Liaisons chiffrées TTY on line par radio HF

Autor(en): **Kirchhofer, Kirk H.**

Objekttyp: **Article**

Zeitschrift: **Pionier : Zeitschrift für die Übermittlungstruppen**

Band (Jahr): **53 (1980)**

Heft 10

PDF erstellt am: **26.04.2024**

Persistenter Link: https://doi.org/10.5169/seals-562325

Kirk H. Kirchhofer

Liaisons chiffrées TTY on line par radio HF

pv. Liaisons sûres, secrètes ou non, mais exemptes d'erreurs sont les préoccupations de tout transmetteur quel que soit l'échelon du réseau.
Harris Corporation, Communication and Information Processing, RF Communications Divisions, Rochester New York, vient de mettre au point un système ARQ (Automatic Repeat Request) c.-à-d. demande automatique de répétition, permettant un contrôle constant de l'exactitude de la transmission, chiffrée ou non.
Equipement Distributors Ltd, Genève dont l'administrateur, A.M. Juillard, est par ailleurs administrateur du bureau administratif Harris Europe Afrique – nous a fourni cet article – nous informe que des démonstrations effectuées en juin 1980 à partir de l'Espagne sur Rochester, New York en ARQ et en ARQ chiffré se sont révélées être un éclatant succès: le trafic a été transmis à la perfection, lettre par lettre, dans les deux sens avec l'amplificateur de puissance hors service et utilisation de la seule alimentation 125W malgré des conditions d'essais très défavorables (mauvaise période dans la journée, antenne d'émission misérable, bruits électriques très forts dus à l'environnement urbain).

Possibilités d'utilisation

Le titre laisse supposer que le système étudié est exclusivement utilisé par les forces navales et aériennes. Il n'y a cependant aucune restriction: les forces terrestres et, bien entendu, les ministères de la Défense ou les services diplomatiques ont à résoudre les mêmes problèmes de transmission et peuvent mettre en œuvre le système en question.
Le système pourrait fort bien être le poste du bureau privé d'un ministre des Affaires étrangères, alors que l'installation embarquée pourrait être l'un des nombreux postes d'une ambassade appartenant à un réseau diplomatique de transmissions. Il faut souligner un autre point: l'accent est mis sur des liaisons sûres et exemptes d'erreurs. L'emploi de microprocesseurs nous aide à réaliser un système de détection et de correction des erreurs qui est bien supérieur à tout ce qui était disponible il y a seulement cinq ans.
Vous êtes responsable des transmissions à bord d'un patrouilleur rapide et vous recevez le message suivant sur votre téléimprimeur (TTY):
from: cdr op-43
to: FPB – L 19
urgent
move immedvketely to position a4/q19 to support fpb 1 24/29 stop enemy activiqd expected: two or tpree craft with inferiol armament stop
Grâce à la redondance de la langue anglaise (ou de toute autre langue pour le sujet qui nous préoccupe) vous avez pu saisir le sens du message, bien qu'il contienne un certain nombre d'erreurs. Supposons maintenant que vous receviez un autre massage, mais chiffré celui-là:
rfgzh jknmb tfvoq arfcd bnhrp lmktr hgfix asitw rgdcm ikzhw gvjkn olejv eefon zhbop paecv lkjbu edeefxcx 2"33:21mlljnbnn kkjmjutrf hertd kikjf rfdse bnbgz6453(20066(..,-7..
Après déchiffrement au moyen de la clé appropriée vous pouvez lire:
from cdr fpb 1–16
to: fpb 1–19
urgent
four (4) unidentified small vessels in the.,–176(mdehbd-lenhthfgtn//'.–...lmnjdhelp herevvbhplsn((.,
sans espoir...

Cela est sans aucun doute dû aux interférences en cours de propagation comme en rencontrent les ondes radio HF.

Télécommunications HF sur grande distance

Le radio HF est aujourd'hui d'un emploi aussi répandu qu'il y a dix ou douze ans sur les grandes distances. Malheureusement les lois physiques ne peuvent être changées: l'influence des conditions ionosphériques pose toujours de graves problèmes: taches solaires et interférences qui en découlent, bruit radioélecrique et propagation suivant des trajectoires multiples. Ces facteurs étant responsables d'erreurs dans la transmission des signaux télégraphiques, il faut trouver les moyens de détecter et de corriger les erreurs.

Détection et correction des erreurs

Un code simple de correction des erreurs télégraphiques n'a pas besoin de voie inverse (simplex seulement) et il est parfois qualifié de système FEC (Forward Error Correction), notamment lorsqu'il est utilisé en modes diffusion. Un code sophistiqué de correction des erreurs peut être considéré comme un code disposant d'un nombre suffisant d'éléments de signaux supplémentaires (bits redondants) pour indiquer et corriger certaines ou toutes les erreurs qui peuvent se produire.
En négligeant de nombreux aspects, tels que les facteurs de charge, les frais, les temps d'attente, la sécurité, etc., on pourrait fort bien répéter automatiquement trois ou quatre fois chaque message pour s'assurer qu'une erreur en ligne n'empêche pas le destinataire de recevoir le télégramme correct. Il y aurait là cependant une surabondance inacceptable. Il serait préférable de ne répéter que les caractères erronés.

ARQ – Automatic Repeat Request

L'ARQ est une méthode très répandue qui consiste à utiliser une sorte de mémoire à l'émission ainsi qu'un code de détection des erreurs aménagé de telle façon que toute erreur détectée déclenche automatiquement une demande de retransmission des caractères en question. Les systèmes ARQ sont rapides et sûrs et, en général, supérieurs aux codes de correction des erreurs qui réduisent substantiellement la cadence de transmission et ne sont pas sûrs. Fondamentalement, il existe deux types de systèmes ARQ: *Stop-and-Wait ARQ et Continuous ARQ*. Le Stop-and-Wait ARQ est le plus courant. Il est utilisé sur circuits semi-duplex et est considéré comme efficace avec de faibles cadences de transmission et des délais de mise en œuvre courts, comme ceux qui caractérisent les circuits TTY.
Sans trop entrer dans le détail, une petite initiation aidera le lecteur à mieux comprendre le système réel décrit ci-dessous.
L'alphabet télégraphique international CCITT No 2 est un code à 5 bits. Pour l'ARQ, les caractères peuvent être étendus à un code de détection des erreurs à rapport constant de 4/3 qui permet de vérifier, entre autres, la parité des caractères transmis, à savoir que le bit de parité ajouté est un un («1») ou un zéro («0») si le nombre «1» ou «0» dans le caractère télégraphique à 5 bits est pair ou impair.

Dans le modèle spécifique décrit ci-dessous, des blocs de trois caractères sont envoyés tant que des réponses formelles sont reçues. La réponse consiste en un caractère de 70 millisecondes qui alterne avec chaque cycle ARQ (trois caractères de données envoyés). Si la station émettrice constate que la réponse n'alterne pas, le bloc précédent de 3 caractères est retransmis jusqu'à ce qu'il soit reçu correctement, c'est-à-dire jusqu'à réception de l'accusé de réception correct. Cette retransmission peut avoir lieu 32 fois avant que le système entreprennet un sous-programme spécial.
Il convient de souligner qu'avec l'avénement du microprocesseur les équipements de chiffrement ont non seulement franchi une ère nouvelle mais l'utilisation et l'exploitation des terminaux ARQ sont devenus considérablement plus souples.
Le terminal ARQ adaptif RF-3500 Harris permet à l'opérateur de choisir le nombre de cycles de répétition (standard = 32) avant d'amorcer la séquence de redémarrage.
Les autres particularités de la conception «interactive» du RF-3500 qui permettent à l'opérateur de contrôler entièrement l'équipement ARQ à partir du clavier du terminal de chiffrement *Cryptomatic HC-580* comprennent:
- sélection de mode et fonctions;
- procédures d'exploitation et d'auto-vérification avec isolement des pannes au niveau de la carte et peut-être même du circuit intégré mise en circuit;
- appels sélectifs (sous forme de nombre ou de caractères);
- et même reconfiguration du système.

L'interface interactif permet à l'opérateur de dialoguer avec le système. Il est guidé par une routine interactive utilisant le clavier et l'imprimeur comme interface humain, rendant ainsi l'exploitation plus facile et offrant également une très grande souplesse.
Une commande à distance séparée n'est donc pas nécessaire et il n'y a pas lieu de placer l'équipement terminal dans la même salle que l'équipement radio.
Voici donc un exemple de séquence d'appel ARQ. Supposons qu'un appel doive être lancé en mode ARQ à une station dotée du numéro SELCALL 13524. L'opérateur active le système en enfonçant la touche BREAK (soit sur le panneau de l'équipement ARQ, soit sur son clavier Cryptomatic HC-580). Le système répond par MODE = et l'opérateur non familier avec la procédure d'exploitation peut demander une aide en formant (HELP) (CR).
Tous les modes possibles que l'opérateur peut choisir (onze) sont affichés sur l'imprimeur (Cryptomatic HC-580). Il choisit ARQ:
MODE =(ARQ) (CR)
et forme le numéro
SELCALL = (13524) (CR)
suivi du message.

Précisons que l'opérateur aurait également pu choisir le mode FEC (Forward Error Correction) ou FEC selectif. Contrairement à l'ARQ ces deux modes sont utilisés en simplex, c'est-à-dire qu'il n'y a pas d'accusé de réception du signal transmis. Dans ces modes, les caractères sont transmis deux fois et comparés à la station de réception. S'il ne concordent pas, un espace est laissé, mais, contrairement au mode ARQ, il n'y a pas de répétition.

Mettons à profit non seulement la technologie moderne, mais aussi les meilleurs produits disponibles sur le marché.
L'émetteur (Harris RF-193) comprend un oscillateur entièrement synthétisé (Harris RF-131) et un amplificateur de puissance de 1 kW (Harris RF-110A). L'émetteur et le récepteur à semiconducteurs (Harris RF-505A) couvrent tous deux la bande de 2,0000 à 29,9999 MHz avec une précision de 1×10^{-8}.
L'un des modules contenus dans le rack est le terminal ARQ adaptif (Harris RF-3500B). Il n'y a que trois touches sur le panneau frontal: RESET, BREAK et ALARM RESET.
Une station ARQ n'exige pas la simultanéité de la transmission et de la réception, mais alterne rapidement entre les deux. Les fréquences de réception et de transmission ne diffèrent en général que de 4% ou moins. Un rapide commutateur émission/réception transistorisé permet de passer en moins de 2 millisecondes d'une antenne à l'autre. L'émetteur fournissant 1 kilowatt, moins de 2 microvolts atteignent le récepteur!
Comme le système en question doit être étudié pour des liaisons extrêmement secrètes, tous les terminaux sont des Cryptomatic HC-580 *(CRYPO AG, Suisse)*. Ils servent à la fois de console pour l'opérateur en mode de transmission en clair et de dispositif d'entrée/sortie en mode de transmission chiffrée. Le Cryptomatic HC-580 est une unité de chiffrement on-line compacte et hautement automatisée commandée par microprocesseur. Il satisfait aux normes les plus strictes en matière de chiffrement. Il est conçu pour le chiffrement et le déchiffrement des messages écrits (TTY) ou des messages sur bande de papier. L'unité de chiffrement fait partie d'un téléimprimeur électronique spécial exempt d'interférences. Le HC-580 est donc un terminal de chiffrement entièrement intégré prêt à être relié à n'importe quel type de réseau de transmissions par téléimprimeur.

Antennes

Alors que la station de base est équipée de deux antennes, les installations d'une embassade ou d'un navire ne sont dotées que d'une seule antenne pour l'émission et la réception. Une antenne unique et un commutateur émission/réception rapide (moins d'une milliseconde) éliminent les problèmes causés par l'interférence mutuelle lorsque les antennes d'émission et de réception sont installées l'une près de l'autre.