(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
22 janvier 2026 (22.01.2026)

WIPO | PCT

(10) Numéro de publication internationale
WO 2026/017824 A1

(51) Classification internationale des brevets :
H04L 69/04 (2022.01) *H03M 7/30* (2006.01)
H04L 69/22 (2022.01)

(21) Numéro de la demande internationale :
PCT/EP2025/070562

(22) Date de dépôt international :
17 juillet 2025 (17.07.2025)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR2407927 19 juillet 2024 (19.07.2024) FR

(71) Déposant : **ORANGE** [FR/FR] ; 111, quai du Président Roosevelt, 92130 Issy-les-Moulineaux (FR).

(72) Inventeurs : **LAMPIN, Quentin** ; ORANGE - Intellectual Property and Licensing, Orange Gardens - 44 Avenue de la République - CS 50010, 92326 Chatillon (FR). **DUFRENE, Louis Adrien** ; ORANGE - Intellectual Property and Licensing, Orange Gardens - 44 Avenue de la République - CS 50010, 92326 Chatillon (FR). **LARUE, Guillaume** ; ORANGE - Intellectual Property and Licensing, Orange Gardens - 44 Avenue de la République - CS 50010, 92326 Chatillon (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) **Title:** RULE-BASED COMPRESSION METHOD AND CORRESPONDING MANAGEMENT ENTITY

(54) **Titre :** PROCÉDÉ DE COMPRESSION PAR RÈGLES ET ENTITE DE GESTION CORRESPONDANTE

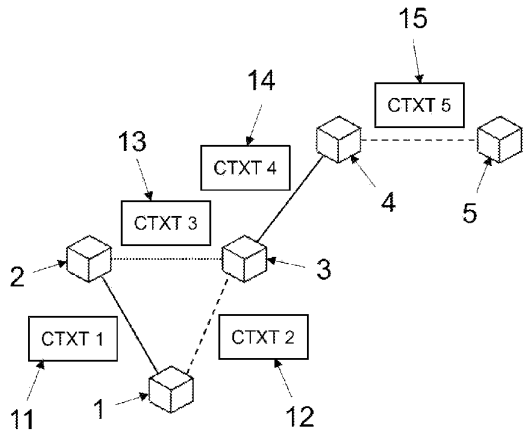


FIG. 1

(57) **Abstract:** The invention relates to a method for determining an identifier of a set of data compression rules, a rule comprising at least one target value of at least one data field, said method being implemented by a data processing unit and comprising: applying a transformation to at least one target value selected from the target values included in the rules of the set of compression rules, the determined identifier resulting from said application.

(57) **Abrégé :** Procédé de détermination d'un identifiant d'un ensemble de règles de compression de données, une règle comprenant au moins une valeur cible d'au moins un champ de données, ledit procédé étant mis en œuvre par une unité de traitement de données et comprenant : appliquer une transformation à au moins une valeur cible sélectionnée parmi les valeurs cibles comprises dans les règles

WO 2026/017824 A1

[Suite sur la page suivante]

MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UY, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— *avec rapport de recherche internationale (Art. 21(3))*

de l'ensemble de règles de compression, l'identifiant déterminé étant le résultat de ladite application.

Description

PROCÉDÉ DE COMPRESSION PAR RÈGLES ET ENTITE DE GESTION CORRESPONDANTE

Domaine technique

[0001] La présente divulgation relève du domaine de la compression et de la décompression de données.

[0002] Elle concerne plus précisément un procédé de détermination d'un identifiant et une entité de gestion correspondante.

[0003] Les télécommunications numériques modernes fonctionnent sur le principe de l'échange de paquets de données entre émetteurs et récepteurs suivant des protocoles tels que le protocole IP (acronyme de l'anglais *Internet Protocol*). Un ensemble de paquets de données relatifs à une communication est envoyé par l'émetteur vers un récepteur. Les paquets contiennent l'adresse du récepteur pour pouvoir lui être adressé grâce à différents algorithmes de routage, et le contenu de la communication est reconstruit par le récepteur en regroupant les données contenues dans les différents paquets. Pour réaliser une communication complète, de nombreux protocoles doivent être utilisés qui remplissent chacun un rôle depuis l'envoi physique de bits, éléments atomiques constituant les données numériques, jusqu'à l'interprétation de données pour les applications informatiques. Les bits sont classiquement regroupés en octets, ensembles de huit bits. Les différents protocoles sont classiquement vus comme étant organisés en couches, un protocole d'une couche s'appuyant sur un protocole d'une couche inférieure. Le modèle OSI (de l'anglais *Open Systems Interconnection*) et le modèle Internet décrivent l'articulation des divers protocoles entre différentes couches.

[0004] Par exemple, dans une version simplifiée, le protocole HTTP (de l'anglais *Hypertext Transfer Protocol*) est un protocole de la couche Application, qui permet de transférer des données vers ou depuis un site web. Les données à transférer sont organisées en paquets de données. Le protocole HTTP utilise le protocole TCP (de l'anglais *Transmission Control Protocol*) qui appartient à la couche Transport, par exemple pour demander le transfert de paquets de données représentant le contenu d'un site web vers un utilisateur. Le protocole TCP, par exemple, fonctionne en trois phases : l'établissement d'une connexion, le transfert de données, et la fin de la connexion. Les protocoles de la couche Transport utilisent un protocole de la couche Réseau, en général le protocole IP (*Internet Protocol*) dans une de ses versions IPv4 ou Ipv6. Ce protocole ne s'intéresse qu'à la transmission de données organisées en paquets d'une adresse vers une autre, sans s'occuper de l'établissement de la connexion ou de l'ordre d'arrivée des paquets de données formant une transmission, ces considérations étant

gérées par le protocole de la couche Transport supérieure. Le protocole IP utilise un protocole de la couche Liaison, par exemple le protocole Ethernet qui organise l'envoi des données élémentaires constituant le paquet, ces données élémentaires étant des bits, transmis en utilisant la couche Physique, que ce soit en utilisant une émission par fibre optique, ou par une communication sans fil suivant les cas.

[0005] D'autres protocoles de la couche Application utilisent d'autres protocoles des couches inférieures pour réaliser leurs fonctions. Par exemple, le protocole CoAP (de l'anglais *Constrained Application Protocol*) utilisé dans le domaine de l'Internet des objets s'appuie en général sur le protocole UDP (de l'anglais *User Datagram Protocol*) de la couche Transport.

[0006] Un point commun à l'ensemble des protocoles sur l'ensemble des couches est l'organisation des données échangées en paquets de données. Un paquet de données est organisé en deux parties : une première partie est l'en-tête (traduction de l'anglais *header*) du paquet qui regroupe les informations nécessaires au protocole qui a la charge de traiter le paquet ; une seconde partie est la charge (traduction de l'anglais *payload*) qui regroupe les données transportées dans le paquet lui-même. Au niveau de la couche Liaison, on parle de trame plutôt que de paquet, et, en plus de l'en-tête, il existe un pied de trame indiquant la fin de la trame.

[0007] Les en-têtes de paquets comprennent des champs. Un champ est un ensemble continu de bits d'une longueur fixe ou variable. Quand un champ est de longueur variable, des mécanismes permettent de savoir quelle est la longueur du champ effectivement transmis. Quand la valeur présente dans un champ de longueur fixe est de longueur variable, des bits de bourrage (traduction de l'anglais *padding*) vont compléter la valeur jusqu'à la longueur fixe du champ. On utilise également le terme bits de remplissage. Un champ dispose d'un identifiant qui indique la nature de la valeur qui est présente dans le champ. Les valeurs présentes dans le champ sont utilisées par le protocole concerné pour traiter le paquet de façon appropriée. Par exemple, dans l'en-tête d'un paquet IP, un champ dont l'identifiant est Version contiendra le numéro de version du protocole utilisé. La taille de ce champ est de quatre bits. D'autres champs concernent par exemple les adresses IP source et destination du paquet. Un en-tête est donc naturellement divisé en plusieurs sections, à savoir les champs de l'en-tête. La charge du paquet peut également être divisée en plusieurs sections, par exemple en définissant des sections d'une longueur constante exprimée en nombre de bits.

[0008] Un outil d'analyse de paquets tel que Wireshark ou tcpdump permet de capturer et analyser des paquets de données. L'analyse permet de séparer un paquet de données échangé sur un réseau entre son en-tête et la charge utile, et de lire les informations comprises dans l'en-tête et les données comprises dans la charge utile et d'identifier les diverses sections d'un paquet, à la fois dans son en-tête et dans sa charge. Nous

rappelons que, à la suite de l'encapsulation des paquets de données, l'en-tête typique d'un paquet sera constitué de plusieurs en-têtes concaténés, un pour chaque protocole encapsulé. Par exemple, une trame Ethernet encapsulant un paquet IP commencera par l'en-tête IP, suivi de l'en-tête UDP. Les champs du paquet IP seront donc suivis dans la trame par les champs du paquet UDP.

[0009] L'ensemble de ces éléments sont bien connus dans l'état de la technique et ne seront pas décrits plus avant.

Technique antérieure

[0010] Il existe un besoin clair de compression des données échangées dans les télécommunications numériques pour économiser au mieux les ressources matérielles et en énergie consommées par les réseaux de télécommunications. Ce besoin explique la création de protocoles dédiés à la compression des paquets de données échangées.

[0011] Les paquets de données échangées sont constitués, comme on l'a vu, d'une part d'un en-tête contenant les informations nécessaires à la transmission du paquet et d'autre part d'une charge utile comprenant les données transmises par le paquet en tant que telles. La compression peut donc porter sur la charge utile, ou bien sur les en-têtes de paquets de données. Comme les valeurs de certains champs des en-têtes de paquets de données vont prendre des valeurs constantes ou variant peu, il est possible de procéder à des compressions très efficaces des paquets de données en cherchant uniquement à comprimer les valeurs des champs des en-têtes des paquets de données.

[0012] Un premier exemple de protocole comprimant les valeurs des champs d'en-têtes de paquets de données est le protocole ROHC (acronyme de l'anglais *Robust Header Compression*) qui est défini par l'organisme de standardisation IETF (pour *Internet Engineering Task Force*) dans le document RFC (*Request For Comments*, documents de spécification à la base d'Internet) numéro 3095. L'idée de base de ce protocole est que certaines valeurs des champs des en-têtes des paquets formant une même communication ne vont pas changer d'une communication sur l'autre. Par exemple, les valeurs des champs d'adresse source et destination vont rester les mêmes pendant une communication. Après un envoi d'un premier paquet contenant les valeurs de ces champs, ces valeurs sont effacées dans les en-têtes des paquets suivants afin de comprimer l'en-tête du paquet, et donc le paquet lui-même, et sont insérées à la réception puisqu'elles sont connues après l'envoi du premier paquet. L'effacement est effectué par un module de compression et l'insertion de la valeur par un module de décompression. D'autres types de compression peuvent être appliqués.

[0013] On obtient ainsi une compression très efficace des paquets de données même si la compression se limite aux en-têtes. Le protocole ROHC est utilisé par exemple dans les réseaux de télécommunications mobiles. Mais il nécessite que soit construit pour

chaque communication un contexte indiquant quelles valeurs peuvent être comprimées, et de quelle manière. Les émetteurs et les récepteurs doivent donc mettre à jour régulièrement les contextes utilisés pour la compression des en-têtes. Cette opération de mise à jour est très coûteuse et d'autres mécanismes vont être préférés dans certains contextes d'utilisation.

[0014] Le contexte des réseaux de communication dédiés aux objets connectés impose des contraintes supplémentaires. On parle ici de réseaux étendus à basse consommation, également dénommés LPWANs, acronyme de l'anglais *Low-Power Wide Area Networks*. Dans un tel réseau, on retrouve des objets connectés qui doivent économiser au maximum leur consommation électrique, comme des compteurs déployés à des endroits n'ayant pas d'alimentation électrique et devant utiliser une batterie pendant plusieurs années. Ces objets communiquent sans fil avec une passerelle qui couvre une zone étendue. La mise à jour du contexte à chaque communication impliquerait une consommation de bande passante élevée, si bien que le protocole ROHC de compression d'en-têtes n'est pas adapté dans ce cadre.

[0015] De plus, les données échangées par ces objets sont souvent de taille très réduite, et peuvent se limiter à signaler que l'objet est toujours actif, ou bien l'objet peut vouloir remonter une seule valeur, telle qu'une température pour un thermomètre, ou un niveau d'eau pour un compteur d'eau. La taille des en-têtes des paquets de données proportionnellement à la taille de la charge utile va donc être proportionnellement plus grande dans le contexte des LPWANs que dans d'autres contextes. Il existe donc un besoin de compression efficace des paquets de données qui, dans le contexte des LPWANs, va se porter sur la compression des valeurs des champs des en-têtes.

[0016] Le protocole SCHC (acronyme de l'anglais *Static Context Header Compression*), défini par l'IETF dans le document RFC numéro 8724, a été conçu pour être utilisé dans le contexte des LPWANs. Il se fonde sur un contexte statique.

[0017] Pour un contexte donné, par exemple un type d'objet connecté déployé dans un réseau donné, des règles de compression vont être définies. Ces règles regroupent des opérations qui peuvent être appliquées aux valeurs des champs des en-têtes de paquets. Ces opérations peuvent être de trois types, toutes fondées sur l'idée que des valeurs de certains champs, ou une partie des valeurs, peuvent être effacées avant transmission puis reconstruites à la réception :

• Un premier type d'opération de compression est l'effacement : la valeur du champ est lue et effacée par le module de compression si la valeur est bien celle attendue. Le module de compression est par exemple situé dans l'objet connecté. La valeur effacée est insérée à la réception par le module de décompression qui, lui, est situé dans la passerelle et qui dispose des mêmes règles que le module de compression. Ce type d'opération est adapté aux champs qui prennent une valeur constante, comme le

champ Version des paquets IP. Si le champ prend une autre valeur que celle attendue, l'opération ne s'applique pas, la règle de compression est ignorée, et une autre règle éventuellement utilisée ou bien la valeur du champ peut être transmise inchangée.

• Un deuxième type d'opération de compression utilise un dictionnaire : un dictionnaire est construit pour certaines valeurs du champ et si la valeur du champ se trouve dans le dictionnaire, le module de compression va remplacer la valeur du champ par son index dans le dictionnaire. Le module de décompression utilise le dictionnaire pour remplacer l'index par la valeur effacée. Là encore, une valeur de champ en-dehors du dictionnaire peut être transmise inchangée si aucune règle ne s'applique.

• Un troisième type d'opération consiste en l'effacement du préfixe : la valeur du champ est une suite de bits, et un préfixe plus ou moins long peut être défini dans une opération de compression. Si la valeur a bien ce préfixe, le préfixe est effacé à la compression et inséré à la décompression, ou bien la valeur est transmise inchangée si le préfixe n'est pas reconnu par l'opération.

[0018] Pour des raisons de complétion, un quatrième type d'opération est défini qui consiste à ignorer la valeur du champ et à la transmettre telle quelle.

[0019] D'autres combinaisons sont possibles, ainsi que d'autres actions de compression/décompression, par exemple pour traiter les champs de longueur variable.

[0020] Un ensemble de règles de compression va alors être défini pour un contexte de déploiement donné. Par exemple, des règles de compression (et leurs règles symétriques de décompression) peuvent être définies pour une passerelle gérant un réseau LPWAN et pour l'ensemble des équipements connectés à ce réseau et à Internet grâce à la passerelle. L'ensemble de règles peut alors traiter en compression et décompression l'ensemble des paquets de données qui s'échangent dans le réseau LPWAN, la compression se limitant aux valeurs des champs des en-têtes. Le protocole SCHC permet de déterminer quelle règle de compression s'applique lorsqu'un paquet de données circule dans le réseau.

[0021] Pour cela, chaque règle de compression présente dans l'ensemble est définie pour un format donné d'en-tête de paquet et va consister en un ensemble d'opérations à appliquer sur les valeurs des champs de l'en-tête d'un paquet qui respecte le format. Plusieurs règles peuvent couvrir un même format d'en-tête de paquet de données. Par exemple, des règles de compression vont être définies pour le format des paquets IP encapsulant un paquet UDP, et ces règles comprendront des opérations pour tous les champs d'un en-tête de paquet IP suivi par un en-tête de paquet UDP.

[0022] Une règle de compression fait partie d'un ensemble de règles et dispose d'un identifiant de règle. L'ensemble de règles va chercher à couvrir l'ensemble des formats possibles d'en-têtes de paquets de données qui peuvent être échangés dans un contexte donné.

[0023] Le protocole SCHC de compression/décompression est appliqué par un module de compression qui va traiter un paquet avant de l'adresser à un module de décompression. Les modules de compression et de décompression disposent du même ensemble de règles, défini pour un contexte donné. Le protocole va consister, lorsqu'un paquet de données doit être traité par le module de compression, à parcourir l'ensemble de règles dont dispose le module de compression afin de retenir une ou plusieurs règles. Si une règle ne correspond pas au format des champs de l'en-tête du paquet traité, la règle n'est pas retenue. Si le format des champs correspond, il faut examiner si les valeurs des champs correspondent à tous les opérateurs de correspondance prévus dans la règle. Si ce n'est pas le cas, la règle là encore n'est pas retenue. Si aucune règle de l'ensemble ne correspond, le paquet est expédié sans traitement. Dans tous les cas, la charge utile du paquet n'est pas traitée par le protocole SCHC. Dans le contexte des LPWANs, la compression du paquet limitée à la compression des valeurs des champs des en-têtes est quand même efficace, car la taille des en-têtes est proportionnellement importante.

[0024] On voit ici l'intérêt de l'opération qui consiste à ignorer la valeur du champ et à la transmettre telle quelle. Cette opération permet de s'assurer qu'une règle pourra effectivement s'appliquer à tous les champs d'un en-tête donné : pour les champs faciles à comprimer, une opération de compression efficace sera définie, et pour les autres champs l'opération qui ne fait rien servira de complétion.

[0025] Finalement, plusieurs règles peuvent être retenues pour lesquelles le format des champs d'une part et les valeurs des champs d'autre part correspondent. Une règle est alors choisie, et une seule, par exemple la première rencontrée dans l'ensemble de règles, ou bien choisie aléatoirement, au choix de l'implémentation du protocole SCHC. Les opérations prévues dans la règle sont appliquées par le module de compression aux valeurs des champs de l'en-tête du paquet. Puis le paquet est transmis avec les valeurs de son en-tête comprimées, ainsi qu'avec l'identifiant de la règle qui a été appliquée. Le module de décompression reçoit le paquet dont les valeurs de l'en-tête ont été comprimées ; utilise l'identifiant de la règle pour trouver les opérations qui ont été appliquées ; et applique les opérations symétriques de décompression. Par exemple, si, pour une valeur d'un champ, l'opération de compression a utilisé un dictionnaire, le module de décompression utilisera la valeur de l'index transmise pour le remplacer par la valeur prévue dans le dictionnaire.

[0026] Comme l'identifiant de la règle utilisée pour la compression doit être transmis, ainsi que certaines valeurs (index des dictionnaires), il va exister une limite au-delà de laquelle ajouter de nouvelles règles de compression dans un contexte donné ne sera plus intéressant car le gain éventuel qu'apporte la règle supplémentaire est dépassé par le coût de transmission induit par l'augmentation de la taille de l'identifiant de

règle au fur et à mesure que de nouvelles règles sont ajoutées. Par exemple, au-delà de huit règles, l'identifiant de règle transmis sera codé sur trois bits au lieu de deux. Si rajouter une neuvième règle ne fait gagner en moyenne qu'un seul bit, l'ajout de cette neuvième règle n'est pas intéressant. De même si une règle ajoutée implique l'utilisation de bits supplémentaires pour encoder les index de dictionnaires.

[0027] Il est facile de voir que les opérations de compression et de décompression dans le protocole SCHC peuvent être sans perte, c'est-à-dire que la décompression de l'en-tête du paquet de données selon les opérations prévues dans le protocole SCHC reconstruit exactement l'en-tête tel qu'il était avant compression. C'est le cas général même s'il peut exister des cadres d'utilisation où ce n'est pas le cas.

[0028] Les ensembles de règles de compression sont donc définies, dans le protocole SCHC, pour un contexte donné, statique, et correspondent aux formats des paquets attendus dans les échanges entre émetteurs et récepteurs. Ils sont définis par un expert qui sait que, dans un contexte de déploiement donné, tel ou tel protocole va être utilisé, selon une encapsulation donnée, et qui sait donc quels formats des en-têtes de paquets sont attendus. L'expert sait également que tel ou tel champ des paquets respectant tel ou tel format prendra une valeur constante, ou bien une valeur parmi un ensemble de taille limitée, ou bien une valeur qui aura souvent le même préfixe. Par exemple, l'expert sait que le champ IP-Version qui apparaîtra dans les en-têtes des paquets respectant plusieurs formats (IP seul, ou IP encapsulant des paquets UDP, ou autre…) sera constante. Ou bien l'expert sait que les valeurs d'adresses IP présentes dans un champ donné appartiennent à une plage limitée et auront donc un préfixe commun. Cette connaissance permet à l'expert de choisir l'opération la plus appropriée pour un champ donné dans un format donné et de l'intégrer dans la règle. L'expert construit donc un ensemble de règles qui sera déployé, par exemple attaché à des modules de compression et de décompression embarqués dans un ensemble d'objets connectés et une passerelle correspondante, pour mettre en œuvre le protocole SCHC.

[0029] Le protocole SCHC a été initialement conçu dans le contexte des réseaux LPWANs mais il pourrait être utilisé dans d'autres contextes, comme les réseaux domestiques, ou pour la compression d'en-têtes de trames Ethernet, ou pour les télécommunications mobiles. En général, les principes de compression de données exposées ici pourraient être utilisés dans tout type de communications par paquet. Les opérations de compression du protocole SCHC pourraient aussi être appliquées à des sections de la charge d'un paquet de données et pas seulement à l'en-tête.

[0030] Dans la situation actuelle, la détermination du contexte est implicitement basée sur le type de liaison utilisé pour la communication. A titre d'exemple, l'utilisation du protocole SCHC selon les principes exposés ci-avant impose un contexte statique et adapté à la technologie de la liaison utilisée.

[0031] Cependant, cette approche présente des limitations, notamment dans des scénarios de communication à sauts multiples ou « multi-sauts » (de l'anglais *multi-hop*) où un même objet connecté peut être amené à interagir avec divers dispositifs de manière distincte. Ces interactions multiples et potentiellement variées peuvent nécessiter des contextes différents, chacun adapté à une communication spécifique. Dans de tels scénarios, l'objet connecté doit gérer simultanément plusieurs contextes de communication, ce qui complique la gestion efficace des interactions et des échanges de données.

[0032] L'approche connue est également inadaptée dans le cas où les contextes sont dynamiques et les ensembles de règles de compression changent avec le temps.

[0033] Il existe un besoin pour un mécanisme capable de faciliter la discrimination efficace de ces contextes multiples tout en minimisant les échanges de données afférents à la résolution de contexte.

[0034] Une telle solution améliorerait significativement les performances globales des réseaux de communication, en particulier de ceux à faible débit.

Résumé

[0035] La présente divulgation vient améliorer la situation.

[0036] Il est proposé un procédé de détermination d'un identifiant d'un ensemble de règles de compression de données, une règle comprenant au moins une valeur cible d'au moins un champ de données,
ledit procédé étant mis en œuvre par une unité de traitement de données et comprenant :
appliquer une transformation à au moins une valeur cible sélectionnée parmi les valeurs cibles comprises dans les règles de l'ensemble de règles de compression, l'identifiant déterminé étant le résultat de ladite application.

[0037] Selon un autre aspect, il est proposé une entité de gestion configurée pour déterminer un identifiant d'un ensemble de règles de compression de données, une règle comprenant au moins une valeur cible d'au moins un champ de données,
l'entité de gestion comprenant :
un module d'application d'une transformation à au moins une valeur cible sélectionnée parmi les valeurs cibles comprises dans les règles de l'ensemble de règles de compression, l'identifiant déterminé étant le résultat de ladite application.

[0038] Selon un autre aspect, il est proposé un procédé de transmission de signal, le procédé comprenant :
une obtention d'au moins un champ de données,
une obtention d'un identifiant d'un ensemble de règles de compression de données comprenant au moins une règle comprenant au moins une valeur cible du champ de données,

une détermination d'un résidu de compression par application de l'ensemble de règles de compression de données au moins au champ de données, et
une transmission d'un signal représentant au moins l'identifiant et le résidu de compression.

[0039] Selon un autre aspect, il est proposé un programme informatique comportant des instructions pour la mise en œuvre de tout ou partie d'un procédé tel que défini dans les présentes lorsque ce programme est exécuté par un processeur. Selon un autre aspect, il est proposé un support d'enregistrement non transitoire, lisible par un ordinateur, sur lequel est enregistré un tel programme.

[0040] Selon un autre aspect, il est proposé un terminal mobile comprenant une entité de gestion telle que définie dans les présentes. Selon un autre aspect, il est proposé un dispositif de communication comprenant une entité de gestion telle que définie dans les présentes.

[0041] La technique proposée permet de déterminer efficacement, de manière rapide et simple, un identifiant à partir d'une ou plusieurs règles de compression de données. La rapidité et la simplicité de la détermination de l'identifiant découlent de l'automatisation du processus de transformation de l'au moins une valeur cible sélectionnée, ainsi que de son caractère direct et déterministe. Ce mode d'obtention est conçu de manière à minimiser, empiriquement, le risque de conflit d'identifiants. Ce faible risque de conflits améliore la fiabilité et la stabilité des connexions. La réduction de la charge de gestion des contextes et l'optimisation de la compression des données permettent une utilisation plus efficace de la bande passante disponible. L'identifiant d'un ensemble de règles de compression qui est déterminé par la technique proposée peut aussi servir d'identifiant d'un contexte donné ou d'un profil donné. Cet identifiant de contexte ou de profil peut être utilisé pour assurer que les participants à une session de communication utilisent les mêmes règles de compression lors de l'émission d'une donnée et de décompression lors de la réception d'une donnée compressée.

[0042] La technique proposée utilise, pour déterminer l'identifiant, une valeur cible sélectionnée. La valeur sélectionnée est sélectionnée parmi les valeurs cibles qui sont présentes dans les règles de compression de données qui appartiennent à l'ensemble de règles de compression pour lequel le procédé selon l'invention va déterminer un identifiant. L'identifiant est déterminé en appliquant une transformation à la valeur cible sélectionnée. La transformation est une opération. Une telle opération prend en entrée au moins une valeur cible ; et le résultat d'appliquer la transformation à la valeur cible est l'identifiant déterrminé. La valeur cible prise en entrée est par exemple exprimée comme une suite de bits, et l'application de la transformation va produire une autre suite de bits qui sera l'identifiant déterminé. La valeur cible peut être exprimée dans d'autres formats, par exemple comme une valeur entière, ainsi

que l'identifiant déterminé. Une transformation appliquée à une valeur cible (par exemple une valeur entière) peut avoir comme résultat un identifiant exprimé dans un autre format (par exemple une suite de bits). Des exemples de transformations ou opérations possibles sont par exemple des permutations ou bien des troncations ou bien des sélections de parties de valeurs en entrée ou bien des opérations de hachage ou bien des opérations arithmétiques ou bien des opérations de hachage ou bien des opérations arithmétiques ou bien des opérations de conversion d'un format dans un autre. La transformation peut également être une combinaison d'opérations. D'autres exemples de transformations sont donnés par la suite. Un exemple de transformation peut être par exemple la combinaison d'opérations suivantes : à partir d'une valeur cible entière, la multiplier par un chiffre donné, puis calculer le haché du résultat selon l'opération de hachage MD5 (ou SHA256 ou toute autre opération de hachage), puis convertir le résultat en suite de bits, puis tronquer la suite de bits obtenue aux huit premiers bits, puis appliquer une permutation donnée à cette suite de huit bits, afin d'obtenir finalement l'identifiant déterminé. Toute autre opération ou combinaison d'opérations peut bien sûr être utilisée comme transformation.

[0043] La technique proposée peut être mise en œuvre indépendamment ou en combinaison avec d'autres méthodes, et peut passer à l'échelle pour être utilisée dans des environnements de communication variés, y compris les réseaux multi-sauts. En étant conçue pour s'intégrer dans le cadre des protocoles de transmission et de compression de données existants, la technique proposée offre une compatibilité ascendante, facilitant son adoption dans les infrastructures de télécommunications actuelles.

[0044] La détermination de l'identifiant peut être mise en œuvre de manière décentralisée par des nœuds d'un réseau de communication, permettant une résolution indépendante de contexte sans transmission explicite d'identifiants de règles entre les nœuds.

[0045] Cette approche améliore l'efficacité des communications entre les dispositifs du système de communication. En réduisant les besoins en transmission de métadonnées, c'est-à-dire de données annexes créées pour les besoins de la communication, la technique proposée optimise la consommation énergétique des dispositifs de communication, prolongeant ainsi leur durée de vie et réduisant les coûts opérationnels. L'élimination de la nécessité de transmettre des identifiants contribue également à la réduction du temps de latence et à l'augmentation de la rapidité des transmissions de données.

[0046] Ces effets techniques combinés se traduisent par une performance accrue, une meilleure qualité de service et une expérience utilisateur améliorée.

[0047] Les caractéristiques exposées dans les paragraphes suivants peuvent, optionnellement, être mises en œuvre, indépendamment les unes des autres ou en combinaison les unes avec les autres.

[0048] Dans un exemple, le procédé comprend une obtention de l'ensemble de règles de compression de données. L'ensemble de règles de compression de données peut être fourni à une entité qui va déterminer l'identifiant ; ou bien, l'ensemble de règles de compression est connu par une entité qui l'utilise et qui va là aussi déterminer l'identifiant.

[0049] Dans un exemple, le procédé comprend en outre une transmission de l'identifiant. La transmission de l'identifiant d'un ensemble de règles de compression permet à un récepteur apte à interpréter l'identifiant d'utiliser un ensemble de règles de décompression approprié pour décompresser des données compressées à l'aide de l'ensemble de règles de compression. Par exemple, dans un réseau IoT où les capteurs envoient des données compressées à une passerelle centrale, la transmission de l'identifiant permet à la passerelle de correctement interpréter et décompresser les données reçues, en permettant de retrouver ultérieurement l'ensemble de règles de compression utilisé, assurant ainsi l'intégrité des informations transmises.

[0050] Dans le domaine des réseaux, un plan est une conception abstraite de l'endroit où se déroulent certains processus. Le terme est utilisé dans le sens de « plan d'existence ». Les deux plans les plus couramment référencés dans les réseaux sont le plan de contrôle et le plan de données (également connu sous le nom de plan de transfert). Le plan de contrôle est la partie d'un réseau qui contrôle la façon dont les paquets de données sont acheminés, c'est-à-dire comment les données sont envoyées d'un endroit à un autre. Dans un exemple, l'identifiant est transmis à une entité du plan de contrôle.

[0051] Dans un exemple, l'identifiant est :
déterminé par une ou plusieurs premières entités du plan de contrôle et/ou du plan de données, et
transmis à une ou plusieurs deuxièmes entités du plan de contrôle et/ou du plan de données,
permettant ainsi à ces deuxièmes entités d'utiliser l'identifiant pour des communications.

[0052] Grâce à ce mode de réalisation, la génération des ensembles de règles de compression peut être centralisée dans une entité du plan de contrôle, y compris la génération des identifiants de ces ensembles, et les informations relatives aux identifiants des ensembles de règles de compression peuvent être transférées à l'intérieur du plan de contrôle pour permettre la mise en place de plusieurs ensembles de compression correspondant aux différents contextes réseau gérées dans le plan de contrôle.

[0053] Ce mode de réalisation permet également d'organiser une génération décentralisée des identifiants des ensembles de règles de compression. Dans ce cas, les identifiants sont générés par des entités réseau pour leurs besoins propres, en partant des

ensembles de règles de compression que ces entités réseau utilisent pour effectuer des compressions, et les identifiants sont transmis pour être utilisés par les entités appartenant au même contexte réseau, qui recevront les compressions effectuées selon des règles de l'ensemble ainsi identifié.

[0054] Dans un exemple, le procédé comprend en outre une vérification d'une unicité de l'identifiant au sein d'une base d'identifiants. La vérification de l'unicité de l'identifiant évite les conflits d'identifiants, améliorant ainsi la stabilité et la fiabilité du réseau. Par exemple, il peut être prévu dans un réseau multi-sauts qu'avant de transmettre un paquet, un nœud vérifie que l'identifiant de contexte n'est pas déjà utilisé à l'échelle de son deux-voisinage, c'est-à-dire de son voisinage immédiat et des voisins de ses voisins. Cela empêche les collisions et garantit que chaque communication utilise un identifiant unique.

[0055] Dans un exemple, l'application de la transformation comprend un encodage et/ou une compression. L'encodage et/ou la compression réduisent la taille de l'identifiant, optimisant ainsi l'utilisation de la bande passante et réduisant le temps de transmission. Il est particulièrement avantageux, dans des réseaux où la bande passante est limitée, tels que des réseaux LPWAN ou LoRaWAN, d'utiliser des identifiants compressés afin de maximiser l'efficacité des transmissions et d'envoyer plus de données utiles par paquet. Dans un exemple, l'encodage est obtenu par une fonction de hachage. Une fonction de hachage transforme des données d'entrée en une empreinte unique. L'encodage est souvent réversible mais peut être irréversible, tandis que le hachage est irréversible.

[0056] Dans un exemple, l'application de la transformation comprend un salage. Le salage ajoute une couche de sécurité en rendant l'identifiant plus difficile à prédire et en réduisant le risque de collisions accidentelles, améliorant ainsi la sécurité et la fiabilité des communications.

[0057] Dans un exemple, le salage est conditionné à une non-unicité d'un précédent identifiant préalablement déterminé par une transformation appliquée à l'au moins une valeur cible et ne comprenant pas ledit salage. Cette méthode permet de résoudre dynamiquement les conflits d'identifiants en appliquant un salage uniquement lorsque nécessaire, simplifiant ainsi à chaque fois que possible le processus de détermination d'identifiants.

[0058] Dans un exemple, le procédé comprend en outre une sélection d'une valeur parmi les valeurs cibles comprises dans les règles de l'ensemble de règles de compression. La valeur cible peut être sélectionnée lors de l'exécution du procédé selon l'invention ou être sélectionnée par ailleurs et fournie à l'entité mettant en œuvre le procédé.

[0059] Dans un exemple, la au moins une valeur cible est sélectionnée selon au moins un critère appliqué à au moins une partie de l'ensemble de règles de compression de

données. Un tel critère est un critère de filtrage qui permet d'isoler une valeur cible précise présente dans une règle de compression appartenant à l'ensemble de règles de compression. Par exemple, le critère utilisé peut être relatif à l'ordre des règles dans l'ensemble des règles et à l'ordre des valeurs dans une règle de l'ensemble ; le critère de filtrage peut être par exemple de sélectionner la première valeur cible présente dans la première règle de l'ensemble de règles de compression.

[0060] Dans un exemple, l'au moins un critère tient compte d'un type de règle et/ou d'une propriété du champ de données. La prise en compte du type de règle et/ou des propriétés des champs de données permet de générer des identifiants plus pertinents et adaptés aux spécificités du réseau et des applications. Par exemple, l'au moins un critère peut tenir compte des propriétés des champs de données spécifiques au(x) protocole(s) de communication utilisé(s) dans un réseau, améliorant ainsi la performance et la fiabilité des échanges de données dans le réseau. Un avantage supplémentaire est que, comme l'identifiant est déduit des champs du jeu de règles, il peut servir de contrôle pour déterminer si le jeu de règles est stable ou s'il a été modifié (accidentellement ou délibérément). Lorsque l'application du critère est conçue pour sélectionner des éléments statiques du jeu de règles, comme des adresses IP, l'identifiant de contexte reste inchangé même si d'autres éléments du jeu de règles changent. Cependant, si le contexte réseau change, les éléments statiques changeront également, entraînant une modification de l'identifiant. Cette approche est heuristique et non une garantie absolue.

[0061] Dans un exemple, l'au moins un critère s'applique aux règles d'effacement complet d'une valeur. Par exemple, l'au moins un critère s'applique seulement aux règles d'effacement complet d'une valeur. En déterminant l'identifiant uniquement à partir de champs qui sont effectivement compressés par effacement complet, on garantit que l'identifiant reste constant tant que ces règles d'effacement complet ne changent pas, même si d'autres règles de compression sont modifiées. Cela peut contribuer à assurer une stabilité de l'identifiant de contexte.

[0062] Dans un exemple, l'au moins une valeur cible sélectionnée est une adresse réseau. Les adresses réseau, telles que les adresses IPv6, sont généralement uniques dans un réseau donné, et un contexte de communication peut souvent être associé ou corrélé à au moins une adresse source et/ou au moins une adresse de destination. Sélectionner une adresse réseau comme valeur cible peut contribuer à assurer que chaque identifiant de contexte est au moins localement distinct et directement lié à la topologie et aux participants du réseau.

Brève description des dessins

[0063] D'autres caractéristiques, détails et avantages apparaîtront à la lecture de la description détaillée ci-après, et à l'analyse des dessins annexés, sur lesquels :

Fig. 1

[0064] [Fig.1] montre un système de communication comprenant une pluralité de nœuds configurés pour communiquer en utilisant un protocole de compression de données, dans un exemple de réalisation.

Fig. 2

Fig. 3

[0065] [Fig.2] et [Fig.3] montrent chacune une règle de compression d'en-tête dans un exemple de réalisation.

Fig. 4

Fig. 5

[0066] [Fig.4] et [Fig.5] montrent deux règles dérivées issues d'un traitement de la règle de compression d'en-tête de [Fig.2], dans un exemple de réalisation.

Fig. 6

[0067] [Fig.6] montre une règle dérivée issue d'un traitement de la règle de compression d'en-tête de [Fig.3], dans un exemple de réalisation.

Fig. 7

[0068] [Fig.7] montre une sélection de champs issue des règles dérivées de [Fig.5] et [Fig.6] ainsi qu'un champ supplémentaire optionnel.

Description des modes de réalisation

[0069] Dans la description qui va suivre, des chiffres de référence identiques désignent des éléments identiques ou ayant des fonctions similaires.

[0070] Quelques termes spécifiques à la présente demande de brevet sont à présent clarifiés pour une meilleure compréhension de la technique proposée.

[0071] Le terme « champ » ou l'expression « champ de données » désigne une unité de données identifiable par sa représentation structurée au sein d'un signal et utilisée pour le traitement ou la transmission des données. Des exemples incluent des champs d'en-tête tels que l'adresse source, l'adresse de destination, le type de service, ainsi que toute métadonnée ou tout champ spécifique dans la charge utile des paquets.

[0072] L'expression « valeur de champ » désigne la donnée ou l'information spécifique contenue dans un champ de données. Des exemples incluent l'adresse IP source, l'adresse IP de destination, ou toute autre valeur dans un champ d'en-tête ou de la charge utile.

[0073] L'expression « propriété de champ » désigne une caractéristique ou un attribut associé à un champ de données. Des exemples incluent la longueur maximale du

champ, le type de données (texte, nombre, adresse IP), ou la valeur par défaut du champ.

[0074] Le terme « identifiant » désigne une donnée ou un ensemble de données permettant de distinguer un objet ou une entité au sein d'un système. Par exemple, un identifiant de champ permet de distinguer un champ parmi un ensemble de champs possibles. L'identifiant d'un champ est ainsi un exemple supplémentaire de propriété de ce champ.

[0075] Selon un autre exemple, un identifiant d'un ensemble particulier de règles de compression de données permet de distinguer cet ensemble particulier de règles de compression de données parmi plusieurs ensembles de règles de compression de données possibles. Lorsqu'un ensemble de règles de compression de données est défini pour un contexte de déploiement, une communication, une session de communication, et/ou un flux de données, alors un identifiant de cet ensemble de règles de compression de données peut être considéré comme équivalent ou substituable à un identifiant de ce contexte de déploiement, de cette communication, de cette session de communication, et/ou de ce flux de données. Le terme « identifiant de contexte unique » (ou *unique context identifier* en anglais) peut être utilisé pour désigner un tel identifiant d'un ensemble particulier de règles de compression de données. En effet, cet identifiant identifie aussi un contexte de communication pour lequel l'ensemble de règles de compression particulier est adapté. Dans certains exemples de réalisation, notamment lorsqu'une approche heuristique est appliquée, il est possible que des identifiants ne soient pas totalement uniques à l'échelle globale d'un réseau. A ce titre, un identifiant de contexte unique est à considérer comme suffisamment distincts pour éviter les conflits dans un contexte local, par exemple à l'échelle du deux-voisinage dans un réseau multi-sauts.

[0076] L'expression « type de règle » désigne une catégorie ou une classification de règles utilisables pour définir des comportements ou des actions sur au moins un champ comprenant au moins une valeur de champ. Des exemples incluent des règles de compression spécifiques telles que "Equal/Not Sent" (si la valeur du champ est égale à une valeur prédéfinie, alors ce champ n'est pas transmis), "Ignore/ Sent" (indépendamment de la valeur du champ, le champ est transmis), ou "Ignore/ Compute" (indépendamment de la valeur du champ, une opération de calcul est effectuée sur sa valeur).

[0077] L'expression « critère appliqué à une règle de compression de données » désigne une condition ou un ensemble de conditions appliquées à la règle de compression de données pour évaluer ou sélectionner des champs, leurs propriétés, et/ou leurs valeurs. Un critère peut tenir compte du type de la règle, des champs eux-mêmes, de leurs propriétés, et/ou de leurs valeurs. Par exemple, un critère peut spécifier de sélectionner

toutes les valeurs de champs auxquels une règle d'un certain type se rapporte et ayant une propriété particulière (par exemple une valeur de champ particulière, ou un identifiant appartenant à une liste d'identifiants prédéterminé). De manière générale, un même critère peut être appliqué à une, plusieurs ou toutes les règles d'un ensemble de règles de compression. Par exemple, il peut être prévu que le critère soit appliqué, ou applicable, à toutes les règles d'un ou plusieurs types particuliers au sein d'un ensemble de règles de compression.

[0078] Le terme « transformation » désigne une opération ou un ensemble d'opérations modifiant la forme, le format et/ou le contenu de données. Des exemples de transformation incluent des opérations de compression et/ou de hachage.

[0079] Le terme « vérification de l'unicité » désigne un processus de validation pour s'assurer qu'un identifiant d'un ensemble de règles de compression de données est unique au sein du système. La vérification peut comprendre par exemple une comparaison de l'identifiant avec une liste d'identifiants connus.

[0080] Le terme « hachage » désigne une fonction mathématique, par exemple une fonction MD5, SHA-128 ou SHA-256, qui convertit des données d'entrée en une chaîne de caractères de longueur réduite également appelée empreinte ou signature. Une caractéristique recherchée d'une fonction de hachage est d'assurer que deux entrées différentes, même proches, auront comme résultat par la fonction de hachage des sorties différentes, alors même que l'espace des valeurs possibles en sortie a une taille très inférieure à celui des valeurs possibles en entrée. Une fonction de hachage cherche donc à minimiser les collisions possibles en sortie. Un hachage est par exemple utilisé pour la vérification de l'intégrité de données et/ou pour la compression de ces données. Une fonction de hachage peut être complétée par une opération de troncature de son résultat pour assurer par exemple que le résultat a une taille donnée et/ou par une opération de poinçonnage (en anglais *puncturing*) par exemple pour améliorer l'efficacité de la compression en éliminant des données redondantes ou non essentielles situées à un emplacement quelconque du résultat de la fonction de hachage. A titre d'exemple, un contrôle de redondance cyclique utilise une procédure de hachage.

[0081] Le terme « salage » désigne un ajout ou une concaténation de données à des données d'entrée avant de les hacher. Le salage est typiquement employé aux fins de renforcer la sécurité de communications étant donné qu'il modifie l'empreinte des données d'entrée. Dans le contexte du présent document, le salage peut être employé pour faciliter la résolution de conflits d'identifiants. Le salage est statique lorsque les données ajoutées aux données d'entrée sont fixes, et il est dynamique lorsque ces données ajoutées sont générées, par exemple aléatoirement.

[0082] L'expression « unité de traitement de données » désigne un composant ou un ensemble de composants matériels et/ou logiciels destiné(s) à exécuter des opérations de traitement sur des données, y compris la détermination des identifiants d'ensembles de règles de compression. Des exemples incluent un processeur, un serveur informatique, ou un dispositif intégré dans un terminal mobile.

[0083] L'expression « entité de gestion » désigne, dans le contexte du présent document, un composant ou un ensemble de composants matériels et/ou logiciels responsables de la gestion d'un système ou d'un service.

[0084] Le terme « module » désigne, dans le contexte du présent document, un composant logiciel ou matériel qui réalise une fonction spécifique dans un système plus large, comme la gestion des règles de compression SCHC. Des exemples incluent un module de compression, un module de transmission, ou un module de gestion d'identifiants.

[0085] L'expression « terminal mobile » désigne un dispositif portable capable de se connecter à un réseau de communication pour échanger des données, en mettant en œuvre des règles de compression. Des exemples incluent un smartphone, une tablette, un ordinateur portable ou tout type d'objet ou dispositif connecté.

[0086] L'expression « dispositif de communication » désigne un appareil ou un ensemble d'appareils permettant l'échange de données entre différents systèmes ou utilisateurs en utilisant un ou des protocoles de communication. Un dispositif de communication peut appliquer des règles de compression et/ou de décompression de données. Des exemples incluent, outre les terminaux mobiles précités et outre des terminaux non mobiles, des équipements de réseau tels qu'un routeur, un modem, une station de base d'un réseau de télécommunications ou une entité de cœur d'un réseau de télécommunications.

[0087] Le terme « traitement » désigne l'ensemble des opérations effectuées sur des données pour obtenir un résultat souhaité, y compris par exemple des opérations de compression, de décompression, de transformation, de transmission, de stockage, d'analyse, etc.

[0088] Le terme « transmission » désigne l'acte ou le processus d'envoi de données d'un point à un autre, en utilisant ou non des règles de compression de données. Des exemples incluent la transmission de paquets de données compressés ou la transmission de messages avec des en-têtes compressés.

[0089] La présente divulgation concerne une technique permettant une détermination efficace et fiable d'un identifiant d'un ensemble de règles de compression de données.

[0090] Il est à présent fait référence à la [Fig.1], qui représente un exemple possible de système de communication convenant pour une mise en œuvre de la technique proposée. Le système de communication comprend une pluralité de nœuds 1, 2, 3, 4, 5, chaque nœud étant un dispositif de communication. L'architecture représentée sur la [Fig.1] peut par exemple correspondre à une architecture multi-sauts, c'est-à-dire celle

d'un système de communication dont les nœuds sont configurés pour être utilisés par d'autres nœuds en tant que relais de communication selon le principe d'un routage à sauts multiples.

[0091] Tous moyens matériels et/ou logiciels adaptés peuvent être utilisés pour la mise en œuvre pratique dudit système de communication et/ou desdits dispositifs de communication. De manière générale, bien que des aspects de la technique proposée puissent être décrits dans le présent document comme étant un processus, un dispositif, un système, une procédure, un procédé ou une méthode, il est à noter que la technique proposée peut également couvrir une mémoire informatique susceptible d'être raccordée à un processeur éventuellement raccordé à une interface de communication, la mémoire stockant des instructions qui, lorsqu'elles sont exécutées par un tel processeur, permettent de réaliser les processus, dispositifs, systèmes, procédures, procédés ou méthodes décrits dans ce document. Parmi les moyens, on compte ceux offerts par des architectures en nuage (traduction de *cloud architecture*) etc.

[0092] Les nœuds sont configurés pour communiquer entre eux en utilisant un protocole de compression de données, c'est-à-dire que chaque communication entre nœuds utilise un ensemble de règles de compression de données, ou contexte de déploiement.

[0093] Dans l'exemple de la [Fig.1], cinq contextes de déploiement sont représentés :
un premier contexte 11 est associé à une communication entre un premier nœud 1 et un deuxième nœud 2,
un deuxième contexte 12 est associé à une communication entre le premier nœud 1 et un troisième nœud 3,
un troisième contexte 13 est associé à une communication entre le deuxième nœud 2 et le troisième nœud 3,
un quatrième contexte 14 est associé à la communication entre le troisième nœud 3 et un quatrième nœud 4, et
un cinquième contexte 15 est associé à la communication entre le quatrième nœud 4 et un cinquième nœud 5.

[0094] Dans l'exemple présenté dans la [Fig.1], par souci de simplification, les contextes correspondent uniquement à des communications point à point entre deux dispositifs de communication distincts. Cette caractéristique n'est pas obligatoire : un contexte peut s'appliquer aux communications entre plus de deux dispositifs de communication. Par exemple, un contexte peut correspondre à un réseau local sans fil, et tous les dispositifs connectés à ce réseau sans fil peuvent partager un même ensemble de règles de compression aptes à compresser efficacement les messages échangés sur le réseau local. La technique présentée s'applique également sans modification aux contextes multicast. Par exemple, dans un réseau de diffusion de contenu multimédia, un serveur de streaming peut diffuser des vidéos à plusieurs récepteurs simultanément. Tous les

récepteurs partageant ce flux peuvent utiliser le même contexte de compression pour recevoir les données de manière efficace. Il est également possible d'avoir plusieurs flux distincts entre les mêmes dispositifs de communication, chacun avec son propre ensemble de règles de compression. Par exemple, dans un contexte où un dispositif de communication envoie simultanément des flux de données de types différents (comme des vidéos en streaming et des messages texte), chaque type de flux peut avoir un ensemble de règles de compression adapté à ses caractéristiques spécifiques. Cela permet d'optimiser la compression pour chaque type de données, améliorant ainsi la performance globale du réseau. De plus, dans un réseau IoT (Internet des objets), un capteur peut envoyer des données à plusieurs dispositifs de collecte. Le même contexte de compression peut être appliqué aux communications entre le capteur et chaque dispositif de collecte, garantissant une transmission efficace des données. Par exemple, des capteurs de température dans une usine peuvent envoyer leurs lectures à différents systèmes de contrôle et de surveillance, tous partageant le même ensemble de règles de compression pour les messages échangés. Ainsi, la flexibilité de la technique permet son application dans divers scénarios de communication, qu'ils soient unicast ou multicast, et pour des flux de données de différentes natures entre les mêmes dispositifs.

[0095] Dans l''exemple de réalisation de la [Fig.1], un exemple d'objectif pouvant être recherché est d'assurer que les contextes associés à une communication impliquant un même nœud (par exemple le premier nœud 1) soient distincts. En d'autres termes, selon cet objectif, il est désirable que chaque nœud utilise un ensemble distinct de règles de compression pour communiquer avec chaque autre nœud.

[0096] En effet, lorsque des contextes de communication simultanément utilisés par un même nœud ne sont pas distincts, il peut en résulter des erreurs de décompression. Par exemple, si le premier nœud 1 utilise le même ensemble de règles de compression pour communiquer avec le deuxième nœud 2 et le troisième nœud 3, les identifiants de règles de compression peuvent devenir ambigus, entraînant des erreurs lors de la décompression des paquets. Cela peut causer une perte de données ou une interprétation incorrecte des paquets reçus, affectant ainsi la fiabilité et la robustesse des communications.

[0097] Ainsi, dans l'exemple considéré, il est souhaitable que :
le premier contexte soit distinct du deuxième contexte et du troisième contexte,
le deuxième, le troisième et le quatrième contexte soient distincts, et
le quatrième contexte soit distinct du cinquième contexte.

[0098] En revanche, il n'y a pas d'inconvénient à ce que le premier contexte soit identique au quatrième contexte, ni à ce que le deuxième ou le troisième contexte soit identique au cinquième contexte, dans la mesure où ces contextes ne sont pas simultanément

actifs pour un même nœud. Plus précisément, les identifiants des contextes peuvent être identiques entre le premier et le quatrième contexte, ainsi qu'entre les identifiants des deuxième ou troisième contextes avec celui du cinquième contexte.

[0099] De manière générale, tant que les nœuds concernés n'ont pas besoin de gérer plusieurs contextes simultanément pour différentes communications, l'utilisation d'ensembles de règles de compression partagés, ou qui partagent un même identifiant, ne pose pas de problème. Cette situation se produit typiquement dans des réseaux où les communications sont suffisamment espacées dans le temps ou gérées par des mécanismes de planification efficaces qui évitent les conflits.

[0100] Un aspect de la technique proposée porte sur un procédé de détermination d'un identifiant d'un ensemble de règles de compression de données (ou de manière équivalente d'un identifiant de contexte de déploiement, pouvant être dénommé identifiant de contexte unique) applicable à tout réseau de communications. Le procédé selon la technique proposée est mis en œuvre par une unité de traitement de données.

[0101] Il comprend, au moins une obtention d'au moins une règle de l'ensemble de règles de compression de données, ladite au moins une règle étant relative à au moins un champ comprenant au moins une valeur de champ.

[0102] Il comprend en outre une détermination de l'identifiant en appliquant une transformation à au moins une valeur de champ sélectionnée selon au moins un critère appliqué à ladite au moins une règle de compression de données.

[0103] Cette technique vise à optimiser la gestion des contextes de compression en garantissant l'unicité des identifiants, minimisant ainsi les risques de conflits et d'erreurs de décompression. L'unicité de l'identifiant de contexte est visée dans un contexte local (deux-voisinage). L'objectif est de garantir que chaque identifiant de contexte est unique au sein de son propre voisinage immédiat, c'est-à-dire les dispositifs avec lesquels il communique directement et ceux avec lesquels ces derniers communiquent. Elle est conçue pour être efficace dans divers types de réseaux utilisant diverses architectures et divers protocoles de communication, y compris les réseaux à faible puissance et à large portée (LPWANs) et les communications multi-sauts.

[0104] La présente technique minimise les conflits d'identifiants et les erreurs de décompression en utilisant des identifiants uniques. Par exemple, dans un réseau multi-sauts, chaque nœud doit s'assurer que ses deux-voisins, c'est-à-dire ses voisins et les voisins de ses voisins, n'utilisent pas le même identifiant de contexte. La gestion des identifiants peut alors être vue comme un problème de coloration de graphe, où chaque arête du graphe représente une communication entre deux nœuds et chaque couleur représente un identifiant distinct. Dans ce contexte, un graphe représente les connexions de voisinage entre dispositifs. Ce graphe de voisinage des contextes n'est pas nécessairement identique au graphe des communications point à point. En

appliquant des concepts issus de la théorie des graphes, il est possible d'assurer que les communications impliquant un même nœud n'utilisent pas des identifiants de contexte conflictuels, améliorant ainsi la fiabilité des communications.

[0105] . Par ailleurs, la théorie des graphes permet de limiter le nombre total d'identifiants nécessaires pour éviter les conflits d'identifiant, diminuant ainsi le nombre de bits requis pour les coder. Cette réduction d'empreinte est particulièrement avantageuse dans des réseaux comme les LPWANs où les ressources en bande passante et en énergie sont limitées.

[0106] La présente technique permet une gestion décentralisée des identifiants, facilitant la mise à l'échelle du réseau et réduisant la complexité de gestion. Chaque nœud peut déterminer de manière indépendante les identifiants de contexte appropriés en fonction des règles de compression de données, sans nécessiter une coordination centrale. Cette décentralisation réduit la complexité et les coûts associés à la gestion centralisée des contextes et permet une mise à l'échelle plus facile du réseau, particulièrement bénéfique dans des environnements où les objets connectés doivent interagir avec divers dispositifs de manière distincte et souvent simultanée.

[0107] À l'inverse, la présente technique permet aussi une gestion plus centralisée des identifiants. Dans un modèle centralisé, une entité centrale est chargée de déterminer les contextes, de calculer les identifiants correspondants et de les transmettre aux dispositifs de communication. Cette approche peut être particulièrement utile dans les réseaux où une coordination stricte est nécessaire pour assurer une performance optimale et éviter les conflits d'identifiants. Dans un réseau centralisé, une entité de gestion du plan de contrôle, telle qu'un serveur de gestion de réseau (NMS, *Network Management System* en anglais) ou un contrôleur SDN (*Software-Defined Networking* en anglais), peut être responsable de la détermination des contextes et de la génération des identifiants. Cette entité centralisée collecte les informations nécessaires depuis les dispositifs de communication, calcule les identifiants appropriés en fonction des règles de compression, et les distribue ensuite aux dispositifs concernés.

[0108] Les ensembles de règles de compression peuvent être obtenus de plusieurs manières. Selon une méthode d'apprentissage par observation du trafic, le trafic réseau est analysé pour identifier les modèles et les caractéristiques des données échangées. Des algorithmes d'apprentissage automatique peuvent être utilisés pour observer le trafic, identifier les régularités et optimiser les règles de compression en conséquence. Par exemple, en observant des flux vidéo, des règles spécifiques à la compression des en-têtes des paquets vidéo peuvent être créées. Alternativement, des règles de compression peuvent être définies manuellement par des administrateurs réseau ou des experts en télécommunications. Ceux-ci utilisent leur connaissance des protocoles et des types de données échangées pour créer des ensembles de règles optimisées pour

des contextes spécifiques. Par exemple, des règles spécifiques peuvent être définies pour compresser les en-têtes IP dans un réseau de capteurs. Alternativement, des ensembles de règles de compression standardisés et définis par des organismes de normalisation tels que l'IETF, par exemple dans les RFCs, peuvent être adoptés et mis en œuvre dans les dispositifs de communication. Optionnellement, les règles de compression peuvent être ajustées dynamiquement en fonction des conditions réseau en temps réel. Par exemple, dans un réseau où la bande passante disponible varie, les règles de compression peuvent être ajustées pour maximiser l'efficacité de la transmission en fonction de la capacité actuelle du réseau.

[0109] Dans un exemple de réalisation, l'obtention d'un identifiant de contexte se fait en plusieurs étapes.

[0110] Une entité de gestion collecte des informations sur le réseau et les dispositifs de communication, ces informations pouvant inclure par exemple les adresses IP, les types de données échangées, les protocoles utilisés, et d'autres paramètres pertinents.

[0111] Les ensembles de règles de compression sont définis selon une ou plusieurs des méthodes exposées ci-avant.

[0112] Des valeurs cibles pertinentes pour les champs de données sont sélectionnées en fonction des règles de compression définies. Cette sélection peut inclure des propriétés statiques comme les adresses IP, les versions de protocole, etc.. Cette sélection est opérée par application d'un ou plusieurs critères de filtrage. Il est souhaitable que ce ou ces critères de filtrage soient judicieusement conçus pour s'assurer que les valeurs cibles sont pertinentes et discriminantes.

[0113] Une transformation, telle qu'un hachage, est ensuite appliquée aux valeurs cibles sélectionnées, cette transformation produisant une séquence de bits unique qui servira d'identifiant de contexte. Il peut être prévu que l'identifiant de contexte ainsi obtenu soit vérifié pour s'assurer de son unicité dans le contexte local ou global, selon les besoins. Ensuite, l'identifiant peut être transmis, par exemple à une entité du plan de contrôle et/ou distribué aux dispositifs de communication concernés. Enfin, l'identifiant peut être utilisé par les dispositifs de communication pour configurer leurs règles de compression et de décompression.

[0114] La technique proposée s'intègre facilement dans les infrastructures existantes, offrant une solution pratique et efficace pour divers environnements de communication, y compris les réseaux LPWANs et les communications multi-sauts. En s'appuyant sur des concepts bien établis de la théorie des graphes et des méthodes de compression de données, cette approche améliore la gestion des contextes de communication de manière transparente. Elle est compatible avec les protocoles de transformation de données actuels, facilitant son adoption dans les infrastructures de télécommunications actuelles et futures.

[0115] Il est à présent fait référence aux figures 2 et 3, qui illustrent deux exemples de règles 21, 22 de compression de données conformément au protocole SCHC. Les principes exposés via cet exemple sont non limitatifs au seul protocole SCHC. Une règle comprend un identifiant de règle (RuleID) et plusieurs descripteurs de champs.

[0116] Chaque descripteur de champ comprend les éléments suivants :
un identifiant (FID) du champ concerné (SCHC) ne traite pas l'en-tête globalement, mais champ par champ), par exemple l'adresse source IPv6,
une longueur (FL) en nombre de bits du champ,
une position (FP) du champ dans l'en-tête de paquet,
un indicateur de direction (DI) indiquant la direction du paquet à laquelle cette description s'applique, trois valeurs étant possibles : Up (Uplink), Dw (Downlink) ou Bi (Uplink et Downlink),
la valeur cible (TV, « Target Value » en anglais), qui est une valeur de référence à laquelle est comparée la valeur du champ,
un opérateur de comparaison (MO, pour « Matching Operator » en anglais), par exemple l'égalité complète (« Equal » en anglais) ou bien l'égalité de seulement les N bits de plus fort poids,
une action de compression et décompression (CDA, pour « Compression Decompression Action » en anglais), qui indique quoi faire si le contenu du champ correspond à la valeur cible : par exemple, ne pas transmettre le champ (« Not-Sent » en anglais, si sa valeur est une valeur connue), ou bien (pour le décompresseur) en recalculer la valeur (« Compute » en anglais) à partir des données.

[0117] Cette définition des descripteurs de champs, incluant des détails supplémentaires tels que la liste exhaustive des actions de compression et décompression possibles, est détaillée par l'IETF dans le document RFC numéro 8724.

[0118] Les exemples de règles fournis dans les figures 2 et 3 sont simplifiés en ce que les règles comprennent un nombre limité de descripteurs de champs. De manière plus générale, les règles peuvent comprendre des descripteurs de l'ensemble des champs susceptibles d'être contenus dans un paquet avant compression de données, incluant par exemple des champs relatifs au protocole IP, des champs relatifs au protocole UDP et des champs relatifs au protocole CoAP.

[0119] Lorsqu'une règle de compression de données, telle que définie par le protocole SCHC conformément à la RFC 8724, est appliquée par un module de compression de données à un paquet comprenant un en-tête composé de plusieurs champs, chaque champ de l'en-tête est traité individuellement selon les descripteurs de champ inclus dans la règle.

[0120] Chaque champ de l'en-tête du paquet est identifié par son identifiant (FID). La valeur du champ est comparée à la valeur cible (TV) définie dans le descripteur de champ

en utilisant l'opérateur de comparaison (MO). Si la valeur du champ correspond à la valeur cible selon l'opérateur de comparaison, l'action de compression (CDA) est appliquée. Par exemple, si l'action est "Not-Sent", le champ n'est pas transmis. Si l'action est "Compute", le champ est recalculé à la réception. Si la valeur ne correspond pas, le champ est inclus dans le résidu de compression.

[0121] La notion de résidu de compression fait référence à la partie de l'en-tête qui n'a pas été compressée et qui doit être transmise avec le paquet. Le résidu de compression peut éventuellement être vide si toutes les valeurs des champs ont été compressées selon les règles de compression appliquées.

[0122] Si une valeur de champ n'est pas compressée parce qu'elle ne correspond pas à la valeur cible, cette valeur est incluse dans le résidu de compression. Cela permet à un module de décompression recevant le paquet à en-tête compressé de reconstruire l'en-tête du paquet original en utilisant les valeurs des champs non compressés transmises dans le résidu de compression.

[0123] La structure d'un paquet de données dont l'en-tête a été compressé par application d'une règle selon la RFC 8724 comprend trois éléments principaux :
l'identifiant (RuleID) de la règle de compression appliquée, cet identifiant permettant au module de décompression de sélectionner la règle appropriée pour décompresser le paquet,
le résidu de compression, qui contient les valeurs des champs de l'en-tête qui n'ont pas été compressés, soit parce qu'ils ne correspondaient pas aux valeurs cibles, soit parce que la règle de compression applicable spécifiait qu'ils devaient être transmis tels quels, et
la charge utile, c'est-à-dire la partie du paquet contenant des données non affectées par le processus de compression d'en-tête.

[0124] On comprend donc que chaque paquet échangé entre nœuds dans un scénario multi-sauts doit inclure un identifiant de règle (RuleID) pour chaque règle de compression appliquée. Cela signifie que si un paquet doit être traité par plusieurs règles de compression, chaque RuleID correspondant doit être inclus dans l'en-tête du paquet. Cela augmente la taille de l'en-tête et, par conséquent, le surcoût de transmission, réduisant ainsi l'efficacité globale des communications.

[0125] Par exemple, considérons le système de la [Fig.1] où les nœuds 1, 2, 3, 4 et 5 sont connectés par paires, dans un scénario multi-sauts. Dans les communications entre nœuds, inclure dans chaque paquet les identifiants de règles nécessaires pour la compression des en-têtes à chaque saut conduit à une duplication d'informations et à un surcoût significatif.

[0126] Dans le même scénario multi-sauts, avec la technique proposée, chaque paquet échangé entre les nœuds n'inclurait qu'un seul identifiant de contexte pour identifier

l'ensemble des règles de compression applicable. Cela réduit considérablement la taille de l'en-tête et donc le surcoût de transmission, améliorant ainsi l'efficacité globale des communications. Il est en outre souhaitable, pour l'application à ce scénario multi-sauts, que l'identifiant de contexte soit calculé de manière à être d'utilisation unique à l'échelle des deux-voisins de chaque nœud.

[0127] La technique proposée présente, selon un aspect, un module de sélection déterministe d'une ou plusieurs valeurs cibles utilisables pour la détermination de l'identifiant de contexte en utilisant les descripteurs de champs des règles de compression. Cette sélection garantit que l'identifiant de contexte peut être reproduit de manière identique à chaque extrémité de la communication.

[0128] Un exemple illustratif de module de sélection heuristique convenant pour mettre en œuvre une telle sélection est à présent exposée, en poursuivant l'exemple des deux règles 21, 22 illustrées en figures 2 et 3. Dans ce but, il est à présent fait référence aux figures 4 à 7.

[0129] Dans un premier temps, les règles sont traitées de manière à séparer les descripteurs de champs applicables au trafic uplink de ceux applicables au trafic downlink.

[0130] Les descripteurs de champs de la première règle 21 sont ainsi dédoublés en :
un premier ensemble 31 de descripteurs de champ applicables au trafic downlink, et
un deuxième ensemble 32 de descripteurs de champ applicables au trafic uplink.

[0131] Ce dédoublement s'effectue en fonction de la valeur de l'indicateur de direction de chaque descripteur de champ :
la valeur 'Dw' indique que le descripteur de champ est applicable au trafic downlink et est donc recensé uniquement dans le premier ensemble 31,
la valeur 'Up' indique que le descripteur de champ est applicable au trafic uplink et est donc recensé uniquement dans le deuxième ensemble 32, et
la valeur 'Bi' indique que le descripteur de champ est applicable à la fois au trafic uplink et au trafic downlink et est donc recensé à la fois dans le premier ensemble et dans le deuxième ensemble 32.

[0132] Un troisième ensemble 33 de descripteurs de champs, applicables au trafic uplink, est formé des descripteurs de champs de la deuxième règle 22, ceux-ci ayant tous la même valeur d'indicateur de direction ('Up').

[0133] Le premier ensemble 31 comprend cinq descripteurs de champs et le deuxième ensemble 32 et le troisième ensemble 33 comprennent chacun six descripteurs de champs.

[0134] Dans un deuxième temps, les ensembles de descripteurs de champs ainsi obtenus sont filtrés selon au moins un critère.

[0135] Dans l'exemple considéré, deux critères sont appliqués successivement.

[0136] Un premier critère est appliqué :

d'une part au premier ensemble 31 en tant que seul ensemble applicable au trafic downlink, et
d'autre part conjointement au deuxième ensemble 32 et au troisième ensemble 33 en tant qu'ensembles de même type, en l'espèce tous deux applicables au trafic uplink.

[0137] Spécifiquement, il s'agit de ne conserver que les descripteurs de champs spécifiant :
un opérateur de comparaison par égalité complète "Equal",
une action de compression "Not-Sent" indiquant que le champ n'est pas transmis, et
une valeur cible identique au sein de chaque ensemble de même type,
et d'exclure les autres descripteurs de champs.

[0138] L'application du premier critère au premier ensemble 31 entraîne :
la conservation de quatre descripteurs de champ dont les identifiants sont « IPv6:SourceAddress », « IPv6:DestinationAddress », « CoAP:Version » et « CoAP:Type »,
ainsi que l'exclusion du descripteur de champ dont l'identifiant est « CoAP:MessageID » car ni l'opérateur de comparaison ni l'action de compression prévues dans ce descripteur de champ ne remplit le premier critère.

[0139] L'application du premier critère aux deuxième et troisième ensembles 32, 33 entraîne :
la conservation de quatre descripteurs de champ dont les identifiants sont « IPv6:SourceAddress », « IPv6:DestinationAddress », « CoAP:Version » et « CoAP:PayloadMarker »,
ainsi que l'exclusion du descripteur de champ dont l'identifiant est « CoAP:MessageID » car ni l'opérateur de comparaison ni l'action de compression prévues dans ce descripteur de champ ne remplissent le premier critère, et
l'exclusion du descripteur de champ dont l'identifiant est« CoAP:Type » car la valeur cible « 0b01 » spécifiée pour ce descripteur de champ au sein du deuxième ensemble 32 est différente de celle « 0b00 » spécifiée pour ce descripteur de champ au sein du troisième ensemble 33, ainsi ce descripteur de champ ne remplit pas le premier critère.

[0140] Un deuxième critère est appliqué : il s'agit de ne conserver, parmi les descripteurs de champ déjà filtrés par application du premier critère, uniquement ceux conservés à la fois pour la gestion du trafic uplink et pour la gestion du trafic downlink.

[0141] L'application du deuxième critère entraîne :
la conservation de trois descripteurs de champ dont les identifiants sont « IPv6:SourceAddress », « IPv6:DestinationAddress », « CoAP:Version » (car présents, après filtration, à la fois au sein du premier ensemble et au sein du deuxième et/ou du troisième ensemble), et

l'exclusion des descripteurs de champ dont les identifiants sont « CoAP:Type » (car absent du deuxième et du troisième ensembles après filtration) et « CoAP:PayloadMarker » (car absent du premier ensemble après filtration).

[0142] Dans un troisième temps, une valeur cible est sélectionnée pour chaque descripteur de champ conservé à l'issue du filtrage.

[0143] Les descripteurs de champ dont les identifiants sont « IPv6:SourceAddress » et « IPv6:DestinationAddress » ont une valeur cible différente selon la direction de trafic considérée.

[0144] Lorsque l'heuristique est mise en œuvre par un émetteur, la direction de trafic pertinente est la direction uplink et il est ainsi choisi de sélectionner, pour ces descripteurs de champs, la valeur cible correspondant au trafic uplink.

[0145] Trois valeurs cibles sont ainsi sélectionnées :
pour l'identifiant « IPv6:SourceAddress », la valeur cible sélectionnée est « [20010db8::04] »,
pour l'identifiant « IPv6:DestinationAddress », la valeur cible sélectionnée est « [20010db8::03] », et
pour l'identifiant « CoAP:Version », la valeur cible sélectionnée est « 0b01 ».

[0146] Dans un quatrième temps, l'identifiant de contexte est déterminé à partir, au moins, des valeurs cibles sélectionnées.

[0147] L'exemple illustratif d'heuristique ainsi détaillé utilise des critères de filtrage conçus de manière à sélectionner des valeurs cibles de champs pertinentes en ce qu'elles sont discriminantes du contexte de déploiement sans a priori que ce soit sur le nombre et la nature des champs de données ou sur les règles de compression employées pour la compression des données.

[0148] Ainsi, ces critères de filtrage sont conçus pour être pertinents pour un grand nombre d'applications utilisant le protocole SCHC, particulièrement dans les réseaux LPWANs et/ou dans des scénarios de communication multi-sauts, mais aussi dans des réseaux LoRaWANs, dans des réseaux MPLS, dans des communications utilisant un schéma de codage TLV, etc...

[0149] Plus généralement, indépendamment du protocole de compression de données utilisées (c'est-à-dire pour un protocole SCHC ou un autre protocole), il est souvent pertinent d'appliquer des critères de filtrage similaires de manière à sélectionner les valeurs cibles les plus discriminantes et représentatives de la configuration du réseau et ainsi assurer l'unicité des identifiants de contexte.

[0150] L'avantage de cette heuristique réside dans sa capacité à sélectionner les valeurs cibles les plus pertinentes pour garantir l'unicité et la représentativité des identifiants de contexte. En filtrant les descripteurs de champs selon des critères stricts, l'heuristique assure que les identifiants générés sont à la fois discriminants et adaptés aux

spécificités du réseau. Cela permet une gestion efficace et fiable des contextes, réduisant les risques de conflits et améliorant la performance globale du réseau. L'heuristique peut être appliquée à des règles de compression utilisant des critères différents, comme les MSB (Most Significant Bit) et LSB (Least Significant Bit). Par exemple, pour des règles où les valeurs cibles sont définies en termes de bits les plus significatifs ou les moins significatifs, des critères de filtrage similaires peuvent être utilisés pour sélectionner les valeurs cibles les plus représentatives.

[0151] Par exemple, il est judicieux de conserver uniquement des valeurs cibles de champs dont les descripteurs spécifient des opérateurs de comparaison stricts (assurant que seules les valeurs identiques sont retenues, ce qui renforce le caractère discriminant du critère de filtrage) et des actions de compression (ou à l'inverse de non-compression) déterministes (de manière à ne laisser aucune ambiguïté sur la manière dont les champs sont traités et ainsi là encore renforcer le caractère discriminant du critère de filtrage).

[0152] Sélectionner des valeurs de champs qui sont statiques dans un contexte réseau donné, comme les adresses IP ou les versions de protocole, permet de garantir la stabilité de l'identifiant de contexte. Prioriser les valeurs de champs qui apparaissent fréquemment dans le trafic réseau assure que l'identifiant de contexte est pertinent pour la majorité des communications.

[0153] Par exemple, lorsqu'un même ensemble de règles de compression de données est utilisé pour gérer des trafics de plusieurs types (par exemple concernant la direction du trafic, uplink, downlink ou bi-directionnel), il est pertinent de ne conserver que des valeurs cibles de champs dont les descripteurs sont communs à tous les types de trafic considérés. La direction de trafic peut être prise en compte par une inversion de certaines valeurs. Par exemple il est pertinent, dans la perspective de s'assurer que les valeurs cibles sélectionnées sont pertinentes pour tous les types de trafic, de comparer une adresse source d'une communication downlink avec une adresse de destination d'une communication uplink et inversement.

[0154] La technique proposée ne saurait toutefois se limiter à l'application d'un ou plusieurs critères particuliers. Selon l'application envisagée, d'autres critères pourraient être appliqués.

[0155] Par exemple, le choix d'un ou plusieurs critères à appliquer pour la sélection d'une ou plusieurs valeurs cibles peut être effectuée de manière experte et en s'appuyant sur des a priori relatif aux champs de données et/ou aux règles de compression utilisées. Par exemple, dans un réseau IoT où les adresses IP sources et destinations sont fixes pour un certain type de communication, le module de sélection peut être configuré pour prioriser la sélection de ces valeurs.

[0156] Par ailleurs la technique proposée ne saurait se limiter à l'application du ou des critères à la totalité de l'ensemble de règles de compression de données à identifier.

Alternativement, il peut être prévu de n'appliquer le ou les critères qu'à une partie de l'ensemble de règles de compression de données, c'est-à-dire seulement à certaines règles de l'ensemble, ou encore seulement à certains descripteurs de champs contenus dans une ou plusieurs règles de l'ensemble.

[0157] Plus généralement, il peut être prévu d'appliquer tout critère de filtrage des descripteurs de champs ou toute combinaison et/ou succession de critères de filtrage des descripteurs de champs à tout ou partie de l'ensemble de règles de compression de données.

[0158] La technique proposée peut en outre être appliquée à tout type de réseau de communication reposant sur tout type de technologie de transmission, et à tout protocole de compression de données utilisant un ensemble d'un nombre quelconque de règles régissant des trafics d'un ou plusieurs types.

[0159] La détermination de l'identifiant de contexte à partir des valeurs cibles sélectionnées est à présent détaillée.

[0160] La [Fig.7] représente un tableau 41 comprenant les valeurs cibles sélectionnées selon l'exemple illustratif d'heuristique et les identifiants des champs correspondants, ainsi qu'une valeur supplémentaire « 0xbeef » dite valeur de salage ou sel, utilisable pour un salage statique.

[0161] Les valeurs cibles sélectionnées (et, optionnellement, la valeur supplémentaire) sont fournies en entrée d'un module de transformation.

[0162] La fonction principale du module de transformation est de déterminer, de manière déterministe, une séquence de bits de longueur inférieure à la somme des longueurs des données qui lui sont fournies en entrée tout en conservant leur caractère distinctif. La séquence de bits ainsi déterminée est ainsi utilisable en tant qu'identifiant de contexte « unique » aux valeurs cibles sélectionnées.

[0163] Le module de transformation comprend par exemple un module de concaténation et un module de hachage.

[0164] Le module de concaténation est configuré pour concaténer tout ou partie des données qui lui sont fournies en entrée. Par exemple, le module de concaténation peut être configuré pour concaténer uniquement les valeurs cibles sélectionnées, ou pour concaténer les valeurs cibles sélectionnées et la valeur supplémentaire, ou encore pour concaténer les valeurs cibles sélectionnées et plusieurs répétitions de la valeur supplémentaire. Alternativement le module de concaténation peut par exemple être remplacé par un module de codage par blocs.

[0165] Le module de hachage est configuré pour déterminer un résultat du hachage des données qui lui sont fournies en entrée. Lorsque le module de hachage reçoit en entrée le résultat de la concaténation des valeurs cibles sélectionnées et de la valeur supplémentaire, le résultat du hachage inclut de manière inhérente un salage statique.

Alternativement, le module de hachage peut par exemple être remplacé par un module de compression appliquant un algorithme tel que Huffman, LZW, etc.

[0166] Le résultat du hachage ou de la compression peut être utilisé directement en tant qu'identifiant de contexte.

[0167] Le résultat du hachage ou de la compression peut également être tronqué et/ou poinçonné pour atteindre une taille inférieure, par exemple une taille souhaitée prédéterminée.

[0168] A titre d'illustration, un exemple de calcul d'un identifiant de contexte est détaillé en se basant sur les valeurs de champ telles qu'indiquées en [Fig.7]. Dans cet exemple, les valeurs de champ sélectionnées, à savoir « 20010db8::04 », « 20010db8::03 » et « 0b01 » sont simplement concaténées et la chaîne de caractères suivante : « 20010db8::0420010db8::030b01 » est obtenue. La chaîne de caractères obtenue est fournie en entrée d'un algorithme de hachage MD5. Un hachage MD5 fournit un résultat déterministe sous la forme d'une chaîne de 32 caractères hexadécimaux. Dans cet exemple, le résultat obtenu est « 816607ec52d01dd4d40efac57e7ab7e6 ». Ce résultat peut être tronqué ou faire l'objet d'un traitement quelconque permettant d'en réduire la taille tout en conservant une propriété d'unicité locale à l'échelle d'un deux-voisinage. Par exemple, il peut être prévu de retenir seuls les quatre derniers bits du codage ASCII du premier caractère du résultat du hachage MD5 en tant que résultat de la transformation des valeurs de champ sélectionnées et d'utiliser ce résultat comme identifiant de contexte. Par exemple, le caractère « 8 » est représenté en code ASCII par la suite de 7 bits « 111000 », dont les quatre derniers bits « 1000 » peuvent être utilisés comme identifiant de contexte.

[0169] L'homme de l'art comprendra aisément que le module de transformation peut comprendre des modules supplémentaires chargés d'apporter des transformations supplémentaires avant ou après codage et avant ou après compression. Par exemple, le module de transformation peut comprendre un module de chiffrement et/ou un module de permutation.

[0170] Le module de transformation peut en outre comprendre des modules de décision, par exemple un module chargé de choisir de concaténer ou non les valeurs cibles sélectionnées avec la valeur supplémentaire et de piloter le module de concaténation en conséquence.

[0171] Un tel module de décision peut par exemple être couplé à un module de négociation d'identifiant.

[0172] Un autre aspect de la technique proposée porte sur un procédé de transmission de signal.

[0173] Le procédé comprend :

une obtention d'au moins un champ de données,

une obtention d'un identifiant d'un ensemble de règles de compression de données comprenant au moins une règle comprenant au moins une valeur cible du champ de données,
une détermination d'un résidu de compression par application de l'ensemble de règles de compression de données au moins au champ de données, et
une transmission d'un signal représentant au moins l'identifiant et le résidu de compression.

[0174] Comme décrit dans les présentes, le champ de données ne saurait être limité à un champ d'en-tête mais peut désigner toute représentation structurée de tout type de donnée(s).

[0175] L'identifiant de l'ensemble de règles de compression de données peut être déterminé de manière déterministe au niveau d'une entité de gestion comprenant :
un module d'obtention de l'ensemble de règles de compression de données, et
un module de détermination de l'identifiant en appliquant une transformation à au moins une valeur cible sélectionnée selon au moins un critère appliqué à au moins une partie de l'ensemble de règles de compression de données. Le module de détermination de l'identifiant peut comprendre par exemple un module de sélection et un module de transformation tels que décrits dans les présentes.

[0176] L'entité de gestion peut être indifféremment localisée au niveau d'un dispositif de communication quelconque (terminal ou équipement de gestion de réseau) pouvant ou non agir en tant qu'émetteur et/ou en tant que récepteur. L'entité de gestion peut être distribuée au niveau d'une pluralité de dispositifs de communication, par exemple au sein d''une architecture en nuage.

[0177] Le « signal représentant au moins l'identifiant et le résidu de compression » peut prendre diverses formes. Il peut contenir l'identifiant de contexte et le résidu de compression en tant que valeurs de champs distinctes. Alternativement, le signal peut contenir un résultat d'une transformation de l'identifiant et/ou du résidu de compression, par exemple une concaténation ou une compression des deux. Cette transformation peut inclure des techniques telles que le salage, le hachage, ou toute autre méthode pertinente pour optimiser la transmission. Par ailleurs, dans le cadre d'un protocole de compression de données tel que le protocole SCHC, le signal peut inclure des représentations compressées de l'identifiant et du résidu de compression selon les règles de compression propres au protocole utilisé, permettant ainsi une transmission efficace et conforme aux spécifications de ce protocole. En somme, le signal peut être configuré pour maximiser l'efficacité et la robustesse de la transmission en adaptant la forme des données transmises selon les besoins spécifiques du réseau et des applications.

[0178] En utilisant des critères de filtrage pour sélectionner les valeurs cibles les plus discriminantes, le procédé de transmission de signal présenté garantit l'unicité et la pertinence des identifiants de contexte, ce qui réduit les risques de collisions d'identifiants et améliore la fiabilité du réseau. Il est applicable à divers types de réseaux et de protocoles de compression, ce qui en fait une solution adaptable et robuste pour la gestion de la compression de données.

[0179] Dans un mode de réalisation, une première entité de gestion détermine l'identifiant de contexte. Cette entité comprend un module d'obtention de l'ensemble de règles de compression de données, un module de sélection qui applique les critères de filtrage aux descripteurs de champs pour sélectionner les valeurs cibles pertinentes, et un module de transformation qui utilise les valeurs cibles sélectionnées pour générer un identifiant de contexte unique.

[0180] Un émetteur met ensuite en œuvre le procédé en obtenant au moins un champ de données et l'ensemble de règles de compression, en appliquant les règles de compression pour déterminer le résidu de compression, et en transmettant un signal incluant l'identifiant de contexte et le résidu de compression.

[0181] Une deuxième entité de gestion, similaire à la première, détermine également l'identifiant de contexte pour un récepteur, garantissant ainsi la cohérence des identifiants de contexte. Le récepteur reçoit ce signal, utilise l'identifiant de contexte pour sélectionner l'ensemble de règles de décompression appropriée, et reconstruit les données originales à partir du résidu de compression.

[0182] Un mécanisme de négociation d'identifiant peut être prévu pour éviter des conflits d'identifiants de contexte qui pourraient tout de même survenir.

[0183] Lorsqu'un nœud (par exemple le nœud 2 de la [Fig.1]) détecte que l'identifiant de contexte utilisé pour communiquer avec un nœud voisin (par exemple, le nœud 1) est identique à celui utilisé pour un autre voisin (par exemple, le nœud 3), un conflit est signalé.

[0184] Pour résoudre le conflit, une valeur de salage ou sel, tel que décrit dans les présentes, peut par exemple être appliquée. Si un conflit persiste après la première application de salage, une nouvelle valeur de salage est appliquée. Ce processus est répété jusqu'à ce qu'aucun conflit ne soit détecté dans le deux-voisinage des nœuds impliqués.

[0185] Spécifiquement, lorsqu'un conflit est détecté, le nœud concerné émet un signal de conflit à ses voisins, incluant l'identifiant de contexte en conflit. Une ou plusieurs des entités de gestion concernée détermine un nouvel identifiant en appliquant une nouvelle valeur de salage et envoie cette information aux nœuds concernés. Les nœuds vérifient ensuite que le nouvel identifiant de contexte, après application du salage, ne génère pas de nouveaux conflits. Si des conflits subsistent, le processus est répété. Si tous les nœuds acceptent, le nouvel identifiant est validé. Ce processus de négociation

assure que les identifiants de contexte sont uniques à l'échelle du deux-voisinage, évitant ainsi les collisions et améliorant la fiabilité des communications dans des réseaux complexes.

[0186] La valeur de salage peut être déployée de plusieurs manières.

[0187] Elle peut être directement fournie aux entités de gestion à l'aide d'une interface ad hoc, ou rendue accessible sous la forme d'une valeur statique stockée dans une base, ou encore incorporée au sein de l'ensemble de règles de compression de données en utilisant des descripteurs de champ fantômes, conçus pour ne jamais être interprétés dans le cadre d'opérations de compression, et spécifiant la valeur de salage comme valeur cible.

Application industrielle

[0188] Les présentes solutions techniques peuvent trouver à s'appliquer dans divers secteurs industriels et technologiques nécessitant des communications efficaces et fiables, telles que l'Internet des objets (IoT), les réseaux de capteurs, les télécommunications, et les systèmes de gestion de réseau. Elles sont particulièrement adaptées pour les environnements à bande passante limitée, les réseaux multi-sauts, et les scénarios nécessitant une faible consommation d'énergie, tout en offrant des solutions robustes pour la gestion des identifiants de contexte et la compression des données.

[0189] La présente divulgation ne se limite pas aux exemples décrits ci-avant, seulement à titre d'exemple, mais elle englobe toutes les variantes que pourra envisager l'homme de l'art dans le cadre de la protection recherchée.

Revendications

[Revendication 1] Procédé de détermination d'un identifiant d'un ensemble de règles de compression de données, une règle comprenant au moins une valeur cible d'au moins un champ de données,
ledit procédé étant mis en œuvre par une unité de traitement de données et comprenant :
appliquer une transformation à au moins une valeur cible sélectionnée parmi les valeurs cibles comprises dans les règles de l'ensemble de règles de compression, l'identifiant déterminé étant le résultat de ladite application.

[Revendication 2] Procédé selon la revendication 1 comprenant une obtention de l'ensemble de règles de compression de données.

[Revendication 3] Procédé selon l'une des revendications 1 ou 2, comprenant en outre une transmission de l'identifiant.

[Revendication 4] Procédé selon l'une des revendications 1 à 3, comprenant en outre une vérification d'une unicité de l'identifiant au sein d'une base d'identifiants.

[Revendication 5] Procédé selon l'une des revendications 1 à 4, dans lequel l'application de la transformation comprend un encodage et/ou une compression.

[Revendication 6] Procédé selon l'une des revendications 1 à 5, dans lequel l'application de la transformation comprend un salage.

[Revendication 7] Procédé selon la revendication 6, dans lequel le salage est conditionné à une non-unicité d'un précédent identifiant préalablement déterminé par une transformation appliquée à l'au moins une valeur cible.

[Revendication 8] Procédé selon l'une des revendications 1 à 7, comprenant en outre une sélection d'une valeur parmi les valeurs cibles comprises dans les règles de l'ensemble de règles de compression.

[Revendication 9] Procédé selon l'une des revendications 1 à 8, dans lequel la au moins une valeur cible est sélectionnée selon au moins un critère appliqué à au moins une partie de l'ensemble de règles de compression de données.

[Revendication 10] Procédé selon la revendication 9, dans lequel l'au moins un critère tient compte d'un type de règle.

[Revendication 11] Procédé selon la revendication 10 dans lequel l'au moins un critère s'applique aux règles d'effacement complet d'une valeur.

[Revendication 12] Procédé selon l'une des revendications 9 à 11, dans lequel l'au moins un critère tient compte d'une propriété du champ de données.

[Revendication 13] Procédé selon la revendication 12 dans lequel l'au moins une valeur cible sélectionnée est une adresse réseau.

[Revendication 14] Entité de gestion configurée pour déterminer un identifiant d'un ensemble de règles de compression de données, une règle comprenant au moins une valeur cible d'au moins un champ de données,
l'entité de gestion comprenant :
un module d'application d'une transformation à au moins une valeur cible sélectionnée parmi les valeurs cibles comprises dans les règles de l'ensemble de règles de compression, l'identifiant déterminé étant le résultat de ladite application.

[Revendication 15] Terminal mobile comprenant une entité de gestion selon la revendication 14.

[Revendication 16] Dispositif de communication comprenant une entité de gestion selon la revendication 14.

[Fig. 1]

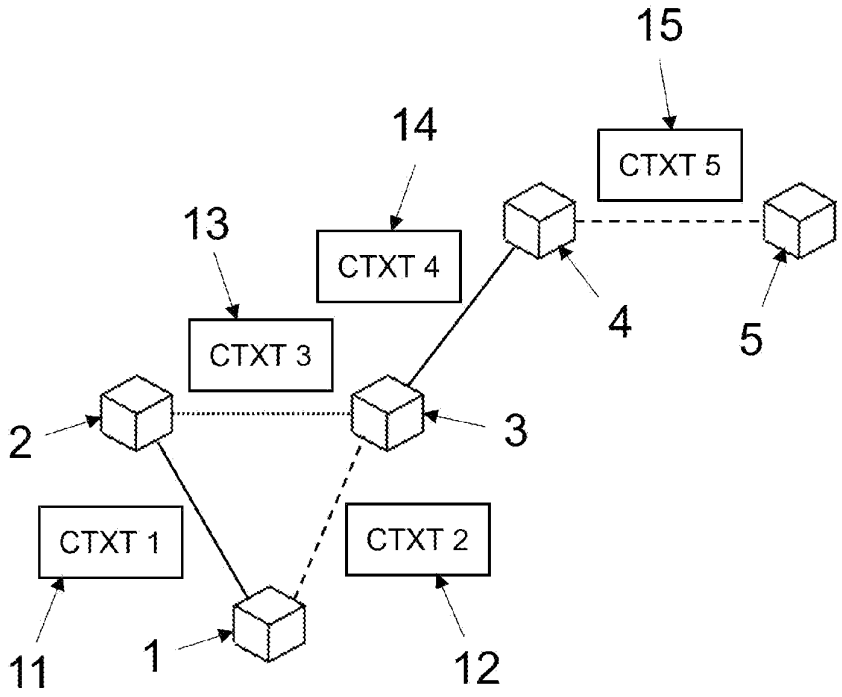


FIG. 1

[Fig. 2]

21

RuleID 1					
FID	FL	FP	DI	MO/CDA	TV
IPv6:SourceAddress	128	0	Up	Equal/ Not-Sent	[20010db8::03]
IPv6:DestinationAddress	128	0	Up	Equal/ Not-Sent	[20010db8::04]
IPv6:SourceAddress	128	0	Dw	Equal/ Not-Sent	[20010db8::04]
IPv6:DestinationAddress	128	0	Dw	Equal/ Not-Sent	[20010db8::03]
CoAP:Version	2	0	Bi	Equal/ Not-Sent	0b01
CoAP:Type	2	0	Up	Equal/ Not-Sent	0b01
CoAP:Type	2	0	Dw	Equal/ Not-Sent	0b10
CoAP:MessageID	16	0	Bi	Ignore/ Value-Sent	N/A
CoAP:PayloadMarker	8	0	Up	Equal/ Not-Sent	0xff

FIG. 2

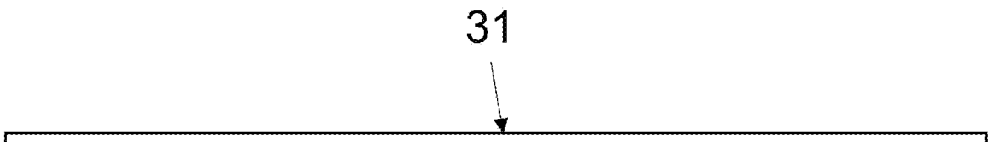
[Fig. 3]

22

RuleID 2					
FID	FL	FP	DI	MO/CDA	TV
IPv6:SourceAddress	128	0	Up	Equal/ Not-Sent	[20010db8::03]
IPv6:DestinationAddress	128	0	Up	Equal/ Not-Sent	[20010db8::04]
CoAP:Version	2	0	Up	Equal/ Not-Sent	0b01
CoAP:Type	2	0	Up	Equal/ Not-Sent	0b00
CoAP:MessageID	16	0	Up	Ignore/ Value-Sent	N/A
CoAP:PayloadMarker	8	0	Up	Equal/ Not-Sent	0xff

FIG. 3

[Fig. 4]



Rule1 (Dw)				
FID	FL	FP	MO/CDA	TV
IPv6:SourceAddress	128	0	Equal/ Not-Sent	[20010db8::04]
IPv6:DestinationAddress	128	0	Equal/ Not-Sent	[20010db8::03]
CoAP:Version	2	0	Equal/ Not-Sent	0b01
CoAP:Type	2	0	Equal/ Not-Sent	0b10
CoAP:MessageID	16	0	Ignore/ Value-Sent	N/A

FIG. 4

[Fig. 5]

32

Rule1 (Up)				
FID	FL	FP	MO/CDA	TV
IPv6:SourceAddress	128	0	Equal/ Not-Sent	[20010db8::03]
IPv6:DestinationAddress	128	0	Equal/ Not-Sent	[20010db8::04]
CoAP:Version	2	0	Equal/ Not-Sent	0b01
CoAP:Type	2	0	Equal/ Not-Sent	0b01
CoAP:MessageID	16	0	Ignore/ Value-Sent	N/A
CoAP:PayloadMarker	8	0	Equal/ Not-Sent	0xff

FIG. 5

[Fig. 6]

33

Rule2 (Up)				
FID	FL	FP	MO/CDA	TV
IPv6:SourceAddress	128	0	Equal/ Not-Sent	[20010db8::03]
IPv6:DestinationAddress	128	0	Equal/ Not-Sent	[20010db8::04]
CoAP:Version	2	0	Equal/ Not-Sent	0b01
CoAP:Type	2	0	Equal/ Not-Sent	0b00
CoAP:MessageID	16	0	Ignore/ Value-Sent	N/A
CoAP:PayloadMarker	8	0	Equal/ Not-Sent	0xff

FIG. 6

[Fig. 7]

41

FID	TV
IPv6:SourceAddress	[20010db8::04]
IPv6:DestinationAddress	[20010db8::03]
CoAP:Version	0b01
Salt	0xbeef

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2025/070562

A. CLASSIFICATION OF SUBJECT MATTER

H04L 69/04(2022.01)i; ***H04L 69/22***(2022.01)i; ***H03M 7/30***(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H03M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GÃ1?4NDOÄ?AN T SCHMIDT HAW HAMBURG M WÃ HLISCH LINK-LAB & FU BERLIN C SCHERB FHNW C MARXER C TSCHUDIN UNIVERSITY OF BASEL C. "Information-Centric Networking (ICN) Adaptation to Low-Power Wireless Personal Area Networks (LoWPANs); rfc9139.txt" 30 November 2021 (2021-11-30), pages 1-25, INFORMATION-CENTRIC NETWORKING (ICN) ADAPTATION TO LOW-POWER WIRELESS PERSONAL AREA NETWORKS (LOWPANS); RFC9139.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARD, INTERNET SOCIETY (ISOC) 4, RUE DES, Retrieved from the Internet: https://tools.ietf.org/html/rfc9139 [retrieved on 2021-11-30] XP015149226 paragraph [4.1.1] paragraph [05.1] paragraph [6.4.2.1] paragraph [08.1] - paragraph [08.2]	1-16

☑ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 October 2025	**14 October 2025**
Name and mailing address of the ISA/EP **European Patent Office** **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands (Kingdom of the)** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	Authorized officer **Aura Marcos, F** Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MINABURO ACKLIO L TOUTAIN IMT-ATLANTIQUE C GOMEZ UNIVERSITAT POLITECNICA DE CATALUNYA D BARTHEL ORANGE LABS JC ZUNIGA SIGFOX A. "Static Context Header Compression (SCHC) and fragmentation for LPWAN, application to UDP/IPv6; draft-ietf-lpwan-ipv6-static-context-hc-23.txt" , No. 23, 28 November 2019 (2019-11-28), pages 1-82, STATIC CONTEXT HEADER COMPRESSION (SCHC) AND FRAGMENTATION FOR LPWAN, APPLICATION TO UDP/IPV6; DRAFT-IETF-LPWAN-IPV6-STATIC-CONTEXT-HC-23.TXT; INTERNET-DRAFT: LPWAN WORKING GROUP, INTERNET ENGINEERING, Retrieved from the Internet: https://tools.ietf.org/html/draft-ietf-lpwan-ipv6-static-context-hc-23 [retrieved on 2019-11-28] XP015136724 paragraph [0003] paragraph [0005] paragraph [07.3] paragraph [8.4.3.1]	1-16
A	802 11 WORKING GROUP OF THE LAN/MAN STANDARDS COMMITTEE OF THE IEEE COMPUTER SOCIETY. "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" , No. D1.0, 01 December 2021 (2021-12-01), pages 1-6544, IEEE DRAFT; DRAFT P802.11REVME_D1.0 REDLINE COMPARED TO D0.4, IEEE-SA, PISCATAWAY, NJ USA, Retrieved from the Internet: https://www.ieee802.org/11/private/Draft_Standards/11me/Draft%20P802.11REVme_D1.0%20Redline%20Compared%20to%20D0.4.pdf [retrieved on 2021-12-01] XP068191568 paragraph [12.4.2]	1-16

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2025/070562

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

INV. H04L69/04 H04L69/22 H03M7/30
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L H03M

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	GÃ1?4NDOÄ?AN T SCHMIDT HAW HAMBURG M WÃ HLISCH LINK-LAB & FU BERLIN C SCHERB FHNW C MARXER C TSCHUDIN UNIVERSITY OF BASEL C: "Information-Centric Networking (ICN) Adaptation to Low-Power Wireless Personal Area Networks (LoWPANs); rfc9139.txt", INFORMATION-CENTRIC NETWORKING (ICN) ADAPTATION TO LOW-POWER WIRELESS PERSONAL AREA NETWORKS (LOWPANS); RFC9139.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARD, INTERNET SOCIETY (ISOC) 4, RUE DES , 30 novembre 2021 (2021-11-30), pages 1-25, XP015149226, Extrait de l'Internet: URL:https://tools.ietf.org/html/rfc9139 [extrait le 2021-11-30] alinéa [4.1.1] -/--	1-16

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
6 octobre 2025	14/10/2025

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Aura Marcos, F

1

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
	alinéa [05.1] alinéa [6.4.2.1] alinéa [08.1] - alinéa [08.2] -----	
A	MINABURO ACKLIO L TOUTAIN IMT-ATLANTIQUE C GOMEZ UNIVERSITAT POLITECNICA DE CATALUNYA D BARTHEL ORANGE LABS JC ZUNIGA SIGFOX A: "Static Context Header Compression (SCHC) and fragmentation for LPWAN, application to UDP/IPv6; draft-ietf-lpwan-ipv6-static-context-hc-23 .txt", STATIC CONTEXT HEADER COMPRESSION (SCHC) AND FRAGMENTATION FOR LPWAN, APPLICATION TO UDP/IPV6; DRAFT-IETF-LPWAN-IPV6-STATIC-CONTEXT-HC-23 .TXT; INTERNET-DRAFT: LPWAN WORKING GROUP, INTERNET ENGINEERING , no. 23 28 novembre 2019 (2019-11-28), pages 1-82, XP015136724, Extrait de l'Internet: URL:https://tools.ietf.org/html/draft-ietf -lpwan-ipv6-static-context-hc-23 [extrait le 2019-11-28] alinéa [0003] alinéa [0005] alinéa [07.3] alinéa [8.4.3.1] -----	1-16
A	802 11 WORKING GROUP OF THE LAN/MAN STANDARDS COMMITTEE OF THE IEEE COMPUTER SOCIETY: "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE DRAFT; DRAFT P802.11REVME_D1.0 REDLINE COMPARED TO D0.4, IEEE-SA, PISCATAWAY, NJ USA , no. D1.0 1 décembre 2021 (2021-12-01), pages 1-6544, XP068191568, Extrait de l'Internet: URL:https://www.ieee802.org/11/private/Dra ft_Standards/11me/Draft%20P802.11REVme_D1. 0%20Redline%20Compared%20to%20D0.4.pdf [extrait le 2021-12-01] alinéa [12.4.2] -----	1-16

1