meios de gestão de comunicação 14 da aeronave receberam da estação no solo uma solicitação com o fim de modificar o nível de

segurança da comunicação, e transmitiram uma mensagem de consentimento da dita solicitação endereçada à estação no solo.

Quando os meios de gestão de comunicação 14 fizerem parte de um processador de tipo ATSU, os meios de vigilância de comunicação 16 integrados aos ditos meios de gestão de comunicação 14, bem como os primeiros meios 22, os segundos meios 24, os terceiros meios 26 e os meios 28 capazes de gerenciar um estado de comunicação, poderão ser executados sob a forma de programas do dito processador ATSU.

O nível de segurança da comunicação pode especialmente ser escolhido no conjunto de níveis seguintes ou em um subconjunto deste conjunto:

- ausência de segurança da comunicação em relação a riscos de ataque por um pirata;
- autenticação do emissor de uma mensagem, por exemplo, usando chaves de autenticação;
- codificação das mensagens transmitidas na linha de dados 12, por exemplo, usando chaves de codificação;
- autenticação do emissor de uma mensagem e codificação destas mensagens transmitidas na linha de dados 12;

Em um modo preferido de realização da invenção, a comunicação pode ser configurada de acordo com:

- um primeiro nível correspondendo a uma ausência de segurança da dita comunicação en relação a riscos de ataque por um pirata;
- um segundo nível de segurança correspondendo a uma autenticação do emissor de uma mensagem; ou
- um terceiro nível de segurança correspondendo a uma autenticação do emissor de uma mensagem, bem como a uma codificação das mensagens transmitidas na linha de dados 12.

Quando os meios de emissão/recepção 10 recebem uma mensagem da linha de comunicação 12, eles a transmitem, por meio da ligação 30, para os meios de gestão de comunicação 14 onde esta mensagem é recebida pelo

roteador 18. Este último a transmite para os primeiros meios 22 integrados aos meios de vigilância de comunicação 16, por meio da ligação 32. Estes primeiros meios 22 analisam esta mensagem de maneira a determinar o nível de segurança correspondente a esta mensagem. Este nível de segurança é transmitido aos segundos meios 24 por meio da ligação 36. Os ditos segundos meios comparam este nível de segurança com um nível de segurança associado à comunicação, o qual pode especialmente corresponder a um nível de segurança pré-selecionado e memorizado nos meios de gestão de comunicação 14. Em particular, este nível de segurança pode ser pré-selecionado após uma solicitação do piloto ou da estação no solo com o fim de modificar este nível de segurança associado à comunicação. O resultado da comparação entre o nível de segurança correspondendo à mensagem recebida e o nível de segurança associado à comunicação é transmitido pelos segundos meios 24 aos terceiros meios 26, por meio de uma ligação 38.

Quando os ditos níveis de segurança comparados são idênticos, os terceiros meios 26 reenviam para o roteador, por meio da ligação 32, uma informação de aceitação da mensagem correspondente uma vez que, neste caso, não detectaram nenhuma tentativa de intrusão na linha de comunicação 12. O roteador transmite então esta mensagem à aplicação de destino, por meio das ligações 34.

Quando os ditos níveis de segurança comparados são diferentes, os terceiros meios 26 reenviam para o roteador, por meio da ligação 32, uma informação de rejeição da mensagem correspondente. Conseqüentemente, o roteador não transmite esta mensagem à aplicação de destino. De maneira vantajosa, os meios de gestão de comunicação 14 enviam uma mensagem para a estação no solo, pelo intermediário da ligação 30, dos meios de emissão/recepção 10 e da linha de comunicação 12, a fim de informar esta estação no solo da rejeição da dita

mensagem. Estes meios de gestão de comunicação 14 também enviam à estação no solo uma mensagem pedindo a modificação do nível de segurança pré-selecionado na dita estação no solo para igualá-lo ao nível de segurança pré-selecionado nos meios de gestão de comunicação 14 da aeronave. Assim, se a mensagem recebida (e rejeitada) for proveniente da estação no solo, esta poderá tomar as providências apropriadas para reenviá-la com o nível de segurança correto. Além disso, os terceiros meios 26 verificam o valor de um estado de comunicação associado à linha de comunicação 12. Os terceiros meios 26 recebem este estado de comunicação dos meios 28 por meio de uma ligação 40. Este estado de comunicação corresponde a um dos ditos pelo menos primeiro e segundo estados precitados. No caso em que corresponde ao primeiro estado (nível de segurança da comunicação estável), considera-se que há uma tentativa de intrusão na linha de comunicação 12 uma vez que, previamente à recepção da dita mensagem, a comunicação estava estabelecida de maneira estável com um nível de segurança correspondente àquele associado à comunicação. Conseqüentemente, os terceiros meios 26 informam uma tentativa de intrusão. Esta tentativa de intrusão pode, por exemplo, ser informada para um processador (não representada na figura 1) de gestão de alarmes da aeronave de tipo FWC ("Flight Warning Computer" em inglês) ou para um meio de tipo DCDU ("Digital Communications Display Unit" em inglês) ou MCDU ("Multifunction Control Display Unit" em inglês) associado à linha de comunicação 12 e capaz de exibir uma informação relativa à tentativa de intrusão. No caso em que o dito estado de comunicação corresponde ao segundo estado (nível de segurança da comunicação em fase de modificação), não se considera que há uma tentativa de intrusão na linha de comunicação 12 uma vez que, previamente à recepção da dita mensagem, o nível de segurança da comunicação estava em fase de modificação: conseqüentemente, a mensagem recebida pode ser

proveniente da estação no solo, mesmo se isso não for garantido. Os terceiros meios 26 não informam uma tentativa de intrusão neste caso.

Em um modo particular de realização da invenção, quando os ditos níveis de segurança comparados pelos segundos meios 24 são diferentes, se o nível de segurança correspondente à mensagem recebida corresponde ao segundo nível (autenticação do emissor da mensagem) e que o nível de segurança associado à comunicação corresponde ao terceiro nível (autenticação do emissor e codificação da mensagem), os terceiros meios 26 reenviam ao roteador, por meios da ligação 32, uma informação de aceitação da mensagem correspondente. O roteador transmite então esta mensagem à aplicação de destino, por meio das ligações 34. De fato, pode-se considerar que neste caso não há tentativa de intrusão na linha de comunicação 12 uma vez que a mensagem é recebida com uma autenticação do emissor: se esta corresponder à dita estação no solo, estima-se que a mensagem não é proveniente de um pirata tentando uma intrusão na linha de comunicação 12.

De acordo com uma primeira variante da invenção, o nível de segurança da comunicação é comum a todas as mensagens que circulam na linha de comunicação 12 entre a aeronave e a estação no solo.

De acordo com uma outra variante, quando as mensagens que circulam na dita linha de comunicação puderem ser classificadas segundo diferentes tipos de mensagens, o nível de segurança da comunicação é função do tipo de mensagem. Isto apresenta a vantagem de permitir adaptar o nível de segurança à importância e à criticidade das mensagens. Assim, é possível enviar com um nível de segurança elevado (por exemplo, o dito terceiro nível) apenas mensagens para as quais isso apresenta uma importância. Isto permite reduzir os custos de exploração da aeronave quando custo de transmissão de uma mensagem aumentar em função do nível de segurança correspondente a esta mensagem. A título de exemplo, um primeiro tipo de

mensagens denominado ATC ("Air Traffic Control" em inglês) pode corresponder às mensagens trocadas entre a aeronave e o controle aéreo, e um segundo tipo de mensagens denominado AOC ("Airline Operational Control" em inglês) pode corresponder às mensagens trocadas entre a aeronave e a companhia aérea que explora esta aeronave. De maneira preferida, quando os terceiros meios 26 informam uma tentativa de intrusão, além disso, eles acrescentam uma unidade a um contador (não representado na figura 1) nos meios de vigilância de comunicação 16. Este contador pode especialmente ser lido durante operações de manutenção da aeronave para fins estatísticos. Em um modo particular de realização, os meios de vigilância de comunicação 16 compreendem vários contadores e, na ocorrência de uma tentativa de intrusão, acrescenta-se uma unidade a um dos ditos contadores escolhido em função do nível de segurança correspondente à mensagem recebida, do nível de segurança da comunicação e do estado de comunicação associado à linha de comunicação 12. Na variante da invenção segundo a qual o nível de segurança da comunicação é função do tipo de mensagem, pode-se associar um contador à cada tipo de mensagem. Neste caso, quando os terceiros meios 26 informam uma tentativa de intrusão, acrescenta-se uma unidade ao contador associado ao tipo de mensagem correspondente à mensagem recebida.

Em um modo particular de realização da invenção, quando os terceiros meios 26 reenviam ao roteador 18 uma informação de rejeição da mensagem recebida, sem informar uma tentativa de intrusão, além disso, eles acrescentam uma unidade a um outro contador (não representado na figura 1) nos meios de vigilância de comunicação 16. Isto corresponde especialmente ao caso em que o nível de segurança correspondente a mensagem recebida e o nível de segurança da comunicação são diferentes, e em que o estado de comunicação corresponde a um nível de segurança em fase de modificação.

Este contador é zerado com uma periodicidade regular, independentemente da recepção das mensagens. Se chegar a ultrapassar um valor predeterminado, os terceiros meios 26 informam uma tentativa de intrusão. De fato, se for possível considerar que não há tentativa de intrusão durante a recepção de um número limitado de mensagens cujo nível de segurança é inapropriado durante uma modificação de nível de segurança da linha de comunicação 12, não ocorre o mesmo quando este número de mensagens for elevado, em particular, quando for superior ao dito valor predeterminado.

REIVINDICAÇÕES

1. Processo de detecção de tentativas de intrusão em uma linha de comunicação, entre uma aeronave e uma estação no solo, caracterizado pelo fato de a comunicação poder ser configurada segundo uma pluralidade de níveis de segurança e de compreender as seguintes etapas:

a) quando uma mensagem é recebida por um meio de recepção (10) associado à dita linha de comunicação (12), analisa-se esta mensagem para determinar o nível de segurança correspondente a esta mensagem;

b) compara-se o dito nível de segurança correspondente a esta mensagem recebida com um nível de segurança associado à comunicação;

c) se os níveis de segurança comparados na etapa b) forem diferentes, efetua-se uma ação relativa à rejeição da mensagem recebida e ao aviso de uma tentativa de intrusão.

2. Processo, de acordo com a reivindicação 1, caracterizado pelo fato de a dita ação relativa à rejeição da mensagem recebida e ao aviso de uma tentativa de intrusão ser escolhida entre as seguintes:

A1) rejeita-se a mensagem recebida e informa-se uma tentativa de intrusão; ou

A2) rejeita-se a mensagem recebida; ou

A3) aceita-se a mensagem recebida.

3. Processo, de acordo com qualquer uma das reivindicações 1 ou 2, caracterizado pelo fato de, quando se rejeitar a mensagem recebida na etapa c), enviar-se na dita linha de comunicação (12) uma mensagem informando o emissor da dita mensagem que esta foi rejeitada.

4. Processo, de acordo com qualquer uma das reivindicações de 1 a 3, caracterizado pelo fato de, na etapa c), verificar-se, além disso, o valor de um estado de comunicação associado à dita linha e efetuar-se a dita ação relativa à rejeição da mensagem recebida e ao aviso de uma tentativa de intrusão em função do dito valor deste estado de comunicação.

5. Processo, de acordo com qualquer uma das reivindicações de 1 a 4, caracterizado pelo fato de, na etapa b), o nível de segurança associado à comunicação corresponder a um nível de segurança pré-selecionado em meios de gestão de comunicação (14).

6. Processo, de acordo com a reivindicação 5, caracterizado pelo fato de, se os níveis de segurança comparados na etapa b) forem diferentes, enviar-se na dita linha de comunicação (12) uma mensagem pedindo que o emissor da dita mensagem recebida modifique o nível de segurança da dita comunicação para igualá-la ao o nível de segurança pré-selecionado nos ditos meios de gestão de comunicação (14).

7. Processo, de acordo com qualquer uma das reivindicações de 1 a 6, caracterizado pelo fato de o nível de segurança da comunicação ser função do tipo de mensagem transmitido.

8. Processo, de acordo com qualquer uma das reivindicações de 2 a 7, caracterizado pelo fato de, na etapa c), quando se realizar a ação A1), além disso, acrescentar-se uma unidade a um contador.

9. Processo, de acordo com qualquer uma das reivindicações de 2 a 8, caracterizado pelo fato de, na etapa c), quando se realizar a ação A2), além disso, acrescentar-se uma unidade a um contador, que é zerado com uma periodicidade predeterminada, e informar-se uma tentativa de intrusão quando o valor do dito contador ultrapassar um valor limite predeterminado.

10. Processo, de acordo com qualquer uma das reivindicações de 1 a 9, caracterizado pelo fato de a comunicação poder ser configurada de acordo com:

- um primeiro nível correspondendo a uma ausência de segurança da dita comunicação en relação a riscos de ataque por um pirata;
- um segundo nível de segurança correspondendo a uma autenticação do emissor de uma mensagem; ou
- um terceiro nível de segurança correspondendo a uma

autenticação do emissor de uma mensagem, bem como a uma codificação das mensagens transmitidas na linha de dados (12).

11. Processo, de acordo com a reivindicação 10 combinada com qualquer uma das reivindicações de 2 a 9, caracterizado pelo fato de, na etapa c), quando o nível de segurança da mensagem recebida corresponder ao dito segundo nível e o nível de segurança associado à comunicação corresponder ao dito terceiro nível, realizar-se a ação A3).

12. Processo, de acordo com a reivindicação 4 combinada com qualquer uma das reivindicações de 2 a 10, caracterizado pelo fato de, na etapa c) realizar-se a ação A1) ou a ação A2) conforme o valor do dito estado de comunicação corresponder respectivamente a um nível de segurança estável ou a um nível de segurança em fase de modificação.

13. Dispositivo de vigilância de comunicação, em uma linha de comunicação (12), entre uma aeronave e uma estação no solo, compreendendo o dito dispositivo (1):

- meios de emissão/recepção (10) de mensagens nesta linha de comunicação (12);
- meios de gestão de comunicação (14) ligados aos ditos meios de emissão/recepção (10),

caracterizado pelo fato de, podendo a comunicação ser configurada segundo uma pluralidade de níveis de segurança, ele compreender além disso meios de vigilância de comunicação (16) compreendendo:

- primeiros meios (22) capazes de analisar uma mensagem recebida pelos ditos meios de emissão/recepção (10) para determinar um nível de segurança correspondente a esta mensagem;
- segundos meios (24) capazes de comparar o dito nível de segurança correspondente a esta mensagem recebida com um nível de segurança associado à comunicação e de fornecer um resultado de comparação;
- terceiros meios (26) capazes de determinar uma ação

associada a esta mensagem recebida em função do resultado de comparação fornecido pelos segundos meios (24).

14. Dispositivo, de acordo com a reivindicação 13, caracterizado pelo fato de os terceiros meios (26) serem, além disso, capazes de verificar o valor de um estado de comunicação associado à dita linha (12), e de determinar a dita ação associada à mensagem recebida em função do valor este estado de comunicação.

15. Dispositivo, de acordo com qualquer uma das reivindicações 13 ou 14, caracterizado pelo fato de os ditos meios de gestão de comunicação (14) compreenderem os ditos meios de vigilância de comunicação (16).

16. Dispositivo, de acordo com qualquer uma das reivindicações de 13 a 15, caracterizado pelo fato de os meios de gestão de comunicação (14) compreenderem, além disso, meios (28) capazes de gerenciar o valor do dito estado de comunicação associado à dita linha (12).

17. Dispositivo, de acordo com qualquer uma das reivindicações de 13 a 16, caracterizado pelo fato de os meios de emissão/recepção (10) de mensagens serem instalados a bordo da dita aeronave.

18. Dispositivo, de acordo com qualquer uma das reivindicações de 13 a 16, caracterizado pelo fato de os meios de emissão/recepção (10) de mensagens serem instalados na dita estação no solo.

19. Aeronave, caracterizada pelo fato de compreender um dispositivo (1) de vigilância de comunicação como identificado em qualquer uma das reivindicações de 13 a 18.

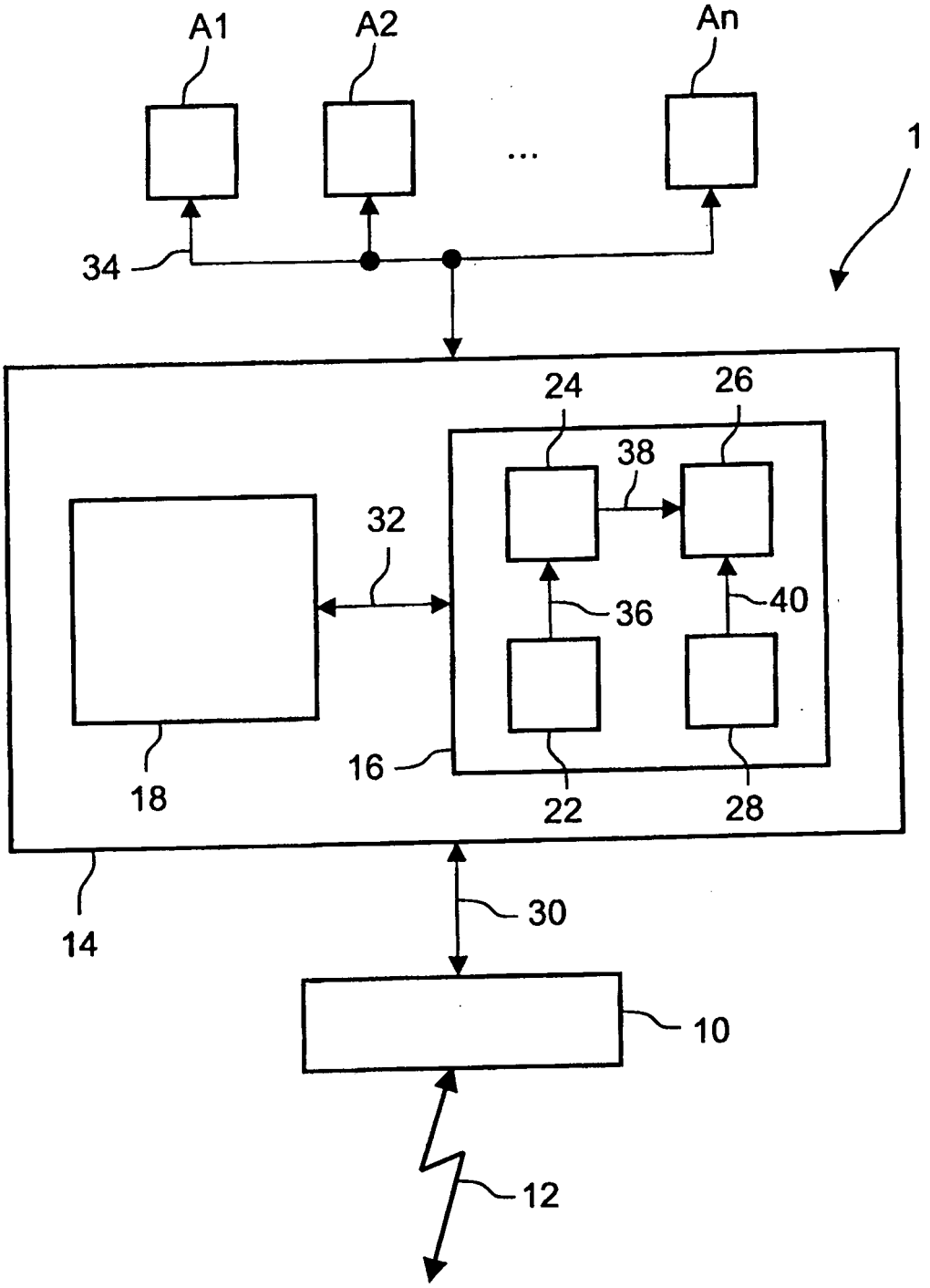


FIG.1

PI0707072-1

RESUMO

"PROCESSO DE DETECÇÃO DE TENTATIVAS DE INTRUSÃO EM UMA LINHA DE COMUNICAÇÃO, DISPOSITIVO DE VIGILÂNCIA DE COMUNICAÇÃO E AERONAVE".

A invenção tem por objeto um processo de detecção de tentativas de intrusão em uma linha de comunicação entre uma aeronave e uma estação no solo, podendo a comunicação ser configurada de acordo com uma pluralidade de níveis de segurança, que compreende as seguintes etapas: a) analisa-se uma mensagem recebida para determinar um nível de segurança correspondente a esta mensagem; b) compara-se o dito nível de segurança com um nível de segurança associado à comunicação; c) se os níveis de segurança comparados na etapa b) são diferentes, efetua-se uma ação relativa à rejeição da mensagem recebida e ao aviso de uma tentativa de intrusão. A invenção também se refere a um dispositivo para executar este processo.