НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ „ВАСИЛ ЛЕВСКИ”

ФАКУЛТЕТ „АРТИЛЕРИЯ, ПВО И КИС”
9713 гр. Шумен, ул. „Карел Шкорпил” №1
телефон: (054)801 040; тел.факс:(054)877 463;
e-mail: nvu-sh@aadcf.nvu.bg

КАТЕДРА „ПРОТИВОВЪЗДУШНА ОТБРАНА”

асистент инж. Станимир Христов Първанов

ИЗСЛЕДВАНЕ НА ВЪЗМОЖНОСТИТЕ ЗА СЪВМЕСТНО ПРИЛОЖЕНИЕ НА ШУМОУСТОЙЧИВО КОДИРАНЕ И ШИФРИРАНЕ В КОМУНИКАЦИОННИТЕ СИСТЕМИ

АВТОРЕФЕРАТ

На дисертационен труд за присъждане на
Образователна и научна степен „ДОКТОР“
Докторска програма по научна специалност:
„Комуникационни мрежи и системи:
НАУЧНА ОБЛАСТ: 5. ТЕХНИЧЕСКИ НАУЧКИ
ПРОФЕСИОНАЛНО НАПРАВЛЕНИЕ 5.3. КОМУНИКАЦИОННА И КОМПЮТЪРНА ТЕХНИКА

Научен ръководител

доц. д-р инж. Венцислав Митков Василев

Шумен

2026г.

Дисертационния труд е обсъден на заседание на катедрен съвет на катедра „Противовъздушна отбрана“ при Факултета „Артилерия, ПВО и КИС“, към Национален Военен Университет „Васил Левски“ на __.__.2026 г. в зала №__ и е насрочен за официална защита пред научно жури в състав:

_____

_____

_____

Докторантът е асистент в катедра „Радарни и комуникационни системи” при факултет „Артилерия, ПВО и КИС” на Национален военен университет „Васил Левски” – Велико Търново.

Основните изследвания по дисертационния труд са проведени в развойната програмна среда MATLAB.

Автор: асистент инж. Станимир Христов Първанов.

Тема: „Изследване на възможностите за съвместно приложение на шумоустойчиво кодиране и шифриране в комуникациите”.

Тираж __

Отпечатан на ___.___. 20__ г.

Издателски комплекс на Национален военен университет „Васил Левски“

Дисертационният труд съдържа: брой страници – 167, брой фигури – 58, брой таблици – 28, брой приложения: 13, брой литературни източници – 129, брой публикации свързани с дисертацията – 5.

Номерацията на фигурите, таблиците и формулите в автореферата отговаря на тези в дисертацията.

Материали по защитата се намират в катедра „Противовъздушна отбрана“.

1. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД.

Мотиви за разработване на дисертационния труд:

- Налице е нарастваща необходимост от изграждане на сигурни комуникационни системи, способни да защитават чувствителната информация от неоторизиран достъп, злонамерено въздействие и компрометиране. В тази връзка съвременните комуникационни организации все по-активно прилагат модерни криптографски протоколи, осигуряващи поверителен и защитен обмен на данни в интернет среда;

- Действащите стандарти и нормативни изисквания, свързани със съхраняването, обработването и предаването на информация, налагат стриктно спазване на установените правила. Това изисква от комуникационните компании да прилагат надеждни механизми за защита на данните, тъй като нарушенията могат да доведат до значителни санкции от страна на регулаторните органи;

- Събирането, обработването и споделянето на потребителски данни увеличават риска от киберпрестъпления, изтичане на информация и неправомерно използване на лични данни. Това обуславя необходимостта от по-високо ниво на контрол, както и от изграждане на ефективни политики за използване, съхраняване и защита на информацията;

- Наред с криптографската защита, съществено значение придобива и използването на шумоустойчиво кодиране, тъй като предаването на данни в реални комуникационни канали е съпроводено с въздействие на шум, смущения и грешки. Съчетаването на шифриране и шумоустойчиво кодиране позволява едновременно повишаване на сигурността и надеждността на комуникационния процес;

- Съвременните бизнес процеси, държавни институции и облачни инфраструктури генерират значителни обеми от информация, което налага използването на надеждни технологии за архивиране, съхранение и обмен на данни. Това поражда необходимост от комуникационни решения, които осигуряват както защита на съдържанието, така и устойчивост при предаване в неблагоприятна

среда.

Актуалност на проблема на дисертационния труд

Кодирането и криптирането на информацията са важни елементи от процеса на създаването и функционирането на комуникационните мрежи. При това кодирането минимизира грешките при предаване на цифрови данни, осигурявайки зададено ниво на достоверност на приетите битове информация чрез добавяне на проверовъчни и контролни битове. От друга страна, криптирането на информацията осигурява най-ефективната защита срещу зачестилите кибератаки и компрометирането на личните данни. Като цяло обаче прилагането както на кодиране така и на криптиране усложнява процеса на предаване и обработка на информация и намалява скоростта на нейното предаване. Това налага разработването на подходи за съвместно използване на шумоустойчиво кодиране и шифриране, осигуряващи едновременно висока криптографска устойчивост, шумозащитеност и необходимата скорост на предаване на информацията чрез максимално рационално използване на възможностите на хардуерните и софтуерните компоненти на комуникационните системи.

Цел на дисертационния труд

Настоящият дисертационен труд има за цел да се разработят алгоритми за шумоустойчиво кодиране, осигуряващи едновременно максимално отношение сигнал/шум и висока криптографска защита на предаваните данни чрез изпълнение по единен замисъл на различни етапи в процеса на обработка на информацията в комуникационните системи.

Предмет на дисертационния труд

Предмет на дисертационния труд са методите и алгоритмите за шумоустойчиво кодиране и шифриране в комуникациите на фона на действието на пасивни и активни смущения, изчислителните процедури за определяне на оптималните стойности на образуващия полином на кодера, скоростта на кода, вида на декодиране, влиянието на различни типове криптиране на информацията върху скоростта на предаване на данните в комуникационния канал.

Научна новост

Теорията на турбо кодирането е доразвита като са обосновани подходи за синтез на турбо кодери, осигуряващи едновременно

различни кодови скорости и криптиране на предаваната информация. В алгоритъма за кодиране се обосновава добавянето на разместващо устройство непосредствено след източника на съобщение, което осигурява висока криптографска защита на предаваните данни и се постига необходимото съотношение сигнал/шум при предаването на информационните сигнали на фона на смущения.

Практическа полезност.

Разработен е модел за съчетаване на шумоустойчиво кодиране и шифриране в комуникационния канал, осигуряващ необходимото съотношение сигнал/шум и висока защитеност срещу неоторизиран достъп.

Съдържание на дисертационния труд

ГЛАВА ПЪРВА: Анализ на принципите на построение на комуникационните системи, използвани в българската армия, полицията и системата за пожарна безопасност и защита на населението.

ГЛАВА ВТОРА: Основни технологии за кодиране на комуникационния канал. Хибридно използване на симетрични и асиметрични алгоритми за криптиране на предаваните данни по незащитен канал.

ГЛАВА ТРЕТА: Синтез на модел за обработка на информацията в комуникационна система, осигуряващ съвместно шумоустойчиво кодиране и шифриране на информацията.

ГЛАВА ЧЕТВЪРТА: Резултати от проведените изследвания на модела за обработка на информацията в комуникационна система, осигуряващ съвместно шумоустойчиво кодиране и шифриране на информацията.

2. КРАТКО СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯТ ТРУД.

ГЛАВА 1. АНАЛИЗ НА ПРИНЦИПИТЕ НА ПОСТРОЕНИЕ НА КОМУНИКАЦИОННИТЕ СИСТЕМИ, ИЗПОЛЗВАНИ В БЪЛГАРСКАТА АРМИЯ, ПОЛИЦИЯТА И СИСТЕМАТА ЗА ПОЖАРНА БЕЗОПАСНОСТ И ЗАЩИТА НА НАСЕЛЕНИЕТО

Сигурните и надеждни комуникации са в основата на ефективното функциониране на съвременните комуникационни системи, намиращи приложение в различни области на обществения живот: отбрана, вътрешна сигурност, гражданска защита, полиция и др. В ерата на

активни хибридни заплахи, кибератаки и електромагнитни въздействия, защитата на физическия слой на излъчването на полезен сигнал става приоритет. В реална бойна обстановка или аварийни условия сигналът в една комуникационна система е слаб и зашумен, което води до грешни решения. Това налага постоянно изследване на технологиите за корекция на грешки и оптимизация на предаването на данни, а крайната цел е надеждна, защитена и високоскоростна връзка.

1.1. Значимост на шумоустойчивостта за съвременните комуникационни системи, използвани в Българската армия, полицията и системата за пожарна безопасност и защита на населението.

Шумоустойчивостта на дадена комуникационна система представлява нейната способност да поддържа ниско ниво на битови грешки (Bit Error Rate - BER), дори при наличие на шум. На практика най-често срещаните модели на шум са AWGN (Additive White Gausion Noise - AWGN) и Rayleigh fading, характерни за военните и полицейски комуникации [3].

В комуникационните системи на МО и МВР се използват устойчиви радиочестотни връзки, работещи в нелицензирани и лицензирани честотни спектри и различни нива на защита. Системите от рода на TETRA, DMR, и LTE/5G имат нужда от надеждно кодиране на канално ниво, с което да преодолеят активно заглушаване, атаки с широколентов шум и смущения от неприятелски източници [2].

Важен елемент в много от кодиращите схеми за турбо-кодове е интерлийвърът, който разбърква реда на битовете преди предаване, така че последователни грешки от канала да се разпределят на отдалечени позиции при декодирането. Правилно проектираният интерлийвър предотвратява създаването на кратки цикли в декодиращите алгоритми и намалява вероятността от т.нар. „error floor“ (застой на грешките при високо съотношение сигнал/шум signal to noise ratio - SNR) [26].

1.2. Анализ на известните технологии за съвместно използване на шумоустойчиво кодиране и шифриране.

За военните и специализираните комуникационни системи е еднакво важно както съобщението да бъде получено без грешки, така и да остане поверително и защитено. Сигурността (чрез криптиране) и надеждността (чрез канално кодиране) се третират като отделни слоеве.

Комуникациите във военната област се осъществяват в условия на високи нива на шум, смущения и преднамерено заглушаване (джаминг). Това налага използването на технологии, които правят комуникациите изключително устойчиви. При аналоговите системи се използва метод на скокообразно изменение на носещите честоти (frequency hopping) и разширяване на честотния спектър (spread spectrum) [46].

При цифровите технологии, аналоговите схеми се комбинират със силни канални кодове и криптиране за цялостна защита. При тактическо ниво на комуникациите в НАТО се използват комбинирани кодове (код на Рийд-Соломон или конволюционно кодиране), които извършват корекция на пакетни или битови грешки в сателитните комуникации на големи разстояния. С въвеждането на стандарта STANAG за военни комуникации, турбо-кодовете също намират място, като предлагат висока надеждност при ниско отношение сигнал/шум [46].

Най-разпространения асиметричен метод за шифриране RSA, позволяващ сигурно предаване на информацията дори между страни, които никога не са обменяли конфиденциална информация. Той се използва в електронната търговия, в сигурното банкиране, в правителствени системи и в почти всички протоколи, които изграждат интернет сигурността [99]. В инфраструктурата за публични ключове, която поддържа интернет сертификатите, RSA все още е най-разпространеният алгоритъм за цифрови подписи [105]. Големите институции, банки и правителства разчитат на RSA за критични операции, тъй като неговото поведение е изключително добре проучено. Протоколите за комуникация дълго време използват RSA за обмен на ключове. Макар новите версии на TLS да преминават към методи с елиптични криви, RSA остава важен елемент за обратна съвместимост и за системи, в които производителността не е първостепенен фактор. В комбинация със симетрични алгоритми като AES, RSA остава надежден механизъм за установяване на защитени сесии.

Квантовите изчисления поставят под въпрос бъдещето на RSA. Алгоритъмът на Шор показва, че факторизация може да бъде извършена ефективно върху квантов компютър [106]. Тази заплаха все още е хипотетична – към момента няма квантов компютър, способен да разбие практически използваните размери на ключовете. В обозримо бъдеще RSA продължава да бъде напълно оправдан избор за защита на данните.

1.3. Изводи от първа глава. Задачи на дисертационния труд.

1. В съвременни условия шумозащитеността и криптографската устойчивост са параметри с критична значимост за комуникационните системи, използвани във въоръжените сили, полицията, пожарната безопасност и защитата на населението от бедствия и аварии. Това налага усъвършенстване на утвърдените канални кодове (турбо, конволюционни, LDPC, и т.н. кодове), както и въвеждането на иновативни решения като интерлийвъри, работещи с различни методи на разбъркване, комуникационни системи, съчетаващи съвместно криптиране и кодиране.

2. Днес прогресът в областта на шумоустойчивото кодиране и криптирането в значителна степен се характеризира с разработването и практическото внедряване на алгоритми, запазващи целостта на информацията дори при ниски отношения сигнал-шум, интензивни смущения или злонамерено подавяне на комуникационните сигнали.

3. Анализът на резултатите от теоретичните и опитно-конструкторските разработки в сферата на кодирането и шифрирането, известни от информационните източници с открит достъп, разкрива необходимостта от системен подход при усъвършенстването на турбо кодовете, тъй като от една страна те практически много плътно се приближават до така наречената *граница на Шенон* (тяхната енергийна ефективност отстъпва на теоретически граничното значение само с 0,5 dB), а от друга страна позволяват в тяхната структура технически просто да бъдат вградени различни технологии за шифриране.

Предвид на горните изводи, целта на дисертационния труд е:

Да се разработят алгоритми за шумоустойчиво кодиране, осигуряващи едновременно максимално отношение сигнал/шум и висока криптографска защита на предаваните данни чрез изпълнение по единен замисъл на различни етапи в процеса на обработка на информацията в комуникационните системи.

За постигане на тази цел е необходимо да бъдат решени следните основни задачи:

1. Анализиране на известните подходи за съвместно използване на шумоустойчиво кодиране и шифриране.

2. Систематизиране на основните етапи на обработка на данните при шумоустойчиво кодиране, както и при симетричните и асиметрични

алгоритми за криптиране на съобщенията, предавани по незащитен канал.

3. Синтезиране на модел за обработка на информацията в комуникационна система, осигуряващ съвместно шумоустойчиво кодиране и шифриране на информацията.

4. Изследване с помощта на имитационно компютърно моделиране на практическата приложимост на модела за обработка на информацията в комуникационна система, осигуряващ съвместно шумоустойчиво кодиране и шифриране на информацията.

ГЛАВА 2. ОСНОВНИ ТЕХНОЛОГИИ ЗА КОДИРАНЕ НА КОМУНИКАЦИОННИЯ КАНАЛ. ХИБРИДНО ИЗПОЛЗВАНЕ НА СИМЕТРИЧНИ И АСИМЕТРИЧНИ АЛГОРИТМИ ЗА КРИПТИРАНЕ НА ПРЕДАВАНИТЕ ДАННИ ПО НЕЗАЩИТЕН КАНАЛ.

Шумоустойчивото кодиране и шифрирането решават различни задачи в комуникационните системи. По тази причина положителен ефект в резултат на реализацията им по единен замисъл може да се постигане само чрез съвместяване на отделни техни етапи. Това обаче налага по-детайлен анализ на техническите процедури при шумоустойчивото кодиране и шифрирането, както и разкриване на приликите и аналогиите в тях. Предвид на този факт в настоящата глава се решава втората задача на дисертационния труд.

2.1. Обща характеристика на конволюционните и турбо кодове.

Каналното шумоустойчиво кодиране е фундаментален процес в цифровите комуникации, чиято основна цел е да защити предаваната информация от грешки, възникващи по време на преноса през неидеален комуникационен канал. Това се постига чрез умишлено добавяне на излишни битове в изходния поток от информация.

Известни са редица способи за кодиране:

- блокови кодове, при които информацията се обработва на блокове с фиксирана дължина; такива са кодовете на: Хеминг, Reed-Solomon и BCH кодовете;

- систематични кодове, където данните за обработка са информационни потоци, като изходният резултат зависи от текущите и предишните входни битове; систематични кодове са: LDPC (код за

проверка на четността при ниска плътност) и Turbo кодове, които се базират на конволюционните кодове.

Линейните блокови кодове се дефинират от фиксирана генераторна матрица G и проверовъчна матрица H[109].

Математическото представяне на линеен блоков кодер е от вида:

$$c = u.\boldsymbol{G} \tag{2.1}$$

където:

с е изходната кодова дума;

- u са входните информационни битове;
- G – генераторна матрица.

Чрез проверовъчната матрица H се изчислява синдрома на грешката:

$$S = r.\boldsymbol{H}^{\mathbf{T}} \tag{2.2}$$

където:

- S е синдром на грешката;
- r е приетата кодова дума;
- H^{T} е транспонираната проверовъчна матрица.

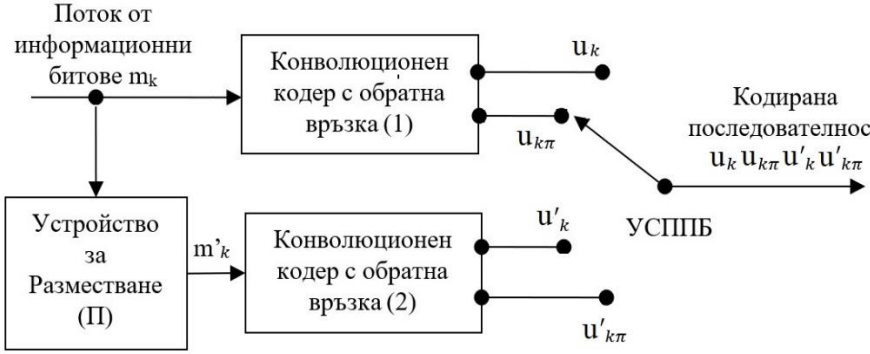
Ако синдромът е S=0, приемникът „взема решение“, че не са настъпили грешки. Ако S≠0, приемникът „взема решение“, че допусната грешка.

Генераторната и проверовъчната матрици винаги са съвместими, т.е. всяка кодова дума изпълнява условието:

$$\boldsymbol{G}.\boldsymbol{H}^{\mathbf{T}} = 0 \tag{2.3}$$

Основното различие между линейните блокови кодове и конволюционните кодове се заключава в принципа на кодиране. Архитектурата на конволюционните кодери включва регистри за преместване, запаметяващи състоянието на системата и генераторни полиноми, описващи връзките между входовете и изходите.

Турбо кодерът е на по-високо ниво в областта на кодирането. Той представлява паралелно съединение на два рекурсивни систематични конволюционни кодера, разделени от разбъркващо устройство, наричано интерлийвър [5, 6, 25, 36].



Фиг. 2.3. Блокова схема на турбо кодер

На фиг. 2.3 е представена блокова схема на турбо кодер. Входната последователност от данни $m_k = [m_1, m_2, \dots, m_n]$ постъпва на рекурсивен конволюционен кодер 1, където информацията се сумира по сума по модул две. На неговия изход се получава кодиран поток от данни u_k, който постъпва на мултиплексор и устройство за селективно пропускане на паритетните изходни потоци.

Входната последователност от данни m_k постъпва и в устройството за разместване, където най-напред се записват предварително зададен брой битове, които след това се разместват по псевдослучаен закон и постъпват на входа на втория RSC кодер, чието устройство и работа са както при първия кодер. Двата кодера работят със скорост 1/2, което означава, че за всеки непроменен информационен бит от входната последователност, кодерът формира два бита на своя изход. Стойността на систематическия изход (u_k) на първият RSC кодер в *i*-тия такт на работа съвпада със значението на входния бит (m_k), а на втория изход се формира проверовъчен бит ($u_{k\pi}$).

Систематическият изход на втория RSC кодер не се използва, а на другият му изход се формира втори проверовъчен бит $u'_{k\pi}$. На изхода на турбо-кодера първо се появява битът u_k от систематическия изход на първия кодер, а след това - двата проверовъчни бита $u_{k\pi}$ и $u'_{k\pi}$ от първия и втория RSC кодер. Кодовата скорост R на целия турбо-кодер е 1/3, като за един входен бит се получават три изходни, образувани от изходите u_k, $u_{k\pi}$, $u'_k\pi$.

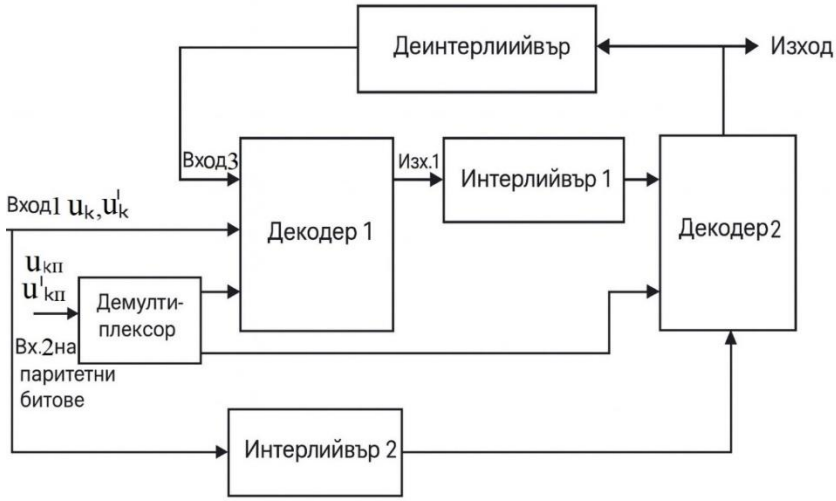
Възможно е формирането на съкратен перфориран (puncturing) код, в който битовете от проверовъчните изходи на кодерите се мултиплексират от устройство за селективно пропускане на паритетните изходни потоци. Тук непроменената последователност от информационни битове се редува от такт към такт, като се взема последователно проверовъчен бит от първия или от втория RSC кодер. Това намалява коригиращата способност на кода, но скоростта нараства до 1/2. Чрез използването на систематически конволюционни кодери в кодовия блок се отделят информационните от проверовъчните битове. Счита се, че в канала за свръзка реално се предава информацията от два кодови блока, като първият блок включва информационната и проверовъчната части на първия RSC кодер, а вторият кодов блок съдържа разместената информационна и проверовъчна части на втория RSC кодер.

На изхода на турбо кодера се формира поток от данни, които постъпват на турбо декодер и се извършва проверка за грешки.

Турбо декодерът извлича систематичните и паритетни битове от получената поредица от данни. Блоковата схема на турбо декодера е представена на фиг. 2.4. Двоичната кодирана входна последователност за турбо декодера се представя във вида:

$$R_k = [\, u_k, u_{k\pi}, u'_k, u'_{k\pi} \,], \tag{2.8}$$

където: - u_k и u'_k са систематичната част от двоичната входна последователност, а $u_{k\pi}$ и $u'_{k\pi}$ са паритетната част.



Фиг. 2.4. Блокова схема на турбо декодер

На входове на първи декодер постъпва систематичната стойност на получената последователност u_k, u'_k и паритетния поток от битове $u_{k\pi}$ и $u'_{k\pi}$.

След обработка на входните данни на изхода на първия декодер се получава мека оценка, като този информационен поток постъпва към разместващо устройство 1, а след това към втори декодер.

На първия вход на втория декодер постъпват от първи декодер преподредена поредица на систематичния поток от данни u_k и u'_k. На втория вход постъпват паритетни битове $m_{k\pi}$ и $m'_{k\pi}$, а на третия директно от входа на турбо декодера постъпва преподредена систематична информация от интерлийвър 2.

Във втори декодер се осъществява обработка на получените данни и се получава втора мека оценка, която се подава на деинтерлийвъра, а след него тази мека оценка постъпва на третия вход на първи декодер. Процесът се повтаря итеративно, докато се постигне нулева вероятност за грешка. На финалния етап се прилага прагова обработка на информационния поток от мекия изход на втори декодер за вземане на твърдо решение за максимална апостериорна правдоподобност.

2.2. Обща характеристика на алгоритмите за криптиране.

Криптирането на дадено съобщение е процес на прикриване по някакъв начин на неговото съдържание, след което се получава

шифриран текст. Процесът на дешифриране на шифрирания текст се нарича декриптиране. Това налага използване на криптиращ и декриптиращ алгоритъм.

Процесите на криптиране и декриптиране се описват със следните изрази:

$$E_K(\mathrm{M}) = \mathrm{C} \tag{2.20}$$

$$\mathrm{D_K}(\mathrm{C}) = \mathrm{M}, \tag{2.21}$$

където:

M е явното съобщение (откритият текст);

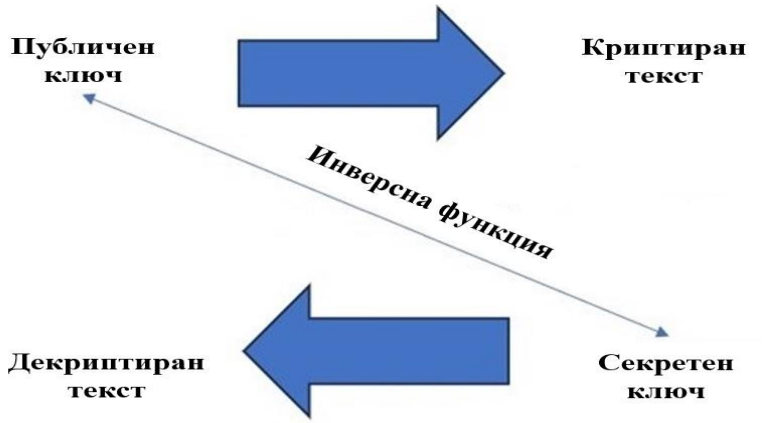
- C е криптираното съобщение;
- E_K е функция криптиране;
- $\mathrm{D_K}$ е функция декриптиране;
- K е секретен ключ.

Известни са симетрични и асиметрични алгоритми за криптиране и декриптиране на информацията. При симетричните алгоритми ключът за криптиране и декриптиране е един и същ. Секретният ключ изисква получателя и подателя предварително да разполагат със съответните ключове и да се грижат за опазването им.

Симетричните алгоритми биват поточни и блокови. Поточните обработват явния текст бит по бит, а блоковите – по групи битове.

При асиметрично RSA криптиране за подателя и получателя ключът е различен и се използват публичен и частен ключ. Подателят използва публичен ключ, за да локализира получателя и да насочи съобщението към него. За да дешифрира съобщението, получателят използва ключ, който е математически свързан с частния. В този алгоритъм публичният ключ служи като „адрес“, докато частният ключ (известен само от получателя) служи като ключ към декриптиране. Това гарантира, че всеки може да изпраща съобщения през незащитена мрежа и само истинският получател може да ги прочете [116, 117].

На фиг. 2.12 схематично е представена работата на RSA алгоритъма.



Фиг. 2.12. Асиметричен RSA алгоритъм за криптиране

Асиметричното криптиране на текст се извършва в съответствие със следния израз [117]:

$$C \equiv \mathrm{M}^{E_k}(modN), \tag{2.30}$$

където: M е съобщението, E_K е криптиращата функция, N е публичния ключ, а C е шифрирания текст.

Декриптирането се осъществява на базата следния израз [117]:

$$M_d \equiv \mathrm{C}^{\mathrm{d}}(\mathrm{m}odN), \tag{2.31}$$

където: C е шифриран текст, d е секретен ключ, N е публичния ключ, а M_d е декриптираното съобщение.

Обобщения израз описващ алгоритъм за криптиране RSA се получава от изрази (2.30), (2.31):

$$M_d \equiv (\mathrm{M}^{\mathrm{e}})^{\mathrm{d}}(modN), \tag{2.32}$$

Където публичният ключ е съставен от стойностите на: “e” и “N”, като числото “d” трябва да се пази в тайна.

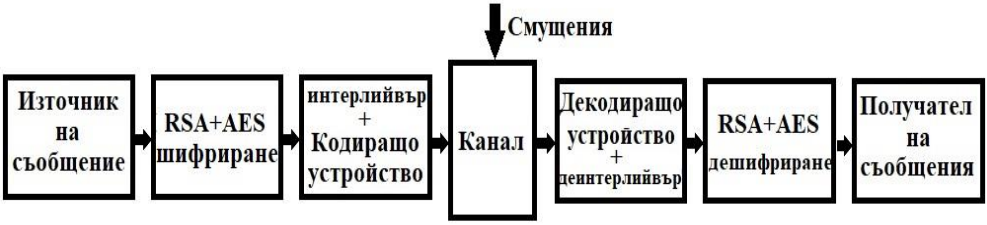
2.3. Криптокодиращи системи с добавени разбъркващи устройства за повишаване на криптоустойчивостта и шумозащитенонстта на канала.

При предаване на защитена информация по незащитен канал не е достатъчно съобщението само да бъде шифрирано. Извършеният литературният анализ в първа глава показва, че възникналите грешки при предаване могат да нарушат шифротекста до степен, при която дешифрирането става силно неточно или практически невъзможно. Именно поради това преди предаването се използва шумоустойчиво

кодиране, което повишава вероятността приемникът да възстанови правилно получената последователност от битове дори при наличие на шум. Според Абаси-Мохадам, Д., Вакили, В. и Фалахати, А., съвременните алгоритми за симетрично шифриране като AES са изключително чувствителни към грешки, като дори една единствена такава, след дешифриране, води до лавинообразно разпространение на грешки [127]. Ето защо, за да се осигури както поверителност, така и достоверност, е необходимо криптирането да се комбинира с мощно коригиращо кодиране. Турбокодовете са особено подходящи за тази цел, тъй като осигуряват корекция на грешки, близка до теоретичната граница на Шанън [126]. За да се увеличи криптоустойчивостта, също така е необходимо съчетаването на асиметрично криптиране, за предаване на сесийните ключове на основния симетричен шифриращ алгоритъм.

2.3.2. Предложена концепция: разбъркващи устройства преди турбо кодера.

Сесийните ключове на симетрияния AES алгоритъм се предават чрез асиметричен RSA алгоритъм. Това реализира комбинирана криптосистема, съчетаваща бързина за шифриране на данните по алгоритъм AES и сигурност на асиметричната криптография за предаване на секретните ключове [125]. AES-256 е устойчив на квантови атаки (алгоритъмът на Гроувър дава само квадратично ускорение), докато асиметричните схеми са уязвими на алгоритъма на Шор [126, 127, 128]. В предложената система асиметричният обмен се използва само за краткотрайни сесийни ключове, което минимизира риска от компрометиране. (работата на RSA алгоритъма е описана в гл. 2. т.2.2). На фиг.2.13 е представена блокова схема на предложената концепция.



Фиг. 2.13. Блок-схема на предложената концепция

В разработената в дисертацията концепция към вече получения шифротекст се добавят едно или две разбъркващи устройства (интерлийвъра) преди турбо кодера. По този начин шифротекстът не само е защитен от основния криптографски алгоритъм, но след това неговите позиции се разбъркват. Ако се означим откритото съобщение с M, шифрираният по RSA алгоритъм симетричния ключ с K_s, а разбъркващите устройства с π_1 и π_2, тогава процесът на криптиране и разбъркване u_s се получава от следния израз:

$$u_s = \pi_2(\pi_1.K_s) = (\pi_2(\pi_1(E_{k_{K_s}}.(M))) \qquad (2.33)$$

След това именно u_s се подава към турбо кодера, а след добавянето на проверовъчни битове от турбо кодера се получава кодираната последователност u_k. На приемната страна първо се извършва турбо декодиране D_{k_s}, след това обратно пренареждане на битовете и чак накрая дешифриране D_k, чрез израза:

$$\mathrm{M} = D_{k_s}(\pi_1{}^{-1}.(\pi_2{}^{-1}(D_{k_{K_s}}.(u_s))) \qquad (2.34)$$

По този начин се получава двуслойна защита: първо битовете са криптографски шифрирани, а след това техните позиции са допълнително скрити чрез едно или две разбъркващи устройства.

Разбъркването на битовете преди турбо кодера са неизвестни за подслушващата страна. В такъв случай недоброжелателите трябва да познаят не само ключа за AES алгоритъма, но и правилното разбъркване, което увеличава трудността, тък като ключовото пространство нараства от умножението на ключовото пространство от двата шифротекста.

Класическият вариант защитава съдържанието [129], а предложената концепция защитава едновременно и съдържанието, и подредбата на вече шифрираните данни. Това позволява да се разглежда разбъркващото устройство като допълнителен шифриращ слой върху вече формирания шифротекст.

Освен, че повишава криптографската неопределеност, това предварително разместване на битове подпомага и турбо декодера, защото локалните пакетни грешки в канала се разпределят равномерно, вместо да се наблюдават концентрирани грешки върху малък брой съседни позиции. Това намалява вероятността единична допусната

грешка да предизвика лавинообразно разпространение на грешки в процеса на дешифриране.

2.3.3. Устойчивост на двойното криптиране и разбъркване срещу атаки от типа „груба сила“.

За да се оцени по-ясно допълнителният ефект върху трудността на атаки от типа „грубата сила“, се извърши оценка за нарастването на ключовото пространството за търсене. Ако класическата хибридна схема използва асиметричен алгоритъм W_{asym} за защита на сеансовия ключ и AES-256 за шифриране на полезните данни, тогава общата изчислителна сложност $W_{classic}$ може да се запише с израза:

$$W_{classic} = W_{asym} \,.\, 2^{256}, \tag{2.35}$$

където W_{asym} е сложността за пробив на асиметричния алгоритъм, а 2^{256} е пространството на ключа при AES-256.

Ако след AES-256 се приложи едно разбъркващо устройство върху блок от 256 позиции, тогава броят на възможните разместванията W_{π} е:

$$W_{\pi} = 256!,$$

следователно общата изчислителна сложност W_1 е:

$$W_1 = W_{asym} \,.\, 2^{256} . 256!,$$

от което следва:

$$256! = 2^{1684} = 10^{507}$$

Това означава, че спрямо класическия вариант комбинаторната трудност G_1 за пълно изчерпване на вариантите за разбъркване се изчислява от израза:

$$G_1 = \frac{W_1}{W_{classic}} = 256! = 10^{507} \tag{2.36}$$

От израза става ясно, че с добавянето на едно разбъркващо устройство с дължина 256 позиции, увеличава пространството за търсене с около 10^{507} пъти.

Ако вместо това се използват две успоредно свързани разбъркващи устройства по 128 позиции, тогава броят на възможните разместванията е:

$$W_{\pi} = 128!$$

$$W_2 = W_{asym} \,.\, 2^{128} . (128!)^2,$$

замествайки се получава:

$$128! = 2^{1432} = 10^{431}.$$

Тогава подобрението спрямо класическия вариант е:

$$G_2 = \frac{W_2}{W_{classic}} = 128! = 10^{431},$$

Този резултат е полезен при избора на архитектурата на системата. Ако основната цел е максимално голямо пространство на възможните разместванията, едно 256-битово разбъркващо устройство е по-изгодно. Ако обаче целта е по-гъвкава реализация, по-кратко време за разместване и по-удобно структуриране на потока, две 128-битови разбъркващи устройства също осигуряват изключително голямо увеличение на комбинаторната сложност. Все пак независимо дали ще бъде използвана конфигурация с едно или две разбъркващи устройства, предложената концепция значително увеличава размера на ключовото пространство в сравнение с метода на Ковтун и Иванов, който се осъществява в шифриране и криптиране в една стъпка и достига размер от 10^6 [126.]

Допълнителен аргумент в полза на предложената концепция е, че в разгледаните публикации системите, основани на турбо-базирано шифриране и кодиране, показват подобрение не само по отношение на сигурността, но и по отношение на BER. В [127] е посочено, че при BER=10^{-3} използването на AES-256 базиран генератор води до подобрение приблизително от 4 до 4.5 dB спрямо някои сравнявани подходи. Това потвърждава, че комбинираният подход е практически обоснован и не се свежда само до теоретично увеличаване на ключовото пространство.

2.4. Изводи от втора глава.

1. Към момента са разработени и практически внедрени голямо множество криптографски алгоритми. Независимо от многообразието на криптографските алгоритми, всички те се реализират чрез дълги поредици от прости *заместванията* и *разместванията* на символите от явния текст.

2. От гледна точка на задачите на настоящото изследване е целсъобразно да се използва класификацията на криптографските алгоритми като алгоритми с едно и също количеството информация в явния текст и шифротекста и алгоритми, в които количеството информация в шифротекста е по-голямо от количеството информация в

явния текст. Алгоритмите от първия клас използват принципа „*no data expansion*“, в резултат на което те осигуряват секретност (конфиденциалност) без да се увеличава скоростта на предаване на информацията по комуникационния канал. Пример на алгоритъм от този клас, намиращ днес много широко приложение, е AES.

3. Турбо кодовете се характеризират със следните положителни свойства.

Първо, те практически достигат така наречената *граница на Шенон*, тъй като тяхната енергийна ефективност отстъпва на теоретически граничното значение само с 0,5 dB.

Второ, използват:

- дълги поредици от разместванията на символите, които едновременно могат да се приложат както за отстраняване на вредните последици от пакетните грешки, така и за криптиране на съобщенията;

- итеративно декодиране, което технически е относително просто и е реализирано практически още през 60-те години на миналия век в космическите програми на NASA.

4. Добавянето на едно или две разбъркващи устройства преди турбо кодера увеличава съществено изчислителната сложност на атака по способа „груба сила“, тъй като към пробива на асиметричния алгоритъм за предаване на секретния ключ и самия ключ за симетричнно шифриране се добавя и необходимостта от правилно подреждане на разбъркания шифротекст. В същото време разбъркването подобрява условията за турбо декодиране, защото разпределя грешките по-равномерно и намаля вероятността те да предизвикат лавинообразно натрупване на грешки в процеса на дешифриране.

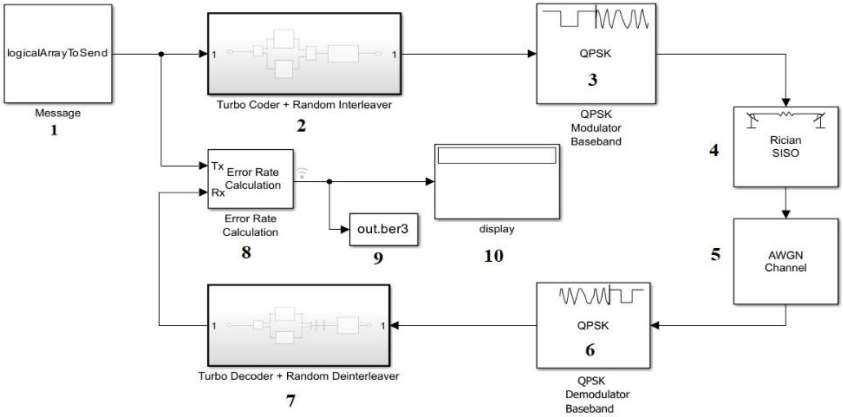
ГЛАВА 3. СИНТЕЗ НА МОДЕЛ ЗА ОБРАБОТКА НА ИНФОРМАЦИЯТА В КОМУНИКАЦИОННА СИСТЕМА, ОСИГУРЯВАЩ СЪВМЕСТНО ШУМОУСТОЙЧИВО КОДИРАНЕ И ШИФРИРАНЕ НА ИНФОРМАЦИЯТА

В предходната глава са анализирани техническите процедури при шумоустойчивото кодиране и шифрирането и са систематизирани приликите и аналогиите в тях. На тази основа в настоящата глава се решава третата задача на дисертационния труд.

3.2. Симулационен модел на комуникационен канал с добавяне на разбъркващи устройства преди турбо кодера и

подреждащи устройства след турбо декодера.

В дисертационния труд се предлага модел на комуникационен канал, който включва добавяне на допълнителни интерлийвъри преди стандартния турбо кодер и деинтерлийвъри след турбо декодера. Целта на предложената модификация на канала за комуникация по отношение на кодирането е подобряване разпределението на грешките, т.е. да бъдат разпръснати възникнали групирани грешки от битове в независими единични грешки и потенциално да се повишат на корекционните способности на кода. От гледна точка на криптографията предварителното разбъркване на шифрираната чрез RSA алгоритъм информация следва да внесе допълнително объркване при разшифрирането от недоброжелатели, които са придобили и компрометирали секретния ключ. На фиг. 3.2 е представена обобщена блок-схема на предложения комуникационен модел с добавени разбъркващи устройства преди турбо кодера и подреждащи устройства след турбо декодера.



Фиг. 3.2. Блок-схема на предложен комуникационен модел

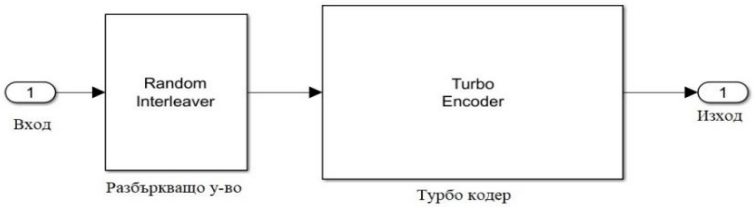
3.2.1. Състав на предложения комуникационен модел.

1 – блок за въвеждане на входното съобщение, 2 – разбъркващи устройства и турбо кодер, 3 – модулатор (BPSK, QPSK или 16-QAM), 4 – канал на Райс, 5 – канал за добавяне на бял Гаусов шум, 6 – демодулатор (BPSK, QPSK или 16-QAM), 7 – подреждащи устройства и турбо декодер, 8 – калкулатор на грешки, 9 – блок свързващ продукта

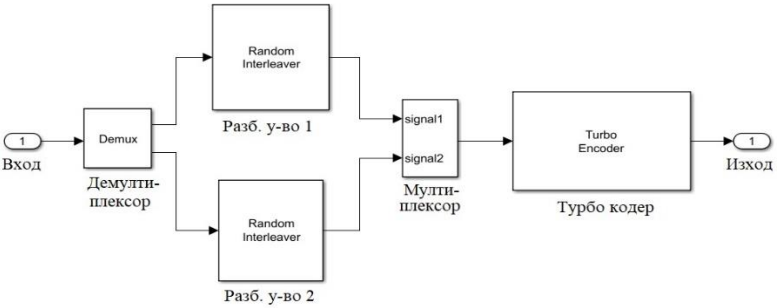
Матлаб със симулационната среда (To Workspace), 10 – дисплей за изобразяване броя на грешките.

3.2.2. Принцип на действие.

Предаваното съобщение представлява последователност от думи и цифри и се въвежда в софтуерна среда „Матлаб“. Следва шифриране чрез RSA алгоритъм и полученият шифротекст във вид на нули и единици постъпва във входния блок (фиг. 3.2). Потокът от информация постъпва за разбъркване, което се осъществява с едно или две успоредно свързани разместващи устройства. Двата варианта за добавяне на разбъркващи устройства преди турбо кодера са изобразени на фиг. 3.3 и фиг. 3.4 съответно.



Фиг.3.3. Блокова схема с едно разбъркващо устройство преди турбо кодера

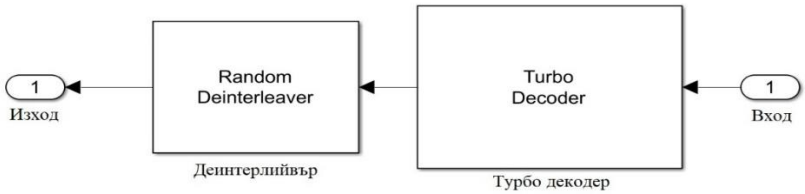


Фиг. 3.4. Блокова схема с две разбъркващи устройство преди турбо кодера

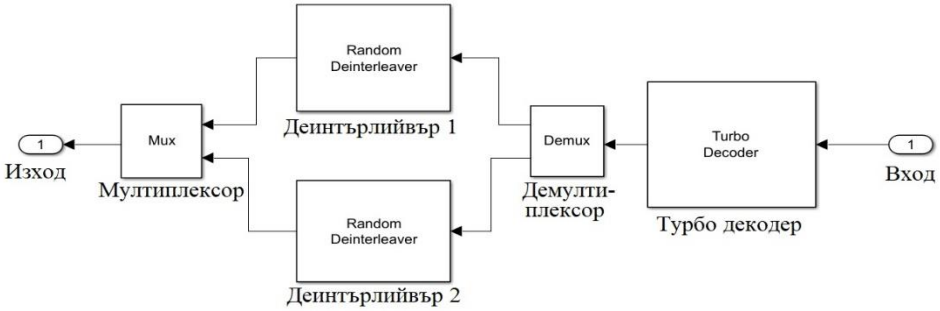
Информацията се разбърква в съответствие с алгоритъма Mersenne Twister (MT19937) и постъпва на турбо кодер (фиг. 3.2). Тук информацията се кодира и се добавят излишък от битове за проверка за грешки. Получава се шифрирано и кодирано съобщение, което постъпва в модулиращо устройство (според избрания вариант на модулация), осъществяващо модулация и предаване на съобщението.

За да се осъществи симулация, максимално близка до реалните условия, модулираният сигнал преминава през канал на Райс и канал за добавяне на бял Гаусов шум. Полученият сигнал с добавения шум постъпва на демодулиращо устройство и на турбо декодера. Следва проверка и поправка на грешки, възникнали при предаването, като се премахва излишъкът от проверовъчни битове. Декодираната последователност от нули и единици постъпва в подреждащи устройства и турбо декодер (деинтерлийвъри), които пренареждат разбъркания шифриран съобщение.

Вариантите за броя на подреждащите устройства след турбо декодера са изобразени на фиг. 3.5 и фиг. 3.6.



Фиг. 3.5. Блокова схема с едно пренареждащо устройство след турбо декодера



Фиг. 3.6. Блокова схема с две пренареждащи устройства след турбо декодера

Полученият шифриран текст се подлага на процедура за калкулиране на грешки, като резултатът се изобразява на дисплей. Шифрираният текст постъпва и за дешифриране в „Матлаб“.

Комуникационният канал с добавяне на разбъркващи устройства преди турбо кодера и подреждащи устройства след турбо декодера може да се приложи при скрито предаване на секретни ключове на AES

алгоритъм чрез RSA асиметрично криптиране. При управлението на дронове комуникацията между оператора и дрона се криптира чрез AES алгоритъм. Предложената структура на комуникационния канал с добавяне на разбъркващи устройства преди турбо кодера и подреждащи устройства след турбо декодера може да се реализира в следните стъпки:

Първата стъпка е стартиране на сесията за комуникация с дрона, която включва следните процедури:

- наземната станция генерира случаен AES session key;
- криптиране на генерирания AES ключ с RSA алгоритъм и добавяне към него на публичен ключ, които се изпращат към дрона.

Дронът използва своя, предварително записан RSA секретен ключ, за да декриптира AES ключа.

Втората стъпка включва симетрично шифроване на потока от данни, съдържащи командите за управление на дрона. Това изисква:

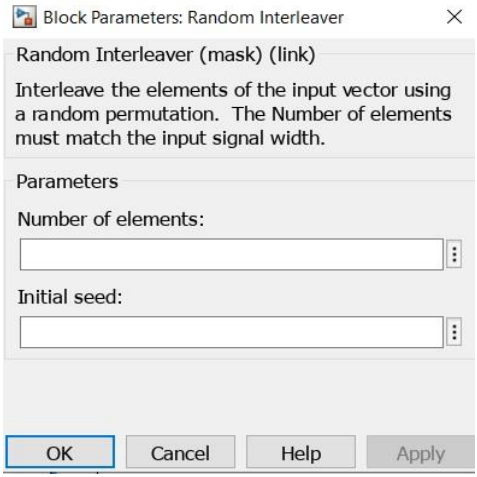
- и двете страни да имат един и същи криптиран AES ключ;
- криптиране на данните със симетричен AES алгоритъм.

3.3. Елементи от състава на предложения модел на комуникационен канал с добавяне на разбъркващи устройства преди турбо кодера и подреждащи устройства след турбо декодера.

3.3.2. Работа и параметри на разбъркващо устройство, преди турбо кодера.

Блокът Random Interleaver (разместващо устройство) е елемент от състава на комуникационните компоненти (Communications Toolbox), включени в симулационна среда „Симулинк“ на софтуерен продукт „Матлаб“. Входният сигнал е във вид на вектор-стълб и разместващото устройство го пренарежда, използвайки случайна пермутация. На фиг. 3.6 е представен контролния панел, от който се задават параметрите на разбъркващо устройство.

Параметърът „Number of elements“ (брой на елементите) показва размера на входния вектор. Следващият параметър „Initial seed“ (начално състояние) инициализира генератора на случайни числа, който извършва пермутацията.



Фиг. 3.6. Контролен панел за задаване на параметрите на разбъркващо устройство

Генераторът на случайни числа е реализиран на базата на детерминистичен алгоритъм, който започвайки от едно начално състояние (seed) формира дълга последователност от псевдо случайни числа. При зададено едно и също начално състояние се получава една и съща последователност. Генераторът работи с вътрешно състояние от 624 цели числа, всяко с размер 32 бита, които после се свеждат до „0“ и „1“. Периодът на повторение на дадена комбинация е достатъчно голям (2^{19937}-1 комбинации) и това го прави почти „безкраен“.

Генерирането на случайни числа се осъществява в съответствие със следния израз [110]:

$$X_{k+N_m} = X_{k+O} \oplus X_k D_i, \tag{3.5}$$

където:

X_k са текущите стойности в състоянието на генератора (думи с дължина 32 бита);

N_m е размерът на масива със състояния;

O – отместване в масива;

$\oplus$ – математическа операция сума по модул 2;

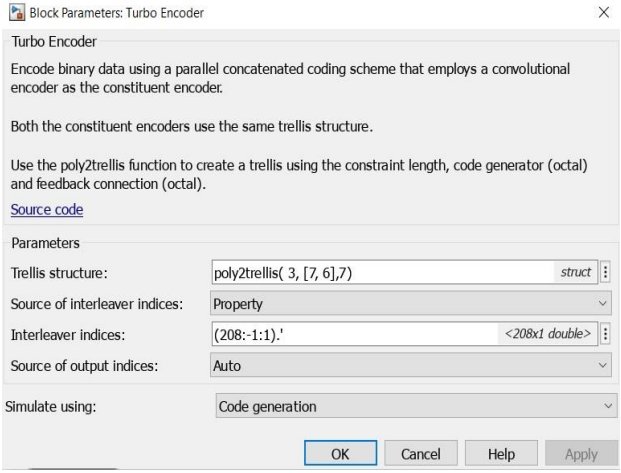
D_i – матрица със зададени размери.

3.3.4. Работа и параметри на турбо кодер.

Турбо кодерът е реализиран с два успоредно свързани RSC кодера и едно разбъркващо устройство между тях. Посредством градивните

елементи на турбо кодера се добавя излишък от битове към предавания поток информационни символи. Добавеният излишък от битове позволява корекция на грешки, възникнали при предаването на информацията. В симулационната среда симулинк, турбо кодерът позволява да се конфигурират различни параметри според предназначението на симулирания комуникационен модел.

Основните параметри, влияещи на работата на турбо кодера, са образуващият полином, който се задава от блока за въвеждане на параметрите в турбо кодера, изобразен на фиг. 3.9. Параметрите са Trellis structure и дължината на входната последователност за интерлийвъра от Interleaver indices.



Фиг. 3.9. Блок за въвеждане на параметрите в турбо кодера

Trellis структурата се формира от следните три елемента:

Trellis = poly2trellis (constraint Length, feed forward, feedback),

Това са:

- Constraint Length - дължина на кодова дума (k);
- feedforward - вектор от генераторни полиноми, които определят изходите на турбо кодера (m_{i1}, m_{i2});
- feedback - един полином, който се използва за обратната връзка.

В този пример полиномът за работата на турбо кодера в среда симулинк се задава в сления вид: poly2trellis (3, [7 6], 7). (пълния списък с изследвани полиноми е поместен в приложение 6).

Цифрата 3 показва дължината на кодовата дума, генераторните полиноми (m_{i1}, m_{i2}) са представени в осмичен вид [7,6]. Тъй като k=3, следва че броят на запаметяващите елементи в регистрите D е L=k-1=2.

Състоянията на регистрите се променят при всеки постъпил текущ бит, като x^0 е текущият постъпил бит, x^1 е един такт закъснение, а x^2 е закъснение два такта закъснение и т.н.

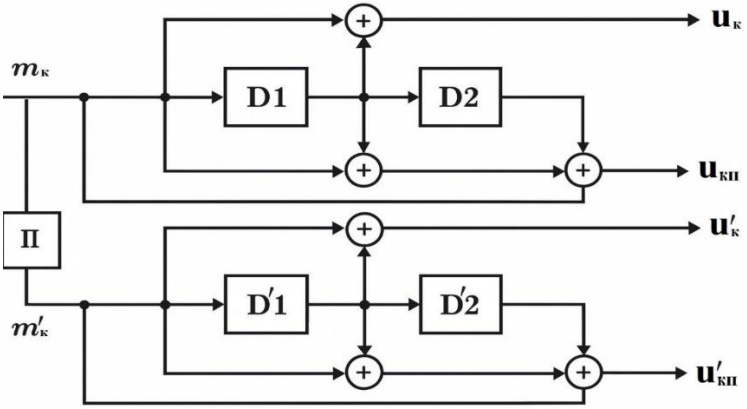
Зададените стойности [7, 6] на генераторните полиноми са в осмичната форма, тъй като турбо кодерът работи с двоични числа, които се преобразуват по следния начин:

- 6_8 (6_2 в двоична форма е 110) и първият генераторен полином е $m_{i1} = \mathbf{1}.x^2+\mathbf{1}.x^1+\mathbf{0}.x^0=x^2+x$
- 7_8 (7_2 в двоична форма е 111) и вторият генераторен полином е $m_{i2} = \mathbf{1}.x^2+\mathbf{1}.x^1+\mathbf{1}.x^0=x^2+x+1$

На фиг. 3.10 е представена блок схема на турбо кодер със зададени параметри poly2trellis(3, [7 6], 7), за която единият изходен сигнал е $\boldsymbol{m_i = x^2 + x}$, а вторият е $\boldsymbol{m'_i = x^2 + x + 1}$.

Числото 2 в степенния показател (x^2) означава, че изходния сигнал m_i е задържан на два такта преди да бъде подложен на сумиране по модул две. В случая дължината на кодова дума е k=3, което означава, че схемата на турбо кодера включва два регистъра D_1 и D_2 за първи RSC кодер и D'_1 и D'_2 за втори RSC кодер. Последователността от битове $m_к$ е входна за системата.

Суматорите по модул 2 се поставят в схемата на турбо кодера според зададените генераторни полиноми. За първи полином m_i се образува изходна последователност $u_к = D_1 \oplus D_2$, а втората изходна последователност $m_{кп}$ се получава при сумиране на текущия бит и $D_1 \oplus D_2$. Обратната връзка се формира при операцията сума по модул две от задържания на два такта бит с текущия. Зададената стойност в полинома е 7, която в двоичен вид е 111.



Фиг. 3.10. Блок схема на турбо кодер със зададени параметри poly2trellis(3, [7 6], 7)

Систематичните конволюционни кодери в кодовия блок позволяват да се отделят информационните от проверовъчните битове. Така в канала за свръзка реално се предават два кодови блока, като първият блок се състои от информационната и проверовъчна част на горния RSC кодер от схемата на фиг.3.10, а вторият кодов блок се състои от разместената информационна и проверовъчна част на долния RSC кодер. Разместената информационна систематична част $m'_{кп}$ на втория кодов блок не се предава в канала за свръзка, защото за нейното възстановяване в декодера се използва устройство за разместване, аналогично на устройството за разместване от кодера.

При отделянето на информационните от проверовъчните битове информацията остава явна, което е позволява на недоброжелатели след натрупване на статистически данни да възстановят предаваната информация.

Предложената схема с допълнителни разбъркващи устройства преди турбо кодера допълнително усложнява задачата за неоторизирано декриптиране на предаваната информация.

3.4. Изводи от трета глава.

1. Турбо кодирането значително повишава надеждността на комуникационния канал, особено когато се използва заедно с разбъркващи устройства, тъй като това намалява вероятността от последователни (пакетни) грешки при предаването на данни.

Използването на два успоредно свързани блока за разбъркване допринася за подобряване скоростта и устойчивостта на предаването на данни в зашумен канал, което прави този подход препоръчителен при реални условия на комуникация.

2. В реални сценарии, трябва внимателно да се изберат параметрите на RSA ключовете и конфигурация на турбо кодера, за да се постигне баланс между сигурност и ефективност на предаване на информацията.

3. Криптиращият алгоритъм RSA е потенциално уязвим, особено когато се използват слаби генератори на случайни числа или се прилагат къси ключове, което подчертава необходимостта от прецизно избиране на криптографските параметри.

4. Важен практически аспект при настройването на симулационната среда е оптимизирането на параметрите на канала на Райс и AWGN канал, за да се моделират реалистично условията на предаване и зашумяване на сигнала, което осигурява максимално близки резултати до действителната работа на комуникационните системи.

ГЛАВА 4. РЕЗУЛТАТИ ОТ ПРОВЕДЕНИТЕ ИЗСЛЕДВАНИЯ НА МОДЕЛА ЗА ОБРАБОТКА НА ИНФОРМАЦИЯТА В КОМУНИКАЦИОННА СИСТЕМА, ОСИГУРЯВАЩ СЪВМЕСТНО ШУМОУСТОЙЧИВО КОДИРАНЕ И ШИФРИРАНЕ НА ИНФОРМАЦИЯТА

В предходната глава е синтезиран модел за обработка на информацията в комуникационна система, осигуряващ съвместно шумоустойчиво кодиране и шифриране на информацията. Чрез решаването на четвъртата задача на дисертационния труд в настоящата глава се обосновава практическата приложимост на синтезирания модел.

4.1. Експериментална постановка на реализираните симулационни модели, използващи турбо кодиране и шифриране.

Симулационният модел на комуникационен канал, използващ шифриране и кодиране с две успоредно свързани разбъркващи устройства, е обоснован в трета глава, параграф 3.2 Той е реализиран в симулационна среда „Simulink“ на софтуерен продукт „Matlab“, версия 2024b. Всички симулации са проведени на 64 битова операционна

система Windows 10, хардуер - Isus FX502V, процесор: Intel(R) Core(TM) i7-6700HQ, CPU 2.60GHz, RAM памет - 24GB.

Изходните параметри, които са зададени на всички симулационни конфигурации, са следните:

- K_{L}-фактор: 10;
- Затихване при разпространение на сигнала (Free Space Path Loss): $FSPL = -119{,}97\ \mathrm{d}B$, изчислено от израз (3.7);
- Разстояние между предавател-приемник: $d_{\mathrm{r}} = 28$км (пресметнато чрез формула 3.8.);
- Времезакъснение на разпространение на полезния сигнал (Path Delay): $Pd = 93{,}33\mu s$ (получено от израз 3.9);
- Мощност на излъчения сигнал: $P_{\mathrm{c}} = 1\ W$;
- Чувствителност на приемника: -90 dBm (1 nW);
- Кодови скорости: R = 1/2, 1/3, 1/4;
- Модулации: BPSK, QPSK, 16-QAM;
- Дължина на предаваното съобщение: 16 бита;
- Брой пъти на предаваното съобщение за една симулация: 1 000 000;
- Диапазон на SNR: 0dB ÷ 30dB, стъпка 0,5dB.

За всяка изследвана кодова скорост (1/2, 1/3 и 1/4) са използвани 48 генеративни полинома (напълно описани в приложение 6) и три вида модулация, а резултатите на всички 144 конфигурации за всяка кодова скорост са представени в приложения 7, 9 и 11. Най-добрите 5 конфигурации, при които се постига оптимално съотношение сигнал/шум от всяка кодова скорост се сравняват със симулационен комуникационен модел. Тук се използва само едно разбъркващо устройство и това е описано в глава 3, параграф 3.2, а базовият комуникационен модел е описан в глава 3, параграф 3.1.

Задачата на симулационния експеримент е да се изследват възможностите за съвместно кодиране и шифриране на информацията, изпращаната по симулационен комуникационен модел, като са заложени максимално неблагоприятни условия за разпространение на сигнала. Целта е да се установят конфигурациите, които най-добре съчетават процедурите по шифриране, турбо кодиране, задаване на

генеративен полином и модулация, достигащи до минимално отношение сигнал/шум (SNR) за различните кодови скорости.

Получените резултати се разделят на следните три критерии:

- За постигнат SNR от 0 до 15 dB и предаване на 10^6 броя съобщения резултатите се считат за отлични (ОР – отлични резултати) и биват допълнително обработвани;
- За SNR в диапазона от 15 до 30 dB се приема, че резултатите са задоволителни (ЗР – задоволителни резултати) и се считат за валидни;
- При SNR над 30dB моделите се считат за незадоволителни (НР – незадоволителни резултати) и не са изследвани в дисертационния труд.

4.2.4. Обобщен статистически анализ на постигнатите резултати на всички 432 конфигурации на моделите с кодови скорости 1/2, 1/3 и 1/4 по параметри: вид декодиране, вид модулация, съотношение сигнал/шум.

Обобщен анализ резултатите от изследването на всички модели при трите, зададени кодови скорости.

От представените резултати от симулативния експеримент следва, че броят на конфигурациите, които отговарят на критерия ЗР при R=1/2 е 59, за R=1/3 са 91, а при скорост R =1/4 броят е 61. Сумарно техният брой е 211 конфигурации, което е ≈ 49 %.

Броят на неотговарящите на този критерий модели е 432 – 211 = 221, т.е. 51% от тези конфигурации. Тези проценти са изобразени на фиг. 4.8.

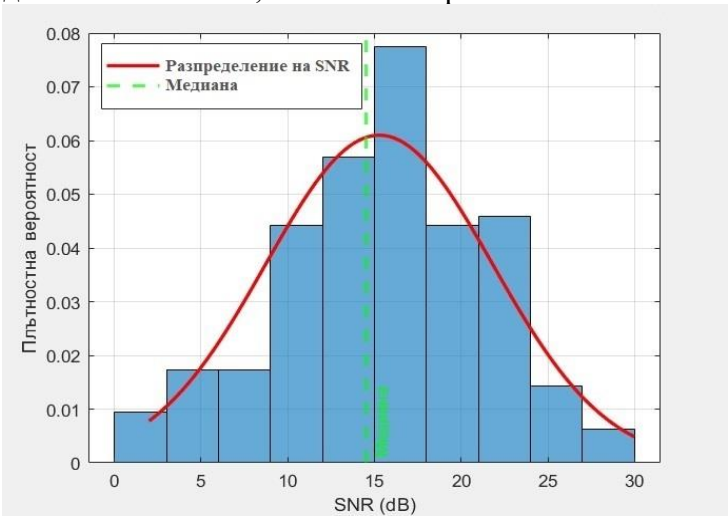
Фиг. 4.8. Кръгова диаграма на обобщените резултати за всички изследвани скорости на кодиране

Статистически анализ на резултатите от изследване на комуникационни модели при кодови скорости R=1/2, R=1/3, R=1/4 (приложения 7, 9 и 11).

Получените резултати за всички изследвани скорости са следните (приложения 7, 9 и 11):

- Минимален SNR = 2 dB;
- Максимален SNR = 30 dB;
- Обхват (Range) = 30 – 2 = 28 dB;
- Математическо очакване (Mean) ≈ 15,27 dB;
- Приблизителна медиана (Median) ≈ 14 – 15 dB;
- Стандартно отклонение (σ) ≈ 6,54 dB.

Изброените характеристики са изобразени на хистограма, която е представена на фиг. 4.9 Тя показва разпределението на вероятностите на приемливите стойности на SNR, получени при обединяване на всички 211 удовлетворяващи конфигурации за трите кодови скорости. Кривата на разпределението показва, че то е по нормален закон.



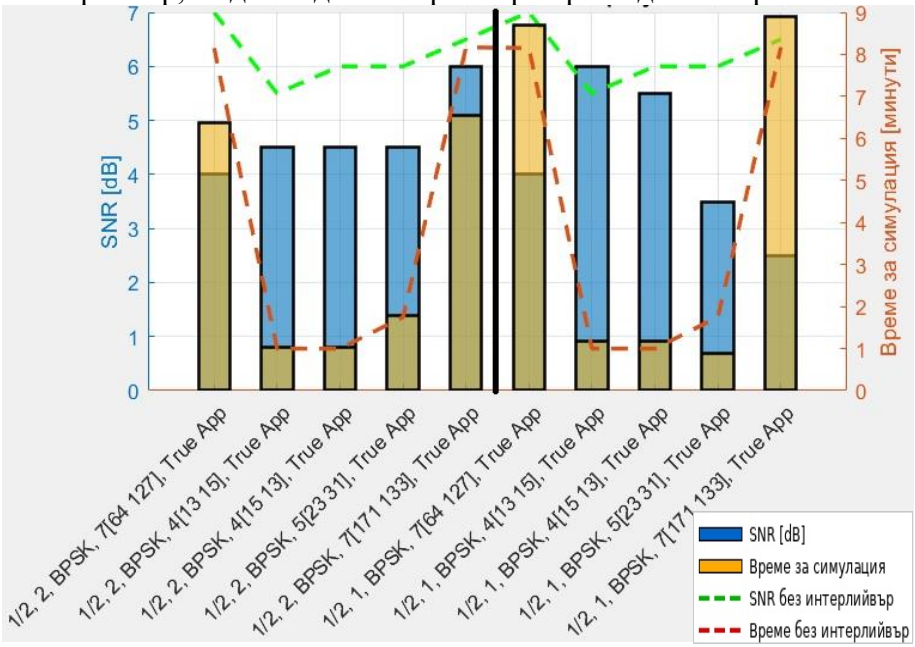
Фиг. 4.9. Хистограма и нормално разпределение на приемливите SNR стойности

Получените стойности на SNR са събрани в интервала 14–16 dB, което е в съответствие с математическото очакване 15,27 dB. Със зелена линия е отбелязана медианата, която има значение около 14–15 dB. Диапазонът (обхват) на изменение на SNR е от 2 dB до 30 dB (28 dB), а

стандартното отклонение е σ ≈ 6,54 dB, което показва умерена разсеяност на резултатите, т.е. повечето стойности са в средния интервал, докато крайни стойности към 2 dB и 30 dB се срещат с по-малка вероятност.

4.3 Анализ на резултатите, получени при използване на оптималните конфигурации с два интерлийвъра спрямо базови комуникационни модели без интерлийвър и симулационен модел с един интерлийвър.

На фиг. 4.15 са обобщени резултатите от комуникационни системи без интерливър, с един и два интерливъра при кодова скорост 1/2.



Фиг. 4.15. Обобщени резултати от комуникационни системи без интерливър, с един и два интерливъра при кодова скорост 1/2

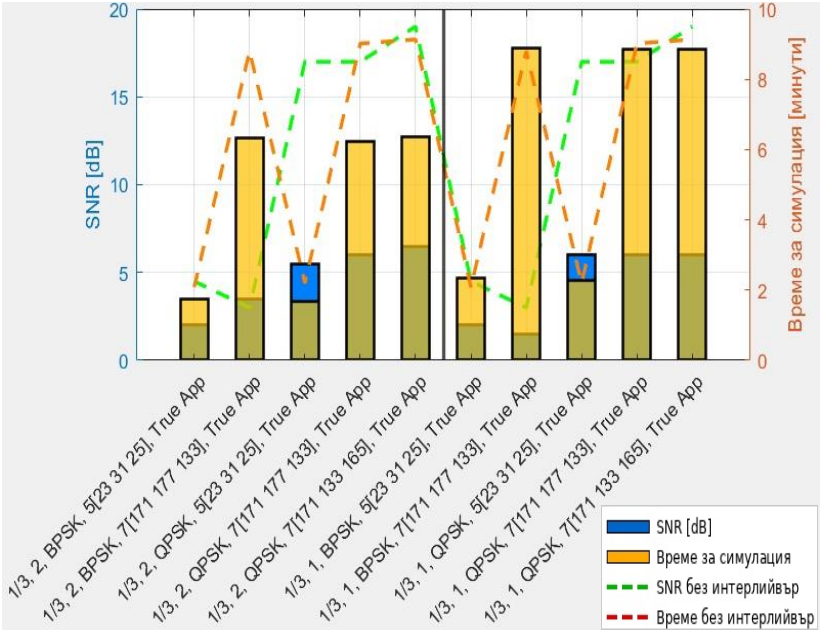
На фиг. 4.15 е представено графическо сравнение на най-добрите конфигурации при кодова скорост R=1/2, вид на модулацията BPSK и декодиращ алгоритъм True-App, като са разграничени два случая – с два интерлийвъра (вляво на фигурата) и с един интерлийвър (вдясно), които са разделени с вертикална черна линия. Сините стълбове отразяват постигнатият SNR, а жълтите стълбове – времето за симулация. Резултатите от базовите комуникационни канали са изобразени с

пунктирни криви. С зелен пунктир е обозначен постигнатия SNR, а с оранжев - продължителността на симулациите.

При конфигурациите с един и два интерлийвъра резултатите, получени при разбъркване (сините стълбове), са разположени под зелената пунктирана линия, което означава, че за същия критерий се изисква по-нисък SNR спрямо моделите без разбъркване. Това показва, че са подобрени коригиращите свойства при използване на един или два интерлийвъра спямо базовия модел, като разликата е в рамките на 0,5–1 dB.

Резултати получени от модели без разбъркващо устройство и скорост на кода 1/3.

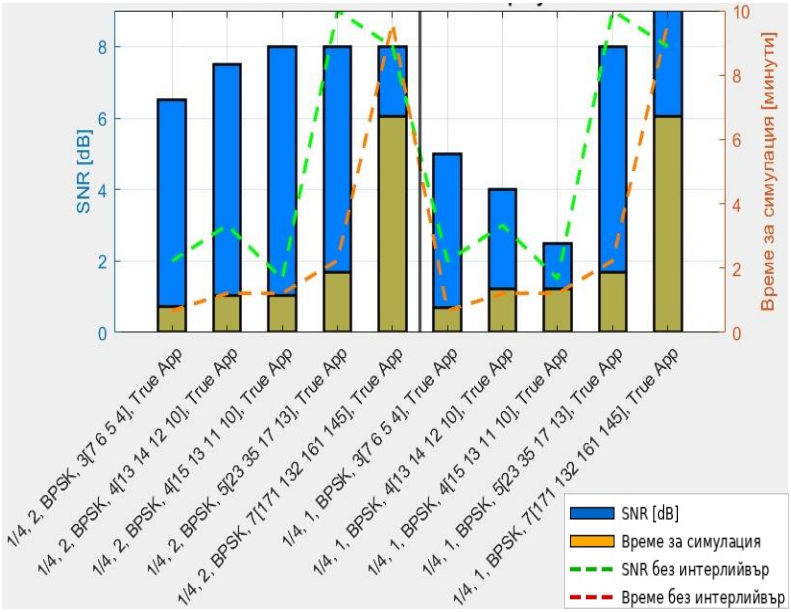
Фиг. 4.19 илюстрира обобщените резултати от конфигурации при скорост R=1/3, като вляво са изобразени получените значения на SNR и времето за симулация при модели с 2 интерлийвъра и вдясно - с 1 интерлийвър, като са разделени с вертикална черна линия. За сравнение са изобразени пунктирани криви: зелена за SNR и оранжева за времето на симулация при базови модели без интерлийвър. Сините стълбове на графиката са разположени под зелената пунктирана линия, което означава необходимостта от по-нисък SNR при предаването на зададените данни. SNR около 1,5 dB се получава при варианта с един интерлийвър и модулация BPSK и полином 7[171 177 133]. При два интерлийвъра най-нисък SNR (около 2 dB) се получава при модулация BPSK с полином 5[23 31 25]. Представянето на конфигурацията с два интерлийвъра отстъпва незначително спрямо постигнатия SNR от модела с един интерлийвър, но значително се намалява времето за симулация.



Фиг. 4.19. Обобщени резултати от комуникационни системи без интерливър, с един и два интерливъра при кодова скорост 1/3

Резултати получени от комуникационни модели без разбъркващо устройство и скорост на кодиране 1/4.

На фиг. 4. 23 са изобразени обобщените резултати от сравняването на комуникационни модели при кодова скорост R=1/4 без интерлийвър спрямо тези с един и два интерлийвъра. Сините стълбове показват SNR [dB], жълтите стълбове – времето за симулация, а зелената и оранжевата пунктирана линия служат за сравнение, като посочват съответно SNR и продължителност на симулацията на базовите модели без интерлийвър. Двете половини на хистограмата са разделени с вертикална черна линия, като вляво са поместени конфигурациите с два интерлийвъра, а вдясно, с един интерлийвър.



Фиг. 4.23. Обобщени резултати от комуникационни системи без интерливър, с един и два интерливъра при кодова скорост 1/4

При кодова скорост R=1/4 най-добро съотношение сигнал/шум се постига без интерлийвър (от 2 до 3 dB). При моделите с един интерлийвър SNR се влошава, спрямо тези без такъв. Конфигурациите, използващи два интерлийвъра, изискват по-висок SNR (от 6,5 до 8 dB), за да предадат зададения брой съобщения без грешка.

4.4. Обобщен анализ на конфигурациите при различен брой разбъркващи устройства, образуващ полином, дължина на кодова дума, скорост на кода и продължителност на симулация.

В таблица 4.18 са представени обобщените резултатите при кодова скорост 1/2, получени при комуникационни модели с едно и две разбъркващи устройства спрямо модели юбез разбъркващи устройства. При скорост R=1/2 компромисно решение между SNR и време за симулация се постига при конфигурация с модулация BPSK и генеративен полином 5[23 31] с едно разбъркващо устройство.

Таблица 4.18

Конфигурация (модулация, ген. полином)	Кодова скорост R	Брой разб. у-ва	SNR [dB]	SNR спрямо конф. без разбъркващо у-во [dB]	Време за преда-ване [min]	Време спрямо модел без разбр. у-ва [%]
BPSK, 4 [1315]	1/2	0	5,5	-	01:00	-
BPSK, 4 [1315]	1/2	1	6	+0,5	01:11	+18,3%
BPSK, 4 [1315]	1/2	2	4	-1,5	01:02	+3,3%
BPSK, 4 [1513]	1/2	0	6	-	01:00	-
BPSK, 4 [1513]	1/2	1	5,5	-0,5	01:11	+18,3%
BPSK, 4 [1513]	1/2	2	4,5	-1,5	01:02	+3,3%
BPSK, 5 [2331]	1/2	0	6	-	01:45	-
BPSK, 5 [2331]	1/2	1	3,5	-2,5	00:54	-48,6%
BPSK, 5 [2331]	1/2	2	4,5	-1,5	01:47	+1,9%
BPSK, 7 [171 133]	1/2	0	6,5	-	08:10	-
BPSK, 7 [171 133]	1/2	1	2,5	-4	08:54	+9%
BPSK, 7 [171 133]	1/2	2	5,5	-1	06:33	-19,8%
BPSK, 7 [64127]	1/2	0	7	-	08:09	-
BPSK, 7 [64127]	1/2	1	4	-3	08:42	+6,7%
BPSK, 7 [64127]	1/2	2	4	-3	06:23	-21,7%

Спрямо модела без разбъркващо устройство за същия полином SNR се подобрява, като от 6 dB спада на 3,5 dB (подобрение с -2,5 dB).

При моделите с един и два интерлийвъра, модулация BPSK и генеративен полином 7[64 127] се наблюдава подобрение на SNR спрямо модела без разбъркващо устройство, което се изразява намаляване от 7 dB на 4 dB (подобрение -3,0 dB).

При модел с едно разбъркващо устройство, модулация BPSK и генеративен полином 7[171 133] се постига подобрение на SNR спрямо модела без разбъркващо устройство от 6,5 dB на 2,5 dB (подобрение -4,0 dB). Това е компромисен вариант за достигане на по-нисък SNR при по-сложни модели, но с по-продължителна симулация.

В таблица 4.19 са анализирани резултатите от конфигурации без, с едно и две разбъркващи устройства, при кодова скорост R=1/3, при модулации BPSK и QPSK и различни генеративни полиноми. Отчетени

са SNR, продължителност на симулация и разликите в постигнатите стойности спрямо базов модел без разбъркващо устройство.

Таблица 4.19

Конфигурация (Модулация, ген. полином)	Кодова скорост R	Брой разб. у-ва	SNR [dB]	SNR спрямо конф. без разбъркващо у-во [dB]	Време за предаване [min]	Време спрямо модел без разбр. у-ва [%]
BPSK, 5 [23 31 25]	1/3	0	4,5	-	02:05	-
BPSK, 5 [23 31 25]	1/3	1	2	-2,5	02:20	+12%
BPSK, 5 [23 31 25]	1/3	2	2	-2,5	01:45	-16%
BPSK, 7 [171 177 133]	1/3	0	3	-	08:48	-
BPSK, 7 [171 177 133]	1/3	1	1,5	-1,5	08:54	+1,1%
BPSK, 7 [171 177 133]	1/3	2	3,5	+0,5	06:19	-28,2%
QPSK, 5 [23 31 25]	1/3	0	17	-	02:12	-
QPSK, 5 [23 31 25]	1/3	1	6	-11	02:17	+3,8%
QPSK, 5 [23 31 25]	1/3	2	5,5	-11,5	01:40	-24,2%
QPSK, 7 [171 133 165]	1/3	0	19	-	09:08	-
QPSK, 7 [171 133 165]	1/3	1	6	-13	08:52	-2,9%
QPSK, 7 [171 133 165]	1/3	2	6,5	-12,5	06:22	-30,3%
QPSK, 7 [171 177 133]	1/3	0	17	-	09:01	-
QPSK, 7 [171 177 133]	1/3	1	6	-11	08:51	-1,8%
QPSK, 7 [171 177 133]	1/3	2	6	-11	06:14	-30,9%

При кодова скорост R=1/3 най-голямо подобрение по критерия за минимално SNR спрямо модела без разбъркващо устройство се постига при конфигурацията, използваща модулация QPSK и генеративен

полином 5[23 31 25]. При модел с едно разбъркващо устройство SNR се подобрява, спрямо същата конфигурация без интерлийвър от 17dB на 6dB (подобрение от -11dB). При модел с две разбъркващи устройства SNR достига 5,5 dB, като подобрението е -11,5dB спрямо модела без интерлийвър.

При конфигурация, използваща модулация BPSK, полином 7[171 177 133] и едно разбъркващо устройство се постига по-ниска стойност на SNR спрямо модела без разбъркване. Резултатите показват, че SNR намалява от 3dB на 1,5 dB (подобрение -1,5 dB).

При модел с две разбъркващи устройства се наблюдава обратната зависимост: SNR се влошава от 3 dB на 3,5 dB (влошаване +0,5 dB).

В таблица 4.20 са представени обобщени резултатите при кодова скорост R=1/4, модулация BPSK и различни генеративни полиноми, като се сравняват трите симулационни модела: без разбъркващо устройство, с едно разбъркващо устройство и с две разбъркващи устройства. Представени са значенията на SNR, времето за симулация и измененията им спрямо базовия модел без разбъркващи устройства.

При кодова скорост R=1/4 и конфигурацията с модулация BPSK, полином 4[15 13 11 10] най-нисък SNR се постига при модела без разбъркващо устройство: SNR=1,5 dB. Моделът с едно разбъркващо устройство влошава SNR спрямо модела без разбъркване от 1,5 dB на 2,5 dB (влошаване +1,0 dB).

При две разбъркващи устройства SNR се влошава спрямо модела без разбъркване до 8 dB (влошаване +6,5 dB), въпреки че продължителността на предаване на данни се съкращава.

При конфигурацията с модулация от типа BPSK, генеративен полином 3[7 6 5 4], моделът без разбъркване е оптимален по SNR и по продължителност на симулацията. При модела с едно разбъркващо устройство SNR се влошава до 5 dB (+3,0 dB).

Таблица 4.20

Конфигурация (Модулация, ген. полином)	Кодова скорост R	Брой разб. у-ва	SNR [dB]	SNR спрямо конф. без разбъркващо у-во [dB]	Време за предаване [min]	Време спрямо модел без разбр. у-ва [%]
BPSK, 3 [7 6 5 4]	1/4	0	2	-	00:41	-
BPSK, 3 [7 6 5 4]	1/4	1	5	+3	00:47	+14,6%
BPSK, 3 [7 6 5 4]	1/4	2	6,5	+4,5	00:48	+17,1%
BPSK, 4 [13 14 12 10]	1/4	0	3	-	01:13	-
BPSK, 4 [13 14 12 10]	1/4	1	4	+1	01:22	+12,3%
BPSK, 4 [13 14 12 10]	1/4	2	7,5	+4,5	01:09	-5,5%
BPSK, 4 [15 13 11 10]	1/4	0	1,5	-	01:13	-
BPSK, 4 [15 13 11 10]	1/4	1	2,5	+1	01:22	+12,3%
BPSK, 4 [15 13 11 10]	1/4	2	8	+6,5	01:09	-5,5%
BPSK, 5 [23 35 17 13]	1/4	0	9	-	02:14	-
BPSK, 5 [23 35 17 13]	1/4	1	8	-1	01:52	-16,4%
BPSK, 5 [23 35 17 13]	1/4	2	8	-1	01:53	-15,7%
BPSK, 7 [171 132 16 1145]	1/4	0	8	-	9:37	-
BPSK, 7 [171 132 161 145]	1/4	1	9	+1	06:43	-30,2%
BPSK, 7 [171 132 161 145]	1/4	2	8	0	06:44	-30%

При конфигурацията с две разбъркващи устройства SNR достига стойност 6,5 dB (влошаване с +4,5 dB), в сравнение с базовия модел.

Изключение прави конфигурацията с кодова скорост R=1/4, модулация BPSK и полином 5[23 35 17 13], при която добавянето на разбъркващи устройства подобрява резултатите едновременно и по двата критерия спрямо модела без разбъркващо устройство. Отношението SNR намалява от 9 dB на 8 dB (подобрение -1,0 dB, спрямо базовия модел.

Общ анализа на резултатите от таблици 4.21, 4.22 и 4.23.

Анализът показва, че приложението на различен брой разбъркващи устройства е силно зависимо от кодовата скорост и конкретния образуващ полином.

При кодова скорост R=1/2 удовлетворяващ резултат между значение на SNR и продължителност на симулацията се наблюдава при модели с модулация BPSK, генеративен полином 5[23 31] и едно разбъркващо устройство. Спрямо модела без интерлийвър SNR се подобрява от 6 dB на 3,5 dB.

При кодова скорост R=1/3 най-добър SNR спрямо модел без разбъркващо устройство се получава при конфигурация с две разбъркващи устройства, модулация QPSK, полином 5[23 31 25], при което SNR се понижава от 17 dB до 5,5 dB.

При кодова скорост R=1/4, за разлика от R=1/2 и R=1/3, моделите с едно и две разбъркващи устройства влошават SNR, което при генеративен полином 4[15 13 11 10] се изразява в SNR от 1,5 dB без интерливър, докато при модели с един интерлийвър SNR достига до 2,5dB, и при два интерлийвъра до 8dB.

При необходимост от от баланс между SNR и минимално време за предаване на данни, следва да се избере конфигурация със скорост на кодиране R=1/3 и модулация QPSK. За оптимален SNR следва да се приложат конфигурации на модел с R=1/2 и модулация BPSK. От анализираните резултати следва, че използването на модели при кодова скорост R=1/4 с разбъркващи устройства не е удачно, поради влошаването на SNR спрямо този при базовия модел.

4.5. Изводи от четвърта глава.

1. Моделите с поставени два интерлийвъра преди турбо кодера демонстрират по-добри резултати от тези с едно разбъркващо устройство, особено при кодови скорости R=1/2 и R=1/3. По отношение

на SNR подобрението спрямо базовите комуникационни модели е между 40 и 70%.

2. При кодова скорост R=1/4 моделите с добавен един интерлийвър преди турбо кодер постигат близки стойности на SNR спрямо конфигурациите с два интерлийвъра.

3. Добавянето на разбъркващи устройства при модели с кодова скорост R=1/4 не е целесъобразно, поради влошаването на отношението SNR спрямо базовите комуникационни модели.

ОБЩИ ИЗОВОДИ

В периода на COVID-19 (2019-2022г) възникнаха нови, по-високи изисквания към дигиталните услуги поради дистанционния метод на работа и обучение.

Избухването на два сериозни военни конфликта, активни към днешна дата, които неоспоримо показаха технологично напреднали оръжия, радарни и сателитни, разузнавателни и насочващи устройства, които доведоха до напълно нови тактики на бойното поле, изискващи безапелационна комуникационно-информационна свързаност чрез шумоустойчиви и криптирани комуникации канали от персонално до командно ниво. Тези и други мотиви налагат задълбоченото изучаване на комуникационните канали с шумоустойчиво и скрито предаване на данни.

Кодирането на канала е задължителна стъпка при съвременните безжични комуникации. То става с добавяне на излишни битове, с което се минимизират грешките при предаване на цифрови данни в силно зашумена комуникационна среда.

Криптиране на информацията е наложителна тъй като личната и корпоративната сигурност е в постоянна опасност от компрометиране заради зачестилите кибератаки.

Целта на дисертационния труд е изследването на възможностите за съчетаване на шумоустойчиво кодиране и шифриране, осигуряващи оптимално съотношение сигнал/шум и скритост на предаваните данни.

В първа глава са разгледани и анализирани научни доклади засягащи съвременните тенденции при различните алгоритми за шифриране на информацията, а така също и постигнати резултати при комуникационни системи използващи шумоустойчиво кодиране.

Във втора глава е описан детайлно математическия модел на работа на използваните алгоритми за кодиране и шифриране на информацията. Предложена е концепция за хибридно използване на симетрични и асиметрични алгоритми за криптиране на предаваните данни по незащитен канал.

В трета глава е извършен синтез на модел за обработка на информацията в комуникационна система, осигуряващ съвместно шумоустойчиво кодиране и шифриране на информацията.

В четвърта глава е извършен математически и статистически анализ на получените резултати от проведените изследвания на модела за обработка на информацията в комуникационна система, осигуряващ съвместно шумоустойчиво кодиране и шифриране на информацията.

Изследвани са 432 конфигурации на комуникационни системи, с 48 образуващи полинома, 4 дължини на кодови думи, три вида скорост на кода и три вида модулация на сигнала. 50% от разгледаните конфигурации покриват критерия SNR=30dB. Така също 28% попадат в критерия SNR=15dB. Най-добрите постигнати резултати са между 2-15dB.

При комуникационните конфигурации със скорост 1/4, резултатите показват, че добавянето на разбъркващи устройства влошава съотношението сигнал/шум и не е приложим метод.

Най-добрите резултати постигнати с две успоредно свързани разбъркващи устройства към комуникационния модел са сравнени с модели с едно разбъркващо устройство и с базов комуникационен модел. Резултатите показват, че при кодови скорости 1/2 и 1/3 комуникационните модели с две разбъркващи устройства показват близки стойности спрямо тези с едно разбъркващи у-во, като и двата способа добавят допълнителна скритост на информацията**.**

Добавянето на асиметричен RSA метод за криптиране на сесийните ключове на основния AES алгоритъм за криптиране на информация не влияе на работата на турбо декодера по приемане и поправка на сгрешени битове, също така не влошава съотношението сигнал/шум, **с което е изпълнена целта на дисертационния труд, а именно да се разработят алгоритми за шумоустойчиво кодиране, осигуряващи едновременно максимално отношение сигнал/шум и висока криптографска защита на предаваните данни чрез**

изпълнение по единен замисъл на различни етапи в процеса на обработка на информацията в комуникационните системи.

НАУЧНИ ПРИНОСИ:

1. Разработен е подход за шумоустойчиво криптиране на комуникацията посредством комбинирано използване на алгоритми RSA и AES (§2.3).

НАУЧНОПРИЛОЖНИ ПРИНОСИ:

1. Анализирани са и са систематизирани операциите на обработка на информаията в специализираните комуникационни системи, използвани в БА, полицията и при защита на населението отбедствия и аварии (§1.1);
2. Анализирани са известните технологии за съвместно използване на шумоустойчиво кодиране и шифриране (§1.2);
3. Синтезиран е модел за обработка на информацията в комуникационна система, осигуряващ съвместно шумоустойчиво кодиране и шифриране на информацията. (§3.2).

ПРИЛОЖНИ ПРИНОСИ:

Синтезирани са и са реализирани в средата на Матлаб следните алгоритми:

1. Алгоритъм за генериране на ключове за асиметрично RSA шифриране(§2.2);
2. Алгоритъм за генериране на ключове за симетрично AES шифриране (§2.2).

Синтезирани са и са разработени в средата на Simulink модели на:

1. Симулационен модел на базов комуникационен канал без разбъркващи устройства (§3.1) ;
2. Симулационен модел на комуникационен канал с добавено едно или две разбъркващо устройство преди турбо кодера и подреждащи устройства след турбо декодера (§3.2);

Посочените модели и алгоритми могат да бъдат използвани като инструмент за проектиране и оценка на защитени комуникационни системи.

3. По метода на симулационното моделиране е доказано, че комбинираното използване на алгоритмите RSA и AES, съчетано с шумоустойчиво кодиране, е приложимо за системи с ограничени

ресурси, като БЛА, IoT или други устройства с вградени комуникационни модули. (§4.4).

СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИЯТА

1. Стоянов, Д., Бочев, Л., Радев, Ив., Първанов, Ст., „Подходи за повишаване киберсигурността при управлението на енергийната инфраструктура“, Русе: Научни трудове на Русенския университет – 2021 г., том 60, издание 3.3.,стр. 182-193, FRI-ONLINE-1-CCT2-08 , ISSN 2603-4123;
2. Илиев М., Беджев Б., Стоянов Д., Първанов Ст. „Технологии за повишаване устойчивостта на умните мрежи към имитационни атаки“, Русе: Научни трудове на Русенския университет – 2021 г., том 60, издание 3.3., стр.138-144, FRI-ONLINE-1-CCT2-02, ISSN 2603-4123;
3. Георгиев Г., Първанов Ст,. Козарев К., “Техники за защита на ключови обекти от безпилотни летателни средства“, Русе: Научни трудове на Русенски университет – 2022 г., том 61, сесия 3.2.,стр. 207-216, 2G.302-2-CCT2-10, ISSN 1311-3331;
4. Маринов Д., Неделчев М., Стоянов Д., Първанов, Ст,. “Подход за изграждане на защитена комуникация посредством комплементарни сигнали“, Русе: Научни трудове на Русенски университет – 2022 г., том 61, сесия 3.2., стр. 153-160, 2G.302-2-CCT2-01, ISSN 1311-3321;
5. Първанов, Ст., Димов, Д., Радев, Ив., „Изследване на различни видове алгоритми за декодиране на турбо кодове и тяхното съвместно използване с блок за криптиране“, сборник с доклади от международна научна конференция „Отбранителни технологии“ DefTech 2022 г., Факултет „Артилерия, ПВО и КИС“ – гр. Шумен, стр.407-413 ISSN 2367-7902;

“VASIL LEVSKI” NATIONAL MILITARY UNIVERSITY

FACULTY OF ARTILLERY, AIR DEFENCE AND CIS
9713, Shumen, “Karel Skorpil” Street - №1
phone: (054)801 040; fax:(054)877 463;
e-mail: nvu-sh@aadcf.nvu.bg

DEPARTMENT OF AIR DEFENCE

Assist. Eng. Stanimir Hristov Parvanov

INVESTIGATION OF THE POSSIBILITIES FOR THE JOINT APPLICATION OF ERROR-CONTROL CODING AND ENCRYPTION IN COMMUNICATION SYSTEMS

THESIS ABSTRACT

for the award of the educational and scientific degree “Doctor” (PhD)
Doctoral programme in the scientific specialty:
“Communication Networks and System”
SCIENTIFIC FIELD: 5. TECHNICAL SCIENCES
PROFESSIONAL FIELD 5.3. COMMUNICATION AND COMPUTER TECHNOLOGY

Scientific supervisor:

Assoc. Prof. Eng. Vencislav Mitkov Vasilev, PhD

Shumen

2026г.

The dissertation was discussed at a meeting of the Department Council of the Department of "Air Defence" at the Faculty of "Artillery, Air Defence and CIS", National Military University "Vasil Levski", held on __.__.2026 in Hall №__, and has been scheduled for official defence before a scientific jury composed of:

_____

_____

_____

_____

The doctoral candidate is an Assistant Professor at the Department of "Radar and Communication Systems" at the Faculty of "Artillery, Air Defence and CIS" of the National Military University "Vasil Levski" – Veliko Tarnovo.

The main research related to the dissertation was conducted in the MATLAB development software environment.

Author: Assist. Eng. Stanimir Hristov Parvanov.

Topic: "Investigation of the Possibilities for the Joint Application of Error-Control Coding and Encryption in Communications".

Print run: __
Printed on: .._.__.__.2026
Publishing Complex of the National Military University "Vasil Levski"

The dissertation comprises: number of pages – 167; number of figures – 58; number of tables – 28; number of appendices – 13; Number of references – 129, number of publications related to the dissertation – 5.

The numbering of the figures, tables, and formulae in the abstract corresponds to that used in the dissertation.

The thesis defence materials are available at the Department of "Air Defence".

Motivation for Developing the Dissertation

- There is a growing need for the development of secure communication systems capable of protecting sensitive information from unauthorized access, malicious interference, and compromise. In this regard, modern communication organizations are increasingly implementing advanced cryptographic protocols that ensure confidential and protected data exchange in an Internet-based environment;
- The current standards and regulatory requirements related to the storage, processing, and transmission of information require strict compliance with established rules. This obliges communication companies to apply reliable data protection mechanisms, since violations may result in significant sanctions imposed by regulatory authorities;
- The collection, processing, and sharing of user data increase the risk of cybercrime, information leakage, and unlawful use of personal data. This determines the need for a higher level of control, as well as for the development of effective policies for the use, storage, and protection of information;
- In addition to cryptographic protection, the application of error-correcting coding is becoming increasingly important, since data transmission over real communication channels is accompanied by the influence of noise, interference, and transmission errors. The combination of encryption and error-correcting coding enables the simultaneous enhancement of both the security and reliability of the communication process;
- Modern business processes, government institutions, and cloud infrastructures generate substantial volumes of information, which necessitates the use of reliable technologies for data archiving, storage, and exchange. This gives rise to the need for communication solutions that ensure both content protection and transmission resilience under adverse communication conditions.

Relevance of the Problem Addressed in the Dissertation

Information coding and encryption are essential elements in the process of establishing and operating communication networks. Coding minimizes errors in the transmission of digital data by ensuring a predefined level of reliability of the received information bits through the addition of check and control bits. On the other hand, information encryption provides the most

effective protection against the increasing frequency of cyberattacks and the compromise of personal data.

In general, however, the application of both coding and encryption complicates the processes of information transmission and processing and reduces the rate of information transfer. This necessitates the development of approaches for the joint application of error-control coding and encryption, ensuring simultaneously high cryptographic robustness, noise immunity, and the required information transmission rate through the most rational use of the capabilities of the hardware and software components of communication systems.

Aim of the Dissertation

The aim of the present dissertation is to develop algorithms for error-control coding that ensure simultaneously a maximum signal-to-noise ratio and a high level of cryptographic protection of the transmitted data through the integrated implementation, within a unified concept, of different stages in the process of information processing in communication systems.

Subject of the Dissertation

The subject of the dissertation comprises the methods and algorithms for error-control coding and encryption in communications under the influence of passive and active interference; the computational procedures for determining the optimal values of the encoder generator polynomial; the code rate; the type of decoding; and the influence of different types of information encryption on the data transmission rate in the communication channel.

Scientific Novelty

The theory of turbo coding has been further developed by substantiating approaches for the synthesis of turbo encoders that simultaneously provide different code rates and encryption of the transmitted information. Within the coding algorithm, the addition of an interleaving device immediately after the message source is substantiated. This ensures a high level of cryptographic protection of the transmitted data and enables the achievement of the required signal-to-noise ratio when transmitting information signals in the presence of interference.

Practical Applicability

A model has been developed for combining error-control coding and encryption in the communication channel, ensuring the required signal-to-noise ratio and a high level of protection against unauthorized access.

Contents of the Dissertation

CHAPTER ONE: Analysis of the design principles of communication systems used in the Bulgarian Army, the police, and the system for fire safety and civil protection.

CHAPTER TWO: Fundamental technologies for communication-channel coding. Hybrid application of symmetric and asymmetric encryption algorithms for data transmitted over an unsecured channel.

CHAPTER THREE: Synthesis of a model for information processing in a communication system ensuring the joint implementation of error-control coding and information encryption.

CHAPTER FOUR: Results from the conducted studies of the information-processing model in a communication system ensuring the joint implementation of error-control coding and information encryption.

SUMMARY OF THE DISSERTATION

CHAPTER ONE ANALYSIS OF THE DESIGN PRINCIPLES OF COMMUNICATION SYSTEMS USED IN THE BULGARIAN ARMY, THE POLICE, AND THE SYSTEM FOR FIRE SAFETY AND CIVIL PROTECTION

Secure and reliable communications constitute the foundation for the effective functioning of contemporary communication systems applied in various spheres of public life, including defence, internal security, civil protection, policing, and related domains. In an era marked by active hybrid threats, cyberattacks, and electromagnetic impacts, the protection of the physical layer in the transmission of the useful signal becomes a priority. Under real combat or emergency conditions, the signal in a communication system is often weak and affected by noise, which may lead to erroneous decisions. This necessitates continuous research into error-correction technologies and data-transmission optimisation, the ultimate objective being the achievement of reliable, secure, and high-speed communication.

1.1. Importance of Noise Immunity for Contemporary Communication Systems Used in the Bulgarian Army, the Police, and the System for Fire Safety and Civil Protection

The noise immunity of a communication system represents its ability to maintain a low bit error rate (BER), even in the presence of noise. In practice, the most commonly encountered noise models are additive white Gaussian

noise (AWGN) and Rayleigh fading, which are characteristic of military and police communications [3].

The communication systems of the Ministry of Defence and the Ministry of Interior employ robust radio-frequency links operating in both licensed and unlicensed frequency bands and at different levels of protection. Systems such as TETRA, DMR, and LTE/5G require reliable channel-level coding in order to overcome active jamming, broadband noise attacks, and interference originating from hostile sources [2].

An important element in many turbo-code coding schemes is the interleaver, which permutes the order of bits prior to transmission, so that consecutive channel errors are distributed over distant positions during decoding. A properly designed interleaver prevents the formation of short cycles in decoding algorithms and reduces the probability of the so-called "error floor", i.e. the stagnation of errors at a high signal-to-noise ratio (SNR) [26].

1.2. Analysis of Known Technologies for the Joint Application of Error-Control Coding and Encryption

For military and specialised communication systems, it is equally important that the message be received without errors and that it remain confidential and protected. Security, provided through encryption, and reliability, provided through channel coding, are generally treated as separate layers.

Military communications are conducted under conditions of high noise levels, interference, and intentional jamming. This requires the use of technologies that render communications highly resilient. In analogue systems, methods such as frequency hopping and spread spectrum are applied [46].

In digital technologies, analogue schemes are combined with powerful channel codes and encryption in order to provide comprehensive protection. At the tactical level of NATO communications, concatenated codes, such as Reed–Solomon codes or convolutional coding, are used to correct packet or bit errors in long-distance satellite communications. With the introduction of STANAG standards for military communications, turbo codes have also found application, offering high reliability at low signal-to-noise ratios [46].

The most widely used asymmetric encryption method, RSA, enables the secure transmission of information even between parties that have never previously exchanged confidential information. It is used in electronic commerce, secure banking, government systems, and in almost all protocols forming the basis of Internet security [99]. Within the public key

infrastructure supporting Internet certificates, RSA still remains the most widespread algorithm for digital signatures [105]. Major institutions, banks, and governments rely on RSA for critical operations, since its behaviour has been studied in great depth. Communication protocols have used RSA for key exchange for a long period of time. Although newer versions of TLS are shifting towards elliptic-curve-based methods, RSA remains an important element for backward compatibility and for systems in which performance is not the primary factor. In combination with symmetric algorithms such as AES, RSA remains a reliable mechanism for establishing secure sessions.
Quantum computing calls into question the future of RSA. Shor's algorithm demonstrates that factorisation can be performed efficiently on a quantum computer [106]. This threat, however, remains hypothetical at present, since there is currently no quantum computer capable of breaking practically used key sizes. In the foreseeable future, RSA therefore continues to be a fully justified choice for data protection.

1.3. Conclusions from Chapter One. Tasks of the Dissertation

1. Under contemporary conditions, noise protection and cryptographic robustness are parameters of critical importance for the communication systems used by the armed forces, the police, fire-safety services, and civil protection structures in cases of disasters and emergencies. This necessitates the improvement of established channel codes, such as turbo, convolutional, LDPC, and other codes, as well as the introduction of innovative solutions, including interleavers operating with different permutation methods and communication systems combining encryption and coding in a unified manner.

2. At present, progress in the field of error-control coding and encryption is largely characterised by the development and practical implementation of algorithms that preserve the integrity of information even at low signal-to-noise ratios, under intense interference, or in conditions of malicious suppression of communication signals.

3. The analysis of the results from theoretical and experimental-design developments in the field of coding and encryption, known from open-access information sources, reveals the need for a systematic approach to the improvement of turbo codes. On the one hand, they approach very closely the so-called Shannon limit in practical terms, their energy efficiency being only approximately 0.5 dB below the theoretical boundary value. On the other

hand, their structure allows various encryption technologies to be technically integrated in a relatively simple manner.

In view of the above conclusions, the aim of the dissertation is:
To develop algorithms for error-control coding that ensure simultaneously a maximum signal-to-noise ratio and a high level of cryptographic protection of the transmitted data through the implementation, within a unified concept, of different stages in the process of information processing in communication systems.

In order to achieve this aim, the following principal tasks must be addressed:

1. To analyse the known approaches for the joint application of error-control coding and encryption.
2. To systematise the main stages of data processing in error-control coding, as well as in symmetric and asymmetric encryption algorithms applied to messages transmitted over an unsecured channel.
3. To synthesise a model for information processing in a communication system that ensures the joint implementation of error-control coding and information encryption.
4. To investigate, by means of simulation-based computer modelling, the practical applicability of the information-processing model in a communication system that ensures the joint implementation of error-control coding and information encryption.

CHAPTER TWO. FUNDAMENTAL TECHNOLOGIES FOR COMMUNICATION-CHANNEL CODING. HYBRID APPLICATION OF SYMMETRIC AND ASYMMETRIC ENCRYPTION ALGORITHMS FOR DATA TRANSMITTED OVER AN UNSECURED CHANNEL.

Error-control coding and encryption address different tasks in communication systems. For this reason, a positive effect resulting from their implementation within a unified concept can be achieved only through the integration of some of their individual stages. This, however, requires a more detailed analysis of the technical procedures involved in error-control coding and encryption, as well as the identification of the similarities and analogies between them. In view of this fact, the present chapter addresses the second task of the dissertation.

2.1. General Characteristics of Convolutional and Turbo Codes.

Channel error-control coding is a fundamental process in digital communications, whose primary objective is to protect the transmitted information from errors arising during transmission through a non-ideal communication channel. This is achieved by the intentional addition of redundant bits to the output information stream. A number of coding methods are known:

- block codes, in which the information is processed in blocks of fixed length; examples include Hamming codes, Reed–Solomon codes, and BCH codes;
- systematic codes, where the data to be processed are information streams and the output result depends on the current and previous input bits; systematic codes include LDPC codes, or low-density parity-check codes, and turbo codes, which are based on convolutional codes. Linear block codes are defined by a fixed generator matrix G and a parity-check matrix H [109].

The mathematical representation of a linear block encoder is of the following form:

$$c = u.\boldsymbol{G} \tag{2.1}$$

where:

- **c** is the output code word;
- **u** denotes the input information bits;
- **G** denotes the generator matrix.

By means of the parity-check matrix H, the error syndrome is calculated as follows:

$$S = r.\boldsymbol{H}^{\mathbf{T}} \tag{2.2.}$$

- where:
- S is the error syndrome;
- r is the received code word;
- H^{T} is the transposed parity-check matrix.

If the syndrome is S=0, the receiver “decides” that no errors have occurred. If S≠0, the receiver “decides” that an error has occurred.

The generator and parity-check matrices are always compatible, i.e. every code word satisfies the condition:

$$\boldsymbol{G}.\boldsymbol{H}^{\mathbf{T}} = 0 \qquad (2.3.)$$

The principal distinction between linear block codes and convolutional codes lies in the coding principle. The architecture of convolutional encoders includes shift registers that store the state of the system, as well as generator polynomials describing the relationships between the inputs and outputs. The turbo encoder represents a higher level in the field of coding. It consists of a parallel concatenation of two recursive systematic convolutional encoders, separated by an interleaving device referred to as an interleaver [5,6, 25,36].

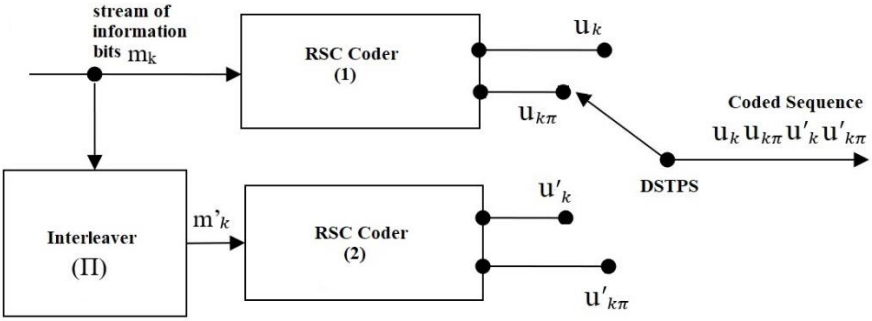


Fig. 2.3. Block Diagram of a Turbo Encoder

Figure 2.3 presents a block diagram of a turbo encoder. The input data sequence $m_k = [m_1, m_2, \dots, m_n]$ is applied to recursive convolutional encoder 1, where the information is combined by modulo-two addition. At its output, a coded data stream u_k is obtained, which is then applied to a multiplexer and to a device for the selective transmission of the parity output streams.

The input data sequence m_k is also applied to the interleaving device, where a predefined number of bits is first stored. These bits are then permuted according to a pseudorandom law and applied to the input of the second RSC encoder, whose structure and operation are identical to those of the first encoder. Both encoders operate at a rate of (1/2), which means that, for each unchanged information bit from the input sequence, the encoder generates two bits at its output. The value of the systematic output (u_k) of the first RSC encoder at the *i*-th clock cycle coincides with the value of the input bit (m_k), while a parity bit ($u_{k\pi}$).is formed at the second output.

The systematic output of the second RSC encoder is not used, while a second parity bit $u'_{k\pi}$ is formed at its other output. At the output of the turbo encoder, the bit u_k from the systematic output of the first encoder appears first, followed by the two parity bits $u_{k\pi}$ and $u'_{k\pi}$ from the first and second RSC encoders. The code rate R of the entire turbo encoder is 1/3, since one input bit produces three output bits, formed by the outputs u_k, $u_{k\pi}$, $u'_k\pi$.

It is possible to form a shortened punctured code in which the bits from the parity outputs of the encoders are multiplexed by a device for the selective transmission of the parity output streams(DSTPS). In this case, the unchanged sequence of information bits alternates from one clock cycle to the next, with a parity bit being taken successively from either the first or the second RSC encoder. This reduces the error-correction capability of the code, but the code rate increases to (1/2). Through the use of systematic convolutional encoders in the coding block, the information bits are separated from the parity bits. It is considered that the information from two code blocks is actually transmitted through the communication channel. The first block includes the information and parity parts of the first RSC encoder, while the second code block contains the interleaved information and parity parts of the second RSC encoder. At the output of the turbo encoder, a data stream is formed, which is applied to the turbo decoder, where error checking is performed. The turbo decoder extracts the systematic and parity bits from the received data sequence. The block diagram of the turbo decoder is presented in Fig. 2.4. The binary coded input sequence for the turbo decoder is represented in the following form:

$$R_k = [\, u_k, u_{k\pi}, u'_k, u'_{k\pi} \,], \qquad (2.8.)$$

where: - u_k и u'_k is the systematic part of the binary input sequence, while $u_{k\pi}$ и $u'_{k\pi}$ is the parity part.

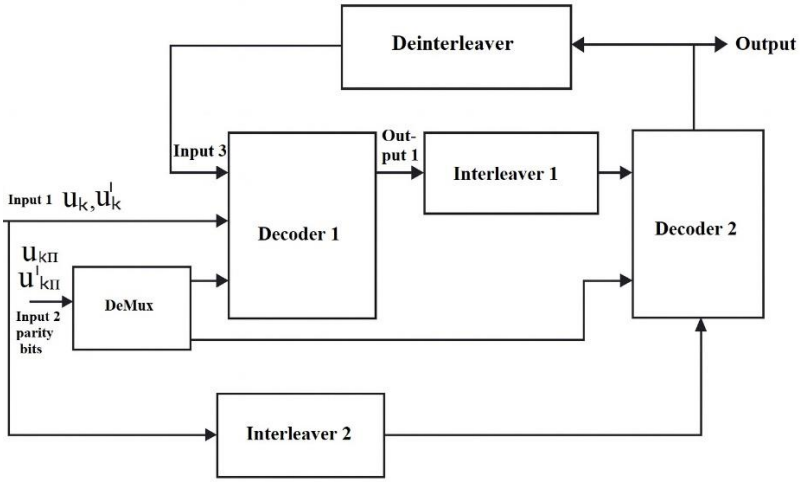


Fig. 2.4. Block Diagram of a Turbo Decoder

The systematic value of the received sequence is applied to the inputs of the first decoder u_k, u'_k and the parity bit stream $u_{k\pi}$ и $u'_{k\pi}$.

After processing the input data, a soft estimate is obtained at the output of the first decoder. This information stream is then applied to interleaving device 1 and subsequently to the second decoder.

At the first input of the second decoder, a reordered sequence of the systematic data stream from the first decoder is applied.u_k and u'_k. At the second input, the parity bits are applied. $m_{k\pi}$ and $m'_{k\pi}$, while at the third input, reordered systematic information from interleaver 2 is applied directly from the input of the turbo decoder.

In the second decoder, the received data are processed and a second soft estimate is obtained. This estimate is applied to the deinterleaver, after which it is fed to the third input of the first decoder. The process is repeated iteratively until a zero probability of error is achieved. At the final stage, threshold processing is applied to the information stream from the soft output of the second decoder in order to make a hard decision based on maximum a posteriori probability.

2.2. General Characteristics of Encryption Algorithms.

The encryption of a given message is a process whereby its content is concealed in a specific manner, resulting in the generation of ciphertext. The reverse process, through which the ciphertext is transformed back into its

original intelligible form, is referred to as decryption. This necessitates the use of both an encryption algorithm and a decryption algorithm.
The processes of encryption and decryption are described by the following expressions:

$$E_K(\mathrm{M}) = \mathrm{C} \quad (2.20.)$$

$$\mathrm{D_K}(\mathrm{C}) = \mathrm{M}, \quad (2.21.)$$

Where:

- M denotes the plaintext message;
- C denotes the encrypted message, or ciphertext;
- E_K denotes the encryption function;
- $\mathrm{D_K}$ denotes the decryption function;
- K denotes the secret key.

Symmetric and asymmetric algorithms for the encryption and decryption of information are known. In symmetric algorithms, the same key is used for both encryption and decryption. The use of a secret key requires the sender and the recipient to possess the corresponding keys in advance and to ensure their protection.
Symmetric algorithms are classified into stream ciphers and block ciphers. Stream ciphers process the plaintext bit by bit, whereas block ciphers process it in groups of bits.
In asymmetric RSA encryption, the sender and the recipient use different keys, namely a public key and a private key. The sender uses the public key in order to identify the recipient and address the message to them. In order to decrypt the message, the recipient uses a private key that is mathematically related to the public key. In this algorithm, the public key serves as an "address", whereas the private key, known only to the recipient, serves as the key for decryption. This ensures that anyone can send messages over an unsecured network, while only the legitimate recipient is able to read them [116, 117].
Figure 2.12 schematically presents the operation of the RSA algorithm.

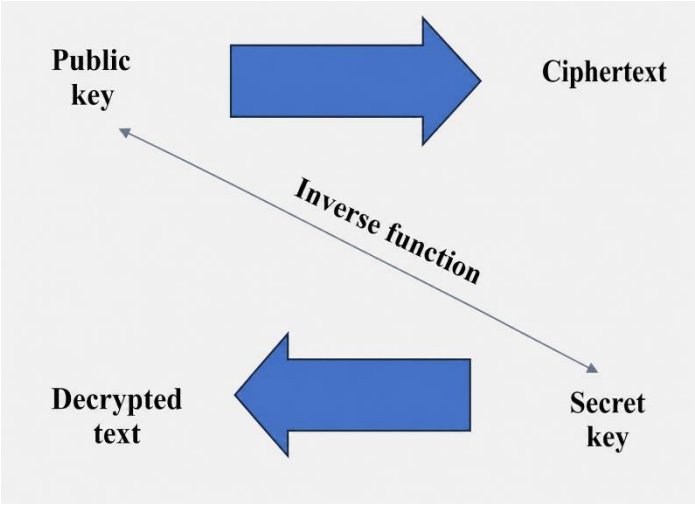


Fig. 2.12. Asymmetric RSA Encryption Algorithm

The asymmetric encryption of text is performed in accordance with the following expression [117]:

$$C \equiv \mathrm{M}^{E_k}(modN), \tag{2.30}$$

where M denotes the message, E_k denotes the encryption function, N denotes the public modulus/public key parameter, and C denotes the ciphertext.

Decryption is carried out on the basis of the following expression [117]:

$$M_d \equiv \mathrm{C}^{\mathrm{d}}(\mathrm{m}odN), \tag{2.31}$$

where C denotes the ciphertext, d denotes the secret key, N denotes the public modulus/public key parameter, and M_d denotes the decrypted message.

The generalized expression describing the RSA encryption algorithm is obtained from expressions (2.30) and (2.31):

$$M_d \equiv (\mathrm{M}^{\mathrm{e}})^{\mathrm{d}}(modN), \tag{2.32}$$

Here, the public key consists of the values e and N, while the value d must be kept secret.

2.3. Cryptographic Coding Systems with Added Interleaving Devices for Increasing the Cryptographic Robustness and Noise Immunity of the Channel.

When protected information is transmitted over an unsecured channel, it is not sufficient for the message merely to be encrypted. The literature review

conducted in Chapter One shows that transmission errors may distort the ciphertext to such an extent that decryption becomes highly inaccurate or practically impossible. For this reason, error-control coding is applied prior to transmission, thereby increasing the probability that the receiver will correctly recover the received bit sequence even in the presence of noise.

According to Abbasi-Moghadam, D., Vakili, V., and Fallahati, A., contemporary symmetric encryption algorithms such as AES are extremely sensitive to errors, since even a single error, after decryption, may lead to an avalanche-like propagation of errors [127]. Therefore, in order to ensure both confidentiality and reliability, encryption must be combined with powerful error-correcting coding. Turbo codes are particularly suitable for this purpose, as they provide error correction close to the theoretical Shannon limit [126]. In order to further increase cryptographic robustness, it is also necessary to combine asymmetric encryption for the transmission of the session keys of the main symmetric encryption algorithm.

2.3.2. Proposed Concept: Interleaving Devices Placed before the Turbo Encoder

The session keys of the symmetric AES algorithm are transmitted by means of the asymmetric RSA algorithm. This implements a combined cryptosystem that integrates the high data-encryption speed of the AES algorithm with the security of asymmetric cryptography for the transmission of secret keys [125]. AES-256 is resistant to quantum attacks, since Grover's algorithm provides only a quadratic speed-up, whereas asymmetric schemes are vulnerable to Shor's algorithm [126, 127, 128]. In the proposed system, asymmetric key exchange is used only for short-lived session keys, which minimises the risk of compromise. The operation of the RSA algorithm is described in Chapter 2, Section 2.2.Figure 2.13 presents a block diagram of the proposed concept.

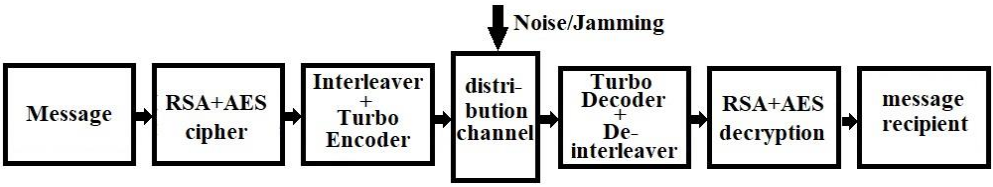


Fig. 2.13. Block Diagram of the Proposed Concept

In the concept developed within the dissertation, one or two interleaving devices are added to the already obtained ciphertext before the turbo encoder. In this way, the ciphertext is not only protected by the main cryptographic algorithm, but its bit positions are subsequently permuted as well.

$$u_s = \pi_2(\pi_1.K_s) = (\pi_2(\pi_1(E_{k_{K_s}}.(M))) \quad (2.33)$$

Subsequently, it is precisely u_s that is fed to the turbo encoder, and after the addition of parity bits by the turbo encoder, the coded sequence u_k is obtained. On the receiving side, turbo decoding D_{k_s} is first performed, followed by inverse reordering of the bits, and only then by decryption D_k, in accordance with the following expression:

$$\mathrm{M} = D_{k_s}(\pi_1{}^{-1}.(\pi_2{}^{-1}(D_{k_{K_s}}.(u_s))) \quad (2.34)$$

In this way, a two-layer protection mechanism is achieved: first, the bits are cryptographically encrypted, and subsequently their positions are additionally concealed by means of one or two interleaving devices.

The bit permutations performed before the turbo encoder are unknown to the eavesdropping party. In this case, malicious actors would have to determine not only the key of the AES algorithm, but also the correct permutation pattern, which increases the difficulty, since the key space expands as a result of the multiplication of the key spaces associated with the two ciphertext representations.

The classical approach protects the content [129], whereas the proposed concept simultaneously protects both the content and the ordering of the already encrypted data. This allows the interleaving device to be regarded as an additional encryption layer applied over the already formed ciphertext.

In addition to increasing cryptographic uncertainty, this preliminary bit permutation also assists the turbo decoder, because local burst errors in the channel are distributed more uniformly instead of being concentrated over a small number of adjacent positions. This reduces the probability that a single admitted error will cause avalanche-like error propagation during the decryption process.

2.3.3. Robustness of Double Encryption and Interleaving against Brute-Force Attacks.

In order to assess more clearly the additional effect on the difficulty of brute-force attacks, an evaluation was carried out of the increase in the key-search space. If the classical hybrid scheme uses an asymmetric algorithm

W_{asym} for protecting the session key and AES-256 for encrypting the payload data, then the overall computational complexity $W_{classic}$ may be expressed as follows:

$$W_{classic} = W_{asym} \cdot 2^{256}, \tag{2.35}$$

where W_{asym} denotes the complexity of compromising the asymmetric algorithm, while 2^{256} represents the key space of AES-256.

If, after AES-256 encryption, one interleaving device is applied to a block of 256 positions, then the number of possible permutations W_π is:

$$W_\pi = 256!,$$

therefore, the overall computational complexity W_1 is:

$$W_1 = W_{asym} \cdot 2^{256} \cdot 256!,$$

from which it follows that:

$$256! = 2^{1684} = 10^{507}$$

This means that, compared with the classical variant, the combinatorial difficulty G_1 associated with the complete exhaustive search of all interleaving variants is calculated by the following expression:

$$G_1 = \frac{W_1}{W_{classic}} = 256! = 10^{507} \tag{2.36}$$

It follows from the expression that the addition of one interleaving device with a length of 256 positions increases the search space by approximately 10^{507} times.

If, instead, two interleaving devices connected in parallel, each with a length of 128 positions, are used, then the number of possible permutations is:

$$W_\pi = 128!$$

$$W_2 = W_{asym} \cdot 2^{128} \cdot (128!)^2,$$

by substitution, the following is obtained:

$$128! = 2^{1432} = 10^{431}.$$

Then, the improvement relative to the classical variant is:

$$G_2 = \frac{W_2}{W_{classic}} = 128! = 10^{431},$$

This result is useful when selecting the system architecture. If the main objective is to achieve the largest possible space of permutations, a single 256-bit interleaving device is more advantageous. However, if the objective is to achieve a more flexible implementation, a shorter interleaving time, and

more convenient structuring of the data stream, two 128-bit interleaving devices also provide an extremely large increase in combinatorial complexity.

Nevertheless, regardless of whether a configuration with one or two interleaving devices is used, the proposed concept significantly increases the size of the key space in comparison with the method of Kovtun and Ivanov, which performs encoding and encryption in a single step and reaches a size of 10^6 [126].

An additional argument in favour of the proposed concept is that, in the publications reviewed, systems based on turbo-based encryption and coding demonstrate improvement not only in terms of security, but also with respect to BER performance. In [127], it is stated that, at BER = 10^{-3}, the use of an AES-256-based generator leads to an improvement of approximately 4 to 4,5 dB compared with some of the approaches under comparison. This confirms that the combined approach is practically justified and is not limited merely to a theoretical increase in the key space.

2.4. Conclusions from Chapter Two

1. At present, a large number of cryptographic algorithms have been developed and practically implemented. Despite the diversity of cryptographic algorithms, all of them are realised through long sequences of simple substitutions and permutations of the symbols of the plaintext.

2. From the perspective of the objectives of the present study, it is appropriate to classify cryptographic algorithms into algorithms in which the amount of information in the plaintext and in the ciphertext is the same, and algorithms in which the amount of information in the ciphertext is greater than the amount of information in the plaintext. Algorithms belonging to the first class apply the principle of "no data expansion", as a result of which they ensure secrecy, or confidentiality, without increasing the rate of information transmission through the communication channel. An example of an algorithm of this class, which is widely used today, is AES.

3. Turbo codes are characterised by the following positive properties. First, they practically approach the so-called Shannon limit, since their energy efficiency is only approximately 0,5 dB below the theoretical limiting value. Second, they employ:

- long sequences of symbol permutations, which can be applied simultaneously both to eliminate the harmful effects of burst errors and to encrypt messages;

- iterative decoding, which is technically relatively simple and was practically implemented as early as the 1960s in NASA space programmes.

4. The addition of one or two interleaving devices before the turbo encoder substantially increases the computational complexity of a brute-force attack, since, in addition to compromising the asymmetric algorithm used for transmitting the secret key and the symmetric encryption key itself, it also becomes necessary to correctly reconstruct the ordering of the interleaved ciphertext. At the same time, interleaving improves the conditions for turbo decoding, because it distributes errors more uniformly and reduces the probability that they will cause avalanche-like accumulation of errors during the decryption process.

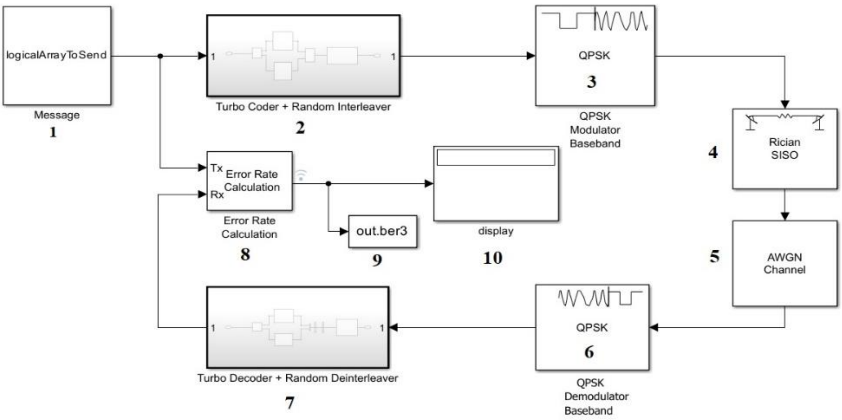
CHAPTER THREE. SYNTHESIS OF AN INFORMATION-PROCESSING MODEL IN A COMMUNICATION SYSTEM ENSURING THE JOINT IMPLEMENTATION OF ERROR-CONTROL CODING AND INFORMATION ENCRYPTION

In the preceding chapter, the technical procedures involved in error-control coding and encryption were analysed, and the similarities and analogies between them were systematised. On this basis, the present chapter addresses the third task of the dissertation.

3.2. Simulation Model of a Communication Channel with the Addition of Interleaving Devices before the Turbo Encoder and Reordering Devices after the Turbo Decoder

The dissertation proposes a model of a communication channel that includes the addition of supplementary interleavers before the standard turbo encoder and deinterleavers after the turbo decoder. The purpose of the proposed modification of the communication channel, from the standpoint of coding, is to improve the distribution of errors, i.e. to disperse occurring clustered bit errors into independent single errors and thereby potentially enhance the error-correction capability of the code. From the standpoint of cryptography, the preliminary interleaving of the information encrypted by means of the RSA algorithm is intended to introduce additional confusion during decryption by malicious actors who have obtained and compromised the secret key. Figure 3.2 presents a generalized block diagram of the proposed communication model with added interleaving devices before the

turbo encoder and reordering devices after the turbo decoder.



Фиг.3.2 Блок-схема на предложен комуникационен модел

3.2.1. Composition of the Proposed Communication Model

1 – input-message entry block, 2 – interleaving devices and turbo encoder, 3 – modulator (BPSK, QPSK, or 16-QAM), 4 – Rice channel, 5 – additive white Gaussian noise channel, 6 – demodulator (BPSK, QPSK, or 16-QAM), 7 – reordering devices and turbo decoder, 8 – error calculator, 9 – block connecting the MATLAB product with the simulation environment (To Workspace), 10 – display for visualising the number of errors.

3.2.2. Principle of Operation

The transmitted message is a sequence of words and digits and is entered into the MATLAB software environment. Encryption is then performed using the RSA algorithm, and the resulting ciphertext, represented as a sequence of zeros and ones, is applied to the input block (Fig. 3.2). The information stream is then subjected to interleaving, which is performed by means of either one interleaving device or two interleaving devices connected in parallel. The two variants for adding interleaving devices before the turbo encoder are shown in Fig. 3.3 and Fig. 3.4, respectively.

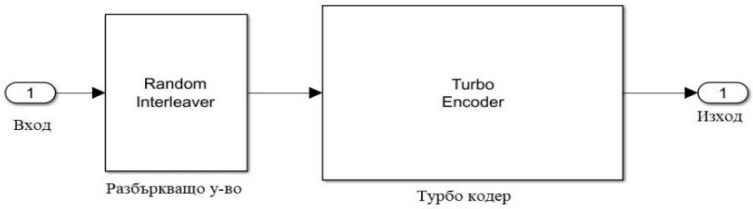


Fig. 3.3. Block Diagram with One Interleaving Device before the Turbo Encoder

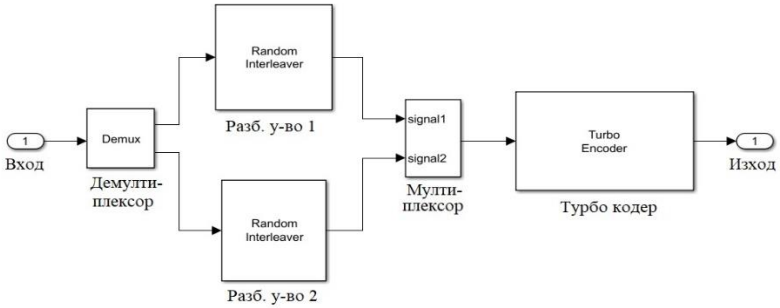


Fig. 3.4. Block Diagram with Two Interleaving Devices before the Turbo Encoder

The information is interleaved in accordance with the Mersenne Twister (MT19937) algorithm and is then applied to the turbo encoder (Fig. 3.2). At this stage, the information is encoded and redundant parity bits for error checking are added. The result is an encrypted and encoded message, which is then fed into a modulation device (depending on the selected modulation scheme), where modulation and transmission of the message are performed. In order to carry out a simulation as close as possible to real operating conditions, the modulated signal passes through a Rice fading channel and a channel for the addition of additive white Gaussian noise (AWGN). The received signal, with the added noise, is then applied to the demodulation device and to the turbo decoder. This is followed by the detection and correction of errors arising during transmission, while the redundant parity bits are removed. The decoded sequence of zeros and ones is then applied to the reordering devices and the turbo decoder (deinterleavers), which restore the original order of the interleaved encrypted message. The variants regarding the number of reordering devices after the turbo decoder are shown in Fig. 3.5 and Fig. 3.6.

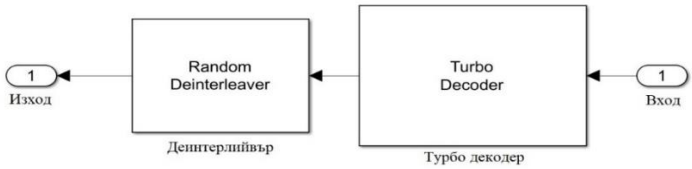


Fig. 3.5. Block Diagram with One Reordering Device after the Turbo Decoder

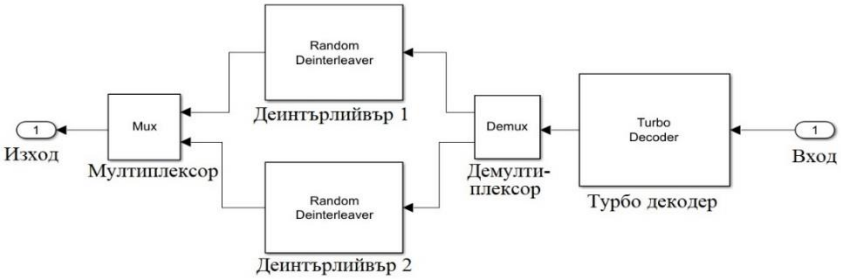


Fig. 3.6. Block Diagram with Two Reordering Devices after the Turbo Decoder

The obtained ciphertext is subjected to an error-calculation procedure, and the result is displayed on a screen. The ciphertext is also transferred to MATLAB for decryption.

The communication channel with added interleaving devices before the turbo encoder and reordering devices after the turbo decoder may be applied for the covert transmission of AES secret keys by means of RSA asymmetric encryption. In drone control, the communication between the operator and the drone is encrypted using the AES algorithm. The proposed structure of the communication channel, incorporating interleaving devices before the turbo encoder and reordering devices after the turbo decoder, may be implemented through the following steps:

The first step is the initiation of the communication session with the drone, which includes the following procedures:

- the ground station generates a random AES session key;
- the generated AES key is encrypted using the RSA algorithm and is accompanied by a public key, which are then transmitted to the drone.

The drone uses its pre-stored RSA private key to decrypt the AES key. The second step involves symmetric encryption of the data stream containing the drone-control commands. This requires:

- both parties to possess the same encrypted AES key;
- encryption of the data using the symmetric AES algorithm.

3.3. Elements of the Composition of the Proposed Communication-Channel Model with the Addition of Interleaving Devices before the Turbo Encoder and Reordering Devices after the Turbo Decoder.

3.3.2. Operation and Parameters of the Interleaving Device before the Turbo Encoder.

The "Random Interleaver" block is an element of the communication components included in the "Communications Toolbox" within the "Simulink" simulation environment of the MATLAB software product. The input signal is represented as a column vector, and the interleaving device rearranges it by using a random permutation. Figure 3.6 presents the control panel from which the parameters of the interleaving device are set.

The "Number of elements" parameter indicates the size of the input vector. The next parameter, "Initial seed", initializes the random-number generator that performs the permutation.

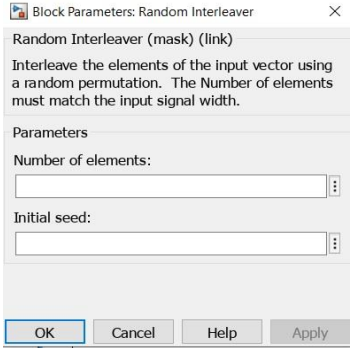


Fig. 3.6. Control Panel for Setting the Parameters of the Interleaving Device

The random-number generator is implemented on the basis of a deterministic algorithm which, starting from an initial state, or "seed", generates a long sequence of pseudorandom numbers. When the same initial state is specified, the same sequence is obtained. The generator operates with an internal state consisting of 624 integers, each having a length of 32 bits, which are subsequently reduced to "0" and "1". The repetition period of a

given combination is sufficiently large, namely ($2^{19937} - 1$ combinations), which makes it practically “infinite”.

The generation of random numbers is performed in accordance with the following expression [110]:

$$X_{k+N_m} = X_{k+O} \oplus X_k D_i, \tag{3.5}$$

where:

X_k are the current values in the state of the generator, represented as 32-bit words;

N_m is the size of the state array;

O – offset within the array;

$\oplus$ – mathematical operation of addition modulo 2;

D_i – matrix with specified dimensions.

3.3.4. Operation and Parameters of the Turbo Encoder

The turbo encoder is implemented by means of two parallel-connected RSC encoders and one interleaving device placed between them. Through the constituent elements of the turbo encoder, redundancy bits are added to the transmitted stream of information symbols. The added bit redundancy enables the correction of errors that occur during information transmission.

In the Simulink simulation environment, the turbo encoder allows various parameters to be configured depending on the purpose of the simulated communication model. The main parameters affecting the operation of the turbo encoder are the generator polynomial, which is specified through the parameter-entry block of the turbo encoder shown in Fig. 3.9. The relevant parameters are the Trellis structure and the length of the input sequence for the interleaver, specified through Interleaver indices.\

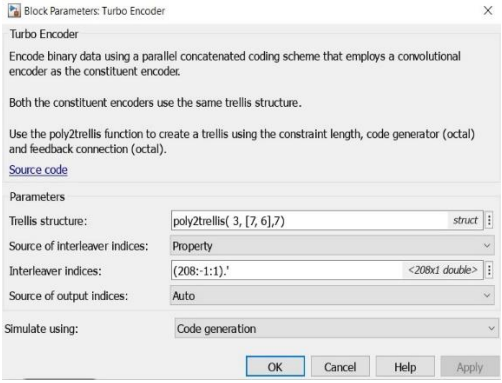


Fig. 3.9. Block for Entering the Parameters of the Turbo Encoder

The trellis structure is formed by the following three elements:

Trellis = poly2trellis (constraint Length, feed forward, feedback),

This are:

- Constraint Length - the length of the code word (k);
- feedforward - a vector of generator polynomials that determine the outputs of the turbo encoder (m_{i1}, m_{i2});
- feedback - a single polynomial used for feedback.

The polynomial defining the operation of the turbo encoder in the Simulink environment is specified in the following form: poly2trellis (3, [7 6], 7).

The digit 3 indicates the constraint length of the code word, while the generator polynomials (m_{i1}, m_{i2}) are represented in octal form as [7,6], it follows that the number of memory elements in the D registers is D e L=k-1=2.

The states of the registers change with each incoming current bit, where x^0, denotes the currently received bit, x^1 denotes a delay of one clock cycle, and x^2 enotes a delay of two clock cycles, and so forth.

The specified values [7,6] of the generator polynomials are given in octal form, since the turbo encoder operates with binary numbers, which are converted as follows:

- 6_8 (6_2 in binary form is: 110) and the first generator polynomial is: $m_{i1} = \mathbf{1}.x^2+\mathbf{1}.x^1+\mathbf{0}.x^0=x^2+x$
- 7_8 (7_2 in binary form is: 111) and the second generator polynomial is: $m_{i2} = \mathbf{1}.x^2+\mathbf{1}.x^1+\mathbf{1}.x^0=x^2+x+1$

Figure 3.10 presents a block diagram of a turbo encoder with parameters specified as poly2trellis(3, [7 6], 7), for which one of the output signals is:

$\boldsymbol{m_i = x^2 + x}$, а вторият е $\boldsymbol{m'_i = x^2 + x + 1}$.

The exponent 2 in (x^2) indicates that the output signal m_i is delayed by two clock cycles before being subjected to modulo-two summation. In this case, the constraint length is k=3, which means that the turbo encoder scheme includes two registers, D_1 и D_2 for first RSC encoder and D'_1 и D'_2 for second RSC encoder. he bit sequence $m_к$ is the input sequence of the system.

The modulo-2 adders form the output sequence indicates that the output signal m_i form the output sequence $u_к = D_1 \oplus D_2$, while the second output sequence $m_{кπ}$ is obtained by summing the current bit with $D_1 \oplus D_2$. The feedback is formed through the modulo-2 addition operation between the bit

delayed by two clock cycles and the current bit. The value specified in the polynomial is 7, which in binary form is 111.

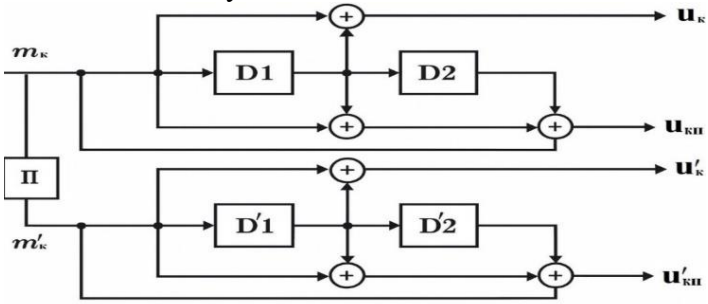


Fig. 3.10. Block Diagram of a Turbo Encoder with Parameters Specified as poly2trellis(3, [7 6], 7)

Systematic convolutional encoders in the coding block make it possible to separate the information bits from the parity bits. Thus, two code blocks are actually transmitted through the communication channel. The first block consists of the information and parity part of the upper RSC encoder in the scheme shown in Fig. 3.10, while the second code block consists of the interleaved information and parity part of the lower RSC encoder.

The interleaved systematic information part $m'_{кп}$ of the second code block is not transmitted through the communication channel, because its recovery in the decoder is performed by means of an interleaving device analogous to the interleaving device used in the encoder.

When the information bits are separated from the parity bits, the information remains explicit, which may allow malicious actors, after accumulating statistical data, to reconstruct the transmitted information.

The proposed scheme with additional interleaving devices before the turbo encoder further complicates the task of unauthorised decryption of the transmitted information.

3.4. Conclusions from Chapter Three

1. Turbo coding significantly increases the reliability of the communication channel, especially when used in conjunction with interleaving devices, since this reduces the probability of consecutive, or burst, errors during data transmission. The use of two interleaving blocks connected in parallel contributes to improving the speed and robustness of

data transmission in a noisy channel, which makes this approach recommended under real communication conditions.

2. In real scenarios, the parameters of the RSA keys and the configuration of the turbo encoder must be carefully selected in order to achieve a balance between security and the efficiency of information transmission.

3. The RSA encryption algorithm is potentially vulnerable, especially when weak random-number generators are used or short keys are applied, which highlights the need for precise selection of the cryptographic parameters.

4. An important practical aspect in configuring the simulation environment is the optimisation of the parameters of the Rice channel and the AWGN channel, in order to realistically model the conditions of signal transmission and noise influence, thereby ensuring results that are as close as possible to the actual operation of communication systems.

CHAPTER FOUR. RESULTS FROM THE CONDUCTED STUDIES OF THE INFORMATION-PROCESSING MODEL IN A COMMUNICATION SYSTEM ENSURING THE JOINT IMPLEMENTATION OF ERROR-CONTROL CODING AND INFORMATION ENCRYPTION.

In the preceding chapter, an information-processing model in a communication system was synthesised, ensuring the joint implementation of error-control coding and information encryption. By addressing the fourth task of the dissertation, the present chapter substantiates the practical applicability of the synthesised model.

4.1. Experimental Setup of the Implemented Simulation Models Using Turbo Coding and Encryption.

The simulation model of a communication channel employing encryption and coding with two interleaving devices connected in parallel is substantiated in Chapter Three, Section 3.2. It was implemented in the Simulink simulation environment of the MATLAB software product, version 2024b. All simulations were conducted on a 64-bit Windows 10 operating system, using the following hardware: “Asus FX502V”, Intel(R) Core(TM) i7-6700HQ CPU at 2.60 GHz, and 24 GB RAM.

The initial parameters set for all simulation configurations are as follows:

- K_{L}-factor: 10;
- Free Space Path Loss: $FSPL = -119{,}97$ dB, calculated from (3.7);
- Distance between the transmitter and the receiver: $d_{\mathrm{r}} = 28$км (calculated using formula 3.8.);
- Path Delay: $Pd = 93{,}33\mu s$ (calculated using formula 3.9);
- Transmitted signal power: $P_{\mathrm{c}} = 1\ W$;
- Receiver sensitivity: -90 dBm (1 nW);
- Code rates: R = 1/2, 1/3, 1/4;
- Modulations: BPSK, QPSK, 16-QAM;
- Length of the transmitted message.: 16 bits;
- Number of transmissions of the message within one simulation: 1 000 000;
- SNR range: 0dB ÷ 30dB, стъпка 0,5dB.

For each investigated code rate (1/2, 1/3, 1/4), 48 generator polynomials were used, fully described in Appendix 6, together with three types of modulation. The results for all 144 configurations for each code rate are presented in Appendices 7, 9, and 11. The best five configurations, in which the optimal signal-to-noise ratio is achieved for each code rate, are compared with a simulation communication model. In this case, only one interleaving device is used, as described in Chapter 3, Section 3.2, while the basic communication model is described in Chapter 3, Section 3.1.

The task of the simulation experiment is to investigate the possibilities for the joint coding and encryption of information transmitted through a simulation communication model, under maximally unfavourable signal-propagation conditions. The objective is to identify the configurations that most effectively combine the procedures of encryption, turbo coding, generator-polynomial specification, and modulation, achieving a minimum signal-to-noise ratio (SNR) for the different code rates.

The obtained results are divided according to the following three criteria:

- For an achieved SNR from 0 to 15 dB and the transmission of 10^6 messages, the results are considered excellent (ER – excellent results) and are subjected to further processing;
- For an SNR in the range from 15 to 30 dB, the results are considered satisfactory (SR – satisfactory results) and are regarded as valid;

- For an SNR above 30 dB, the models are considered unsatisfactory (UR – unsatisfactory results) and are not investigated further in the dissertation.

The obtained results are classified according to the following three criteria:

- For an achieved SNR in the range from 0 to 15 dB and the transmission of 10^6 messages, the results are considered excellent (ER – excellent results) and are subjected to further processing;
- For an SNR in the range from 15 to 30 dB, the results are considered satisfactory (SR – satisfactory results) and are regarded as valid;
- For an SNR above 30 dB, the models are considered unsatisfactory (UR – unsatisfactory results) and are not investigated further in the dissertation.

4.2.4. Generalized Statistical Analysis of the Results Achieved for All 432 Model Configurations with Code Rates of 1/2, 1/3, and 1/4 According to the Following Parameters: Type of Decoding, Type of Modulation, and Signal-to-Noise Ratio.

Generalized Analysis of the Results from the Study of All Models at the Three Specified Code Rates.

From the presented results of the simulation experiment, it follows that the number of configurations meeting the SR criterion is 59 for (R = 1/2), 91 for (R = 1/3), and 61 for (R = 1/4). Their total number is 211 configurations, which corresponds to approximately 49%. The number of models not meeting this criterion is (432 - 211 = 221), i.e. 51% of the configurations. These percentages are illustrated in Fig. 4.8.

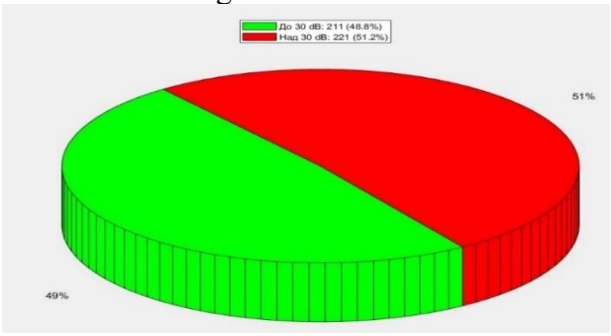


Fig. 4.8. Pie Chart of the Generalized Results for All Investigated Coding Rates

Statistical Analysis of the Results from the Study of Communication Models at Code Rates (R = 1/2, R = 1/3, R = 1/4) (Appendices 7, 9, and 11).

The results obtained for all investigated code rates are as follows (Appendices 7, 9, and 11):

- Minimum SNR = 2 dB;
- Maximum SNR = 30 dB;
- Range = 30 – 2 = 28 dB;
- Mean ≈ 15.27 dB;
- Median ≈ 14–15 dB;
- Standart Deviation (σ) ≈ 6.54 dB.

The listed characteristics are illustrated in a histogram presented in Fig. 4.9. It shows the probability distribution of the acceptable SNR values obtained by combining all 211 satisfactory configurations for the three code rates. The distribution curve indicates that it follows an approximately normal distribution.

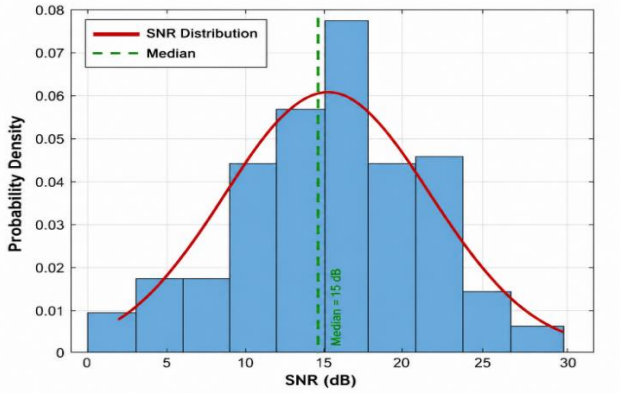


Fig. 4.9. Histogram and Normal Distribution of the Acceptable SNR Values

The obtained SNR values are concentrated in the interval of 14–16 dB, which is consistent with the mean value of 15.27 dB. The median is marked with a green line and has a value of approximately 14–15 dB. The SNR variation range extends from 2 dB to 30 dB, corresponding to a range of 28 dB, while the standard deviation is (\sigma \approx 6.54) dB. This indicates a moderate dispersion of the results, i.e. most values are concentrated in the middle interval, whereas extreme values close to 2 dB and 30 dB occur with lower probability.

4.3 Analysis of the Results Obtained Using the Optimal Configurations with Two Interleavers Compared with Baseline Communication Models without an Interleaver and a Simulation Model with One Interleaver.

Figure 4.15 summarises the results obtained for communication systems without an interleaver, with one interleaver, and with two interleavers at a code rate of (1/2).

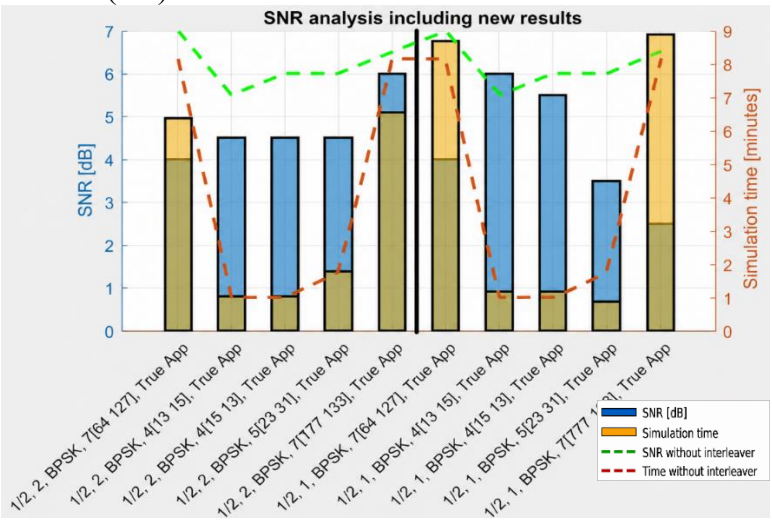


Fig. 4.15. Generalized Results from Communication Systems without an Interleaver, with One Interleaver, and with Two Interleavers at a Code Rate of 1/2

Figure 4.15 presents a graphical comparison of the best configurations at a code rate of (R = 1/2), using BPSK modulation and the True-App decoding algorithm, with two cases being distinguished: configurations with two interleavers (on the left-hand side of the figure) and configurations with one interleaver (on the right-hand side), separated by a vertical black line. The blue bars represent the achieved SNR, whereas the yellow bars indicate the simulation time. The results of the baseline communication channels are depicted by dashed curves. The achieved SNR is marked by a green dashed line, while the simulation duration is marked by an orange dashed line.

For the configurations with one and two interleavers, the results obtained with interleaving (the blue bars) are positioned below the green dashed line, which means that, for the same criterion, a lower SNR is required

in comparison with the models without interleaving. This indicates that the error-correction properties are improved when one or two interleavers are used relative to the baseline model, with the difference being in the range of 0.5–1 dB.

Results Obtained from Models without an Interleaving Device and with a Code Rate of (1/3).

Figure 4.19 illustrates the generalized results obtained for configurations at a code rate of (R = 1/3). On the left-hand side, the achieved SNR values and simulation times for models with two interleavers are presented, while on the right-hand side those for models with one interleaver are shown, the two cases being separated by a vertical black line. For comparison, dashed curves are included: a green one for SNR and an orange one for the simulation time of the baseline models without an interleaver. The blue bars in the graph are positioned below the green dashed line, which indicates the requirement for a lower SNR in the transmission of the specified data. An SNR of approximately 1.5 dB is achieved in the variant with one interleaver, BPSK modulation, and polynomial 7[171 177 133]. In the case of two interleavers, the lowest SNR, approximately 2 dB, is obtained with BPSK modulation and polynomial 5[23 31 25]. The performance of the configuration with two interleavers is only marginally inferior in terms of the achieved SNR compared with the model employing one interleaver; however, the simulation time is reduced significantly.

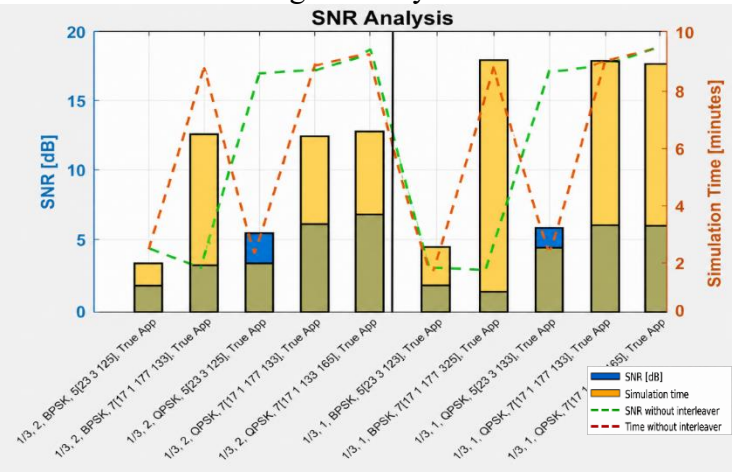


Fig. 4.19. Generalized Results from Communication Systems without an Interleaver, with One Interleaver, and with Two Interleavers at a Code Rate of 1/3

Results Obtained from Communication Models without an Interleaving Device and with a Code Rate of (1/4).

Figure 4.23 presents the generalized results from the comparison of communication models at a code rate of (R = 1/4) without an interleaver and those employing one and two interleavers. The blue bars indicate the SNR [dB], the yellow bars represent the simulation time, while the green and orange dashed lines serve as reference values, indicating, respectively, the SNR and the simulation duration of the baseline models without an interleaver. The two halves of the histogram are separated by a vertical black line, with the configurations employing two interleavers shown on the left-hand side and those employing one interleaver shown on the right-hand side.

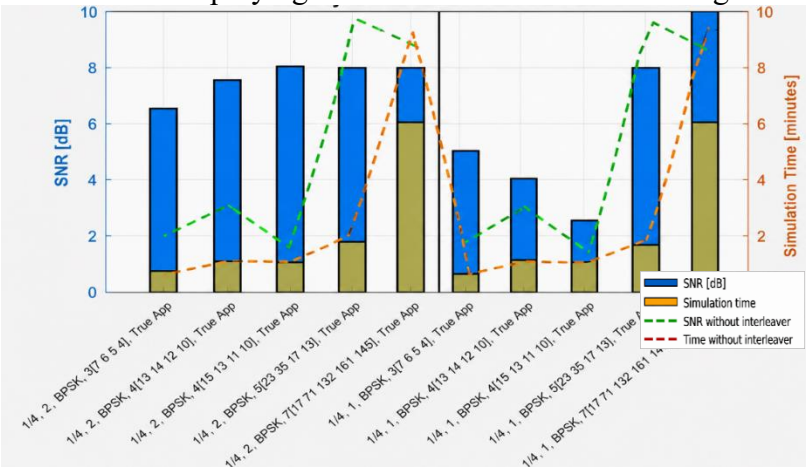


Fig. 4.23. Generalized Results from Communication Systems without an Interleaver, with One Interleaver, and with Two Interleavers at a Code Rate of 1/4

At a code rate of (R = 1/4), the best signal-to-noise ratio is achieved without an interleaver, in the range of 2 to 3 dB. In the models with one interleaver, the SNR deteriorates compared with the models without an interleaver. The configurations employing two interleavers require a higher SNR, ranging from 6.5 to 8 dB, in order to transmit the specified number of messages without error.

4.4. Generalized Analysis of the Configurations with Different Numbers of Interleaving Devices, Generator Polynomials, Constraint Lengths, Code Rates, and Simulation Durations.

Table 4.18 presents the generalized results obtained at a code rate of (R = 1/2) for communication models with one and two interleaving devices, compared with models without interleaving devices. At R = 1/2, a compromise solution between SNR and simulation time is achieved in the configuration with BPSK modulation, generator polynomial (5[23 31]), and one interleaving device.

Table 4.18

Configuration (modulation, generator polynomial)	Code Rate R	Number of inter-leaver divices	SNR [dB]	SNR relative to the configuration without an interleaving device [dB]	Transmi ssion time [min]]	Time relative to the model without interleaving devices [%]
BPSK, 4 [1315]	1/2	0	5,5	-	01:00	-
BPSK, 4 [1315]	1/2	1	6	+0,5	01:11	+18,3%
BPSK, 4 [1315]	1/2	2	4	-1,5	01:02	+3,3%
BPSK, 4 [1513]	1/2	0	6	-	01:00	-
BPSK, 4 [1513]	1/2	1	5,5	-0,5	01:11	+18,3%
BPSK, 4 [1513]	1/2	2	4,5	-1,5	01:02	+3,3%
BPSK, 5 [2331]	1/2	0	6	-	01:45	-
BPSK, 5 [2331]	1/2	1	3,5	-2,5	00:54	-48,6%
BPSK, 5 [2331]	1/2	2	4,5	-1,5	01:47	+1,9%
BPSK, 7 [171 133]	1/2	0	6,5	-	08:10	-
BPSK, 7 [171 133]	1/2	1	2,5	-4	08:54	+9%
BPSK, 7 [171 133]	1/2	2	5,5	-1	06:33	-19,8%
BPSK, 7 [64127]	1/2	0	7	-	08:09	-
BPSK, 7 [64127]	1/2	1	4	-3	08:42	+6,7%
BPSK, 7 [64127]	1/2	2	4	-3	06:23	-21,7%

Relative to the model without an interleaving device for the same polynomial, the SNR is improved, decreasing from 6 dB to 3.5 dB, corresponding to an improvement of -2.5 dB. In the models with one and two interleavers, BPSK modulation, and generator polynomial (7[64 127]), an improvement in SNR is observed relative to the model without an interleaving

device, expressed as a decrease from 7 dB to 4 dB, corresponding to an improvement of -3.0 dB. In the model with one interleaving device, BPSK modulation, and generator polynomial (7[171 133]), an improvement in SNR is achieved relative to the model without an interleaving device, decreasing from 6.5 dB to 2.5 dB, corresponding to an improvement of -4.0 dB. This represents a compromise variant for achieving a lower SNR in more complex models, but with a longer simulation duration.

Table 4.19 analyses the results obtained from configurations without, with one, and with two interleaving devices at a code rate of (R = 1/3), using BPSK and QPSK modulations and different generator polynomials. The SNR, simulation duration, and differences in the achieved values relative to the baseline model without an interleaving device are reported. At a code rate of (R = 1/3), the greatest improvement according to the minimum SNR criterion relative to the model without an interleaving device is achieved by the configuration using QPSK modulation and generator polynomial (5[23 31 25]). In the model with one interleaving device, the SNR improves, relative to the same configuration without an interleaver, from 17 dB to 6 dB, corresponding to an improvement of -11 dB. In the model with two interleaving devices, the SNR reaches 5.5 dB, with an improvement of -11.5 dB relative to the model without an interleaver.

Table 4.19

Configuration (modulation, generator polynomial)	Code Rate R	Number of inter-leaver divices	SNR [dB]	SNR relative to the configuration without an interleaving device [dB]	Transmission time [min]]	Time relative to the model without interleaving devices [%]
BPSK, 5 [23 31 25]	1/3	0	4,5	-	02:05	-
BPSK, 5 [23 31 25]	1/3	1	2	-2,5	02:20	+12%
BPSK, 5 [23 31 25]	1/3	2	2	-2,5	01:45	-16%
BPSK, 7 [171 177 133]	1/3	0	3	-	08:48	-
BPSK, 7 [171 177 133]	1/3	1	1,5	-1,5	08:54	+1,1%
BPSK, 7 [171 177 133]	1/3	2	3,5	+0,5	06:19	-28,2%
QPSK, 5 [23 31 25]	1/3	0	17	-	02:12	-
QPSK, 5 [23 31 25]	1/3	1	6	-11	02:17	+3,8%

QPSK, 5 [23 31 25]	1/3	2	5,5	-11,5	01:40	-24,2%
QPSK, 7 [171 133 165]	1/3	0	19	-	09:08	-
QPSK, 7 [171 133 165]	1/3	1	6	-13	08:52	-2,9%
QPSK, 7 [171 133 165]	1/3	2	6,5	-12,5	06:22	-30,3%
QPSK, 7 [171 177 133]	1/3	0	17	-	09:01	-
QPSK, 7 [171 177 133]	1/3	1	6	-11	08:51	-1,8%
QPSK, 7 [171 177 133]	1/3	2	6	-11	06:14	-30,9%

In the configuration using BPSK modulation, polynomial (7[171 177 133]), and one interleaving device, a lower SNR value is achieved compared with the model without interleaving. The results show that the SNR decreases from 3 dB to 1.5 dB, corresponding to an improvement of -1.5 dB.

In the model with two interleaving devices, the opposite dependence is observed: the SNR deteriorates from 3 dB to 3.5 dB, corresponding to a deterioration of +0.5 dB.

Table 4.20 presents the generalized results at a code rate of (R = 1/4), with BPSK modulation and different generator polynomials, comparing the three simulation models: without an interleaving device, with one interleaving device, and with two interleaving devices. The SNR values, simulation time, and their variations relative to the baseline model without interleaving devices are presented.

At a code rate of (R = 1/4), for the configuration with BPSK modulation and polynomial (4[15 13 11 10]), the lowest SNR is achieved by the model without an interleaving device: (SNR = 1.5) dB. The model with one interleaving device deteriorates the SNR relative to the model without interleaving, increasing it from 1.5 dB to 2.5 dB, corresponding to a deterioration of +1.0 dB.

With two interleaving devices, the SNR deteriorates relative to the model without interleaving, reaching 8 dB, which corresponds to a deterioration of +6.5 dB, although the duration of data transmission is reduced.

For the configuration with BPSK modulation and generator polynomial (3[7 6 5 4]), the model without interleaving is optimal both in terms of SNR and simulation duration. In the model with one interleaving device, the SNR deteriorates to 5 dB, corresponding to a deterioration of +3.0 dB.

Table 4.20

Configuration (modulation, generator polynomial)	Code Rate R	Number of inter-leaver divices	SNR [dB]	SNR relative to the configuration without an interleaving device [dB]	Transmission time [min]]	Time relative to the model without interleaving devices [%]
BPSK, 3 [7 6 5 4]	1/4	0	2	-	00:41	-
BPSK, 3 [7 6 5 4]	1/4	1	5	+3	00:47	+14,6%
BPSK, 3 [7 6 5 4]	1/4	2	6,5	+4,5	00:48	+17,1%
BPSK, 4 [13 14 12 10]	1/4	0	3	-	01:13	-
BPSK, 4 [13 14 12 10]	1/4	1	4	+1	01:22	+12,3%
BPSK, 4 [13 14 12 10]	1/4	2	7,5	+4,5	01:09	-5,5%
BPSK, 4 [15 13 11 10]	1/4	0	1,5	-	01:13	-
BPSK, 4 [15 13 11 10]	1/4	1	2,5	+1	01:22	+12,3%
BPSK, 4 [15 13 11 10]	1/4	2	8	+6,5	01:09	-5,5%
BPSK, 5 [23 35 17 13]	1/4	0	9	-	02:14	-
BPSK, 5 [23 35 17 13]	1/4	1	8	-1	01:52	-16,4%
BPSK, 5 [23 35 17 13]	1/4	2	8	-1	01:53	-15,7%
BPSK, 7 [171 132 161 145]	1/4	0	8	-	9:37	-
BPSK, 7 [171 132 161 145]	1/4	1	9	+1	06:43	-30,2%
BPSK, 7 [171 132 161 145]	1/4	2	8	0	06:44	-30%

In the configuration with two interleaving devices, the SNR reaches a value of 6.5 dB, corresponding to a deterioration of +4.5 dB compared with the baseline model.

An exception is the configuration with a code rate of (R = 1/4), BPSK modulation, and polynomial (5[23 35 17 13]), in which the addition of interleaving devices improves the results simultaneously according to both criteria relative to the model without an interleaving device. The SNR decreases from 9 dB to 8 dB, corresponding to an improvement of -1.0 dB relative to the baseline model.

General Analysis of the Results from Tables 4.21, 4.22, and 4.23.

The analysis shows that the application of a different number of interleaving devices is strongly dependent on the code rate and the specific generator polynomial.

At a code rate of (R = 1/2), a satisfactory balance between the SNR value and the simulation duration is observed in models using BPSK modulation, generator polynomial (5[23 31]), and one interleaving device. Relative to the model without an interleaver, the SNR improves from 6 dB to 3.5 dB.

At a code rate of (R = 1/3), the best SNR relative to the model without an interleaving device is achieved in the configuration with two interleaving devices, QPSK modulation, and polynomial (5[23 31 25]), where the SNR decreases from 17 dB to 5.5 dB.

At a code rate of (R = 1/4), unlike (R = 1/2) and (R = 1/3), the models with one and two interleaving devices deteriorate the SNR. For generator polynomial (4[15 13 11 10]), this is expressed by an SNR of 1.5 dB without an interleaver, whereas in the models with one interleaver the SNR reaches 2.5 dB, and in the models with two interleavers it reaches 8 dB.

When a balance between SNR and minimum data-transmission time is required, a configuration with a code rate of (R = 1/3) and QPSK modulation should be selected. For optimal SNR, configurations of the model with (R = 1/2) and BPSK modulation should be applied. The analysed results indicate that the use of models with a code rate of (R = 1/4) and interleaving devices is not appropriate, due to the deterioration of SNR relative to that achieved by the baseline model.

4.5. Conclusions from Chapter Four.

1. The turbo-encoder models with two preliminary interleavers demonstrate better results than those with one interleaving device, especially at code rates (R = 1/2) and (R = 1/3). In terms of SNR, the improvement relative to the baseline communication models is between 40% and 70%.

2. At a code rate of (R = 1/4), the turbo-encoder models with one preliminary interleaver achieve SNR values close to those obtained by the configurations with two interleavers.

3. The addition of preliminary interleaving devices in models with a code rate of (R = 1/4) is not appropriate, due to the deterioration of the SNR relative to the baseline communication models.

GENERAL CONCLUSIONS

During the COVID-19 period (2019–2022), new and higher requirements emerged for digital services as a result of the remote mode of work and education.

The outbreak of two major military conflicts, still ongoing to date, has indisputably demonstrated the role of technologically advanced weapons, radar and satellite systems, reconnaissance and targeting devices, which have led to entirely new tactics on the battlefield. These tactics require unconditional communication and information connectivity through noise-resistant and encrypted communication channels, ranging from the individual level to the command level. These and other factors necessitate an in-depth study of communication channels providing error-resistant and covert data transmission.

Channel coding is an essential stage in contemporary wireless communications. It is performed by adding redundant bits, thereby minimising errors in the transmission of digital data in a highly noisy communication environment.

Information encryption is imperative, since personal and corporate security is under constant threat of compromise due to the increasing frequency of cyberattacks.

The aim of the dissertation is to investigate the possibilities for combining error-control coding and encryption in order to ensure an optimal signal-to-noise ratio and the concealment of the transmitted data.

The first chapter reviews and analyses scientific publications concerning current trends in information encryption algorithms, as well as the

results achieved in communication systems employing error-correcting coding.

The second chapter provides a detailed description of the mathematical model underlying the operation of the coding and encryption algorithms used in the study. It also proposes a concept for the hybrid application of symmetric and asymmetric cryptographic algorithms to secure data transmitted over an unprotected communication channel.

The third chapter is devoted to the synthesis of an information processing model for a communication system that ensures the joint implementation of error-correcting coding and information encryption.

The fourth chapter presents a mathematical and statistical analysis of the results obtained from the conducted research on the proposed information processing model in a communication system ensuring the combined application of error-correcting coding and information encryption.

A total of 432 communication system configurations were investigated, including 48 generator polynomials, 4 codeword lengths, 3 code rates, and 3 signal modulation schemes. Fifty percent of the examined configurations satisfy the criterion of SNR = 30 dB, while 28% meet the criterion of SNR = 15 dB. The best results obtained fall within the range of 2 to 15 dB.

For communication configurations with a code rate of 1/4, the results show that the inclusion of interleaving devices degrades the signal-to-noise ratio and therefore does not constitute an effective practical approach.

The best results achieved with two parallel-connected interleaving devices incorporated into the communication model were compared with those obtained from models using a single interleaving device and from a baseline communication model. The results indicate that, for code rates of 1/2 and 1/3, the communication models with two interleaving devices achieve values close to those obtained with a single interleaving device, while both approaches provide an additional degree of information concealment.

The introduction of the asymmetric RSA method for encrypting the session keys of the primary AES-based encryption algorithm does not affect the operation of the turbo decoder in the reception and correction of erroneous bits, nor does it degrade the signal-to-noise ratio. **Therefore, the objective of the dissertation has been achieved, namely, to develop error-correcting coding algorithms that ensure both a maximal signal-to-noise**

ratio and a high level of cryptographic protection of transmitted data through the unified integration of different stages in the information processing chain of communication systems.

APPLIED RESULTS:

1. An approach has been developed for noise-resistant communication encryption through the combined use of RSA and AES algorithms (§2.3).

SCIENTIFIC AND APPLIED CONTRIBUTIONS:

1. The information-processing operations in the specialised communication systems used by the Bulgarian Army, the police, and in the protection of the population against disasters and emergencies have been analysed and systematised (§1.1);

2. The known technologies for the joint application of error-control coding and encryption have been analysed (§1.2);

3. An information-processing model has been synthesised in a communication system, ensuring the joint implementation of error-control coding and information encryption (§3.2).

APPLIED CONTRIBUTIONS:

The following algorithms have been synthesised and implemented in the MATLAB environment:

4. Algorithm for generating keys for asymmetric RSA encryption (§2.2);

5. Algorithm for generating keys for symmetric AES encryption (§2.2);

Models of the following have been synthesised and developed in the Simulink environment:

6. Simulation model of a baseline communication channel without interleaving devices. (§3.1) ;

7. Simulation model of a communication channel with one or two interleaving devices added before the turbo encoder and reordering devices after the turbo decoder. (§3.2);

The specified models and algorithms may be used as a tool for the design and evaluation of secure communication systems.

8. By means of simulation modelling, it has been demonstrated that the combined use of the RSA and AES algorithms, in conjunction with error-control coding, is applicable to resource-constrained systems such as UAVs, IoT devices, or other devices with embedded communication modules (§4.4).

LIST OF PUBLICATIONS RELATED TO THE DISSERTATION

1. Stoyanov, D., Bochev, L., Radev, Iv., Parvanov, St., “Approaches to Enhancing Cybersecurity in the Management of Energy Infrastructure”, Ruse: Proceedings of the University of Ruse – 2021, Vol. 60, Issue 3.3, pp. 182–193, FRI-ONLINE-1-CCT2-08, ISSN 2603-4123;

2. Iliev, M., Bedzhev, B., Stoyanov, D., Parvanov, St., “Technologies for Increasing the Resilience of Smart Grids to Spoofing Attacks”, Ruse: Proceedings of the University of Ruse – 2021, Vol. 60, Issue 3.3, pp. 138–144, FRI-ONLINE-1-CCT2-02, ISSN 2603-4123;

3. Georgiev, G., Parvanov, St., Kozarev, K., “Techniques for Protecting Critical Sites against Unmanned Aerial Vehicles”, Ruse: Proceedings of the University of Ruse – 2022, Vol. 61, Session 3.2, pp. 207–216, 2G.302-2-CCT2-10, ISSN 1311-3331;

4. Marinov, D., Nedelchev, M., Stoyanov, D., Parvanov, St., “An Approach to Establishing Secure Communication by Means of Complementary Signals”, Ruse: Proceedings of the University of Ruse – 2022, Vol. 61, Session 3.2, pp. 153–160, 2G.302-2-CCT2-01, ISSN 1311-3321;

5. Parvanov, St., Dimov, D., Radev, Iv., “Investigation of Different Types of Turbo-Code Decoding Algorithms and Their Joint Use with an Encryption Block”, Proceedings of the International Scientific Conference “Defence Technologies” — DefTech 2022, Faculty of Artillery, Air Defence and CIS, Shumen, pp. 407–413, ISSN 2367-7902.