ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ
Факултет по телекомуникации
Катедра „Комуникационни мрежи”

маг. инж. Димитрия Ангелова Михайлова

МЕТОДИ И АЛГОРИТМИ ЗА СИГУРНИ КОМУНИКАЦИИ НА ФИЗИЧЕСКО НИВО В БЕЗЖИЧНИ ТЕЛЕКОМУНИКАЦИОННИ МРЕЖИ

А В Т О Р Е Ф Е Р А Т

на дисертация за придобиване на образователна и научна степен
"ДОКТОР"

Област: 5. Технически науки

Професионално направление: 5.3. Комуникационна и компютърна техника

Научна специалност: Комуникационни мрежи и системи

Научни ръководители:
проф. д-р Георги Любенов Илиев
доц. д-р Златка Вълкова-Джарвис

Рецензенти:
доц. д-р Камелия Симеонова Николова
доц. д-р Габриела Лъчезарова Атанасова

СОФИЯ, 2019 г.

Дисертационният труд е обсъден и насочен за защита от Катедрения съвет на катедра „Комуникационни мрежи“ към Факултет по телекомуникации на ТУ-София на редовно заседание, проведено на 04.02.2019 г.

Публичната защита на дисертационния труд ще се състои на 20.05.2019 г. от 15,00 часа в Конферентната зала на БИЦ на Технически университет – София на открито заседание на научното жури, определено със заповед № ОЖ-5.3-05 / 13.02.2019 г. на Ректора на ТУ-София в състав:

1. доц. д-р Камелия Симеонова Николова – председател
2. проф. д-р Георги Любенов Илиев – научен секретар
3. проф. д-р Розалина Стефанова Димова
4. доц. д-р Иван Стефанов Узунов
5. доц. д-р Габриела Лъчезарова Атанасова

Рецензенти:

1. доц. д-р Камелия Симеонова Николова
2. доц. д-р Габриела Лъчезарова Атанасова

Материалите по защитата са на разположение на интересуващите се в канцеларията на Факултет по телекомуникации на ТУ-София, блок № 1, кабинет № 1254.

Дисертантът е редовен докторант към катедра „Комуникационни мрежи“ на Факултет по телекомуникации. Изследванията по дисертационната разработка са направени от автора, като някои от тях са подкрепени от научноизследователски проекти.

Автор: маг. инж. Димитрия Ангелова Михайлова

Заглавие: Методи и алгоритми за сигурни комуникации на физическо ниво в безжични телекомуникационни мрежи

Тираж: 30 броя

Отпечатано в ИПК на Технически университет – София

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

Фундаментален въпрос в съвременните безжични телекомуникационни мрежи е свързан с установяването на сигурност на предоставяните услуги. Механизмите и протоколите за сигурност, използвани на горните слоеве от архитектурния модел на мрежата, зависят от конкретните приложения и са идентични за кабелните и безжичните мрежи. В зависимост от типа на мрежата, долните два слоя – канален и физически, които определят характеристиките като среда на предаване, модулация и кодиране и отговарят за разпределение на системните ресурси и корекция на грешки от предаването, се различават. Именно поради тази причина, в безжичните мрежи се наблюдават нови предизвикателства като атаки и уязвимости, свързани със сигурността.

С бързото развитие на безжичните комуникации и появата на нови типове мрежи се наблюдават нови изисквания за високи скорости на предаване, обхват на големи разстояния, динамично променяща се среда и директна комуникация между устройствата. Появява се необходимостта от разработване на технологии за достъп до комуникационната среда, която може и да е децентрализирана, на голям брой устройства с различни инфраструктурни изисквания, хардуерни и софтуерни ограничения. Традиционните механизми за постигане на сигурност не са разработени, за да покрият високите критерии на такъв тип мрежи съобразно ограниченията, което поставя под съмнение възможностите им за реализация и ефективна работа в нововъзникващите комуникационни системи.

Това налага разработването на нови методи и алгоритми за сигурност на комуникациите в безжични мрежи, приложими в системи с ограничени ресурси. В последното десетилетие, обект на засилен научноизследователски интерес са похватите, изследващи сигурността на физическия слой. Въпреки множеството предимства на методите за сигурност на физическия слой, съществуват и редица предизвикателства и проблеми, които трябва да бъдат решени за широкомащабното и функционалното им приложение в съвременните комуникационни системи.

Настоящият дисертационен труд е посветен на изследване и подобряване на съществуващите методи за предоставяне на сигурност в безжични мрежи чрез използване на средства и подходи, заложени на физическия слой.

Цел на дисертационния труд, основни задачи и методи за изследване

Основната цел на настоящия дисертационен труд е ***да се подобри сигурността на съвременните безжични комуникационни системи чрез оптимизиране и разработване на методи, техники и алгоритми за сигурни комуникации на физическо ниво с ниска изчислителна сложност.***

За постигане на тази цел е необходимо да се решат следните задачи:

1. Сравнителен критичен анализ на методи и алгоритми за сигурни комуникации в безжични телекомуникационни мрежи.

2. Анализ на методите за откриване на атаката „пилотно замърсяване“ и разработване на техника за усъвършенстване на съществуващ метод.

3. Разработване и предлагане на нов ефективен метод за откриване на атаката „пилотно замърсяване“.

4. Определяне на условията, осигуряващи оптимална работа на новопредложения метод за откриване на атаката „пилотно замърсяване“.

5. Анализ на методите за потискане на ефекта от атака на заглушаване и предлагане на нов адаптивен метод с ниска изчислителна сложност.

Методологията на изследване в дисертацията включва използването на аналитични и симулационни подходи. Разработени са нов метод за откриване на атаката „пилотно замърсяване“ и техника за подобряване на работата на един от съществуващите методи. Методът и техниката се основават на анализ на N-PSK диаграмата на състоянията. Предложен е и метод за намаляване на ефекта от атака на заглушаване чрез адаптивна филтрация на смущаващия сигнал в приемника посредством LMS алгоритъма. За да се оцени ефективността на предложените в дисертационния труд методи, техники и алгоритми чрез експериментални изследвания, е използван програмния продукт Matlab.

Научна новост

Научната новост в настоящия дисертационен труд е свързана с предлагането на нови методи, техники и алгоритми за подобряване на сигурността на физическо ниво в безжични телекомуникационни мрежи. Анализът на съществуващите методи за противодействие на основните видове атаки, използвани срещу сигурността на физическия слой, се извършва, за да се установят сценариите на атаки, които са неоткриваеми от методите, и необходимостта от тяхната оптимизация. В дисертацията са разработени техника за усъвършенстване на един от методите за откриване на атаката „пилотно замърсяване“, както и нов метод, способен да открие всички възможни типове PCA. Формулирани са условията за оптимална работа на новопредложения метод и е разработен алгоритъм за изчисляване на стойностите на отместванията на диаграмата на състоянията, които методът използва по време на тренировъчната фаза за оценка на канала. Предложен е адаптивен метод с ниска изчислителна сложност за противодействие на атака на заглушаване с теснолентови смущения.

Практическа приложимост

По тематиката на дисертационния труд е работено в рамките на два научноизследователски договора: Договор № 172ПД0016-07, тема: „Методи и алгоритми за сигурни комуникации на физическо ниво в безжични телекомуникационни мрежи”; Договор № BG05M2OP001-2.009-0033-C01, тема: „Стимулиране на съвременни научни изследвания чрез създаване на научно-иновативна среда за насърчаване на млади изследователи от ново поколение в Технически университет – София и Национална компания „Железопътна инфраструктура” в областта на инженерно-техническите науки и технологичното развитие”.

Публикации

Основните постижения и резултати от дисертационния труд са представени в общо ***8*** авторски публикации, ***6*** от които на международни конференции и ***2*** в международно научно списание. Една от публикациите е самостоятелна, а останалите 7 са в съавторство. Международни конференции са: *First International Balkan Conference on Communications and Networking (BalkanCom) 2017, 21st International Conference on Circuits, Systems, Communications and Computers (CSCC) 2017, Global Wireless Summit (GWS) 2017, Advances in Wireless and Optical Communications (RTUWO) 2017, 4th EAI International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures (Fabulous), 2019, Wireless*

Telecommunications Symposium (WTS) 2019. Международните научни списания са: *WSEAS Transactions on Communications 2017, World Academy of Science, Engineering and Technology, International Journal of Computer and Information Technology (IJCIT), 2018*.

Структура и обем на дисертационния труд

Дисертационният труд е в обем от *159* страници, като включва увод, *4* глави за решаване на формулираните основни задачи, списък на основните приноси, списък на публикациите по дисертацията и използвана литература. Цитирани са общо *182* литературни източници, като всички са на латиница и един от тях е интернет адрес. Работата включва общо *44* фигури и *32* таблици. Номерата на фигурите и таблиците в автореферата съответстват на тези в дисертационния труд.

II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

ГЛАВА 1. Критичен анализ на методи и алгоритми за сигурни комуникации в безжични телекомуникационни мрежи

1.1. Сигурност в съвременните безжични комуникационни системи

Сигурност в мобилните мрежи от пето поколение

С нарастването на необходимостта от все по-високи скорости на предаване на данните в безжичните комуникационни системи и появата на услуги като Интернет на нещата IoT, M2M, електронно здравеопазване, обучение и банкиране се появява нуждата от нови технологии, които да осигурят по-голям капацитет в сравнение със съществуващите. Съвременните клетъчни мрежи от четвърто поколение - 4G, не са в състояние да поемат очакваното нарастване на мобилния трафик, което налага разработването на пето поколение безжични мрежи – 5G. Някои основни изисквания към 5G включват поддръжката на много високи скорости на предаване и ниска латентност, спектрална и енергийна ефективност, глобално покритие и висока надеждност. Използването на 5G като платформа за предаване на конфиденциална информация в голяма част от бъдещите приложения и услуги формира сигурността като фундаментален въпрос за безжичните мрежи от пето поколение.

Сигурността в съвременните безжични системи основно се базира на криптографски техники и свързаните с тях протоколи, работещи на различните нива от слоестия архитектурен модел на мрежата. Недостатък на тези решения е фактът, че в публичните безжични мрежи те не са достатъчно сигурни, а подобряване на съществуващите протоколи за криптиране и автентикация би довело до сериозни ограничения и допълнителни разходи за потребителите на публичната мрежа. Това налага разработването на нови подходи за сигурни комуникации, базирани на теория на информацията и известни като сигурност на физическия слой – PLS.

Използването на PLS техники в 5G мрежите има две основни предимства пред традиционната криптография. От една страна, PLS не се позовава на изчислителната сложност, благодарение на което може да постигне сигурни и надеждни комуникации дори в присъствието на нелегитимен потребител, разполагащ с устройства с неограничена изчислителна мощност. Не такъв е случаят, когато сигурността на системата е заложена чрез изчислително-базираните криптографски техники и може лесно да бъде

компрометирана, ако неоторизиран потребител разполага с достатъчно капацитет за решаването на сложния математически проблем на криптоалгоритъма. От друга страна, структурата на 5G мрежата обикновено е децентрализирана, което предполага, че устройствата могат по всяко време и на случаен принцип да се свързват към мрежата или да я напускат. Това значително усложнява обмена и управлението на криптографски ключове. Следователно, PLS техниките могат да се използват в 5G като допълнително ниво на защита в съществуващите схеми за сигурност, за обмен на криптографски ключове или самостоятелно за сигурно предаване на данни.

Сигурност в Интернет на нещата

С развитието на IoT се очаква предметите от ежедневието да станат част от една заобикаляща среда, в която милиарди физически устройства, оборудвани с различни видове сензори и задвижващи механизми, са свързани към Интернет чрез хетерогенни мрежи за достъп. Директните комуникации между устройствата, както и тези между устройство и потребител, стават възможни чрез протокола IPv6 и M2M приложенията. Основната идея, заложена в IoT, е едромащабното разгръщане на M2M комуникациите, чрез които става възможно изпълняването на задачи за наблюдение и контрол с минимална човешка намеса.

IoT сензорите и устройствата обикновено се характеризират с компактни размери, които са причина за редуцирани хардуер, памет за съхранение и значителни енергийни ограничения. Тези свойства на устройствата намаляват възможностите им за обработка на сигнали и откриват нови предизвикателства, свързани със сигурността. Големият брой M2M устройства в IoT системите, в съчетание с хетерогенните технологии за радиодостъп и динамично променящата се среда, затрудняват имплементирането на традиционните криптографски протоколи, изискващи обмен на ключове и управление на сертификати.

Следователно, използването на традиционни криптографски техники в IoT мрежите е възпрепятствано от специфичните особености и ограничените ресурси на включените устройства. Ефективно решение за сигурни комуникации в IoT е чрез методи за сигурност на физическия слой, които могат да заменят криптографските протоколи или да се използват като допълнение към някои по-леки криптоалгоритми. PLS техниките използват разликите в условията на канала, за да усилят приетия сигнал при предназначените приемници, като същевременно намалят нивото на сигнала при неоторизирани потребители. Тези методи обикновено не зависят от технологията за радиодостъп и предлагат „вградена“ сигурност, която е непробиваема от гледна точка на теория на информацията.

1.2. Сигурност на физическия слой в безжични мрежи

Изчислителната сложност, характерна за традиционните методи за криптиране на данни, и необходимостта от управление на ключове са предпоставка за засилен научноизследователски интерес към разработването на нови методи за сигурни комуникации, базирани на физическите свойства на радиоканала. Работата на Шенон (Shannon), свързана с математическата теория на комуникациите, поставя основите на сигурността на физическия слой в безжични мрежи. Докато трудът на Шенон е свързан със системи за симетрично криптиране, Уинър (Wyner) първи представя идеята за сигурност на комуникационния канал без използване на споделен таен ключ.

PLS в безжичните мрежи осигурява конфиденциалност чрез механизми, които намаляват възможността потенциален неоторизиран потребител да получи информация за конфиденциалните съобщения. Тези механизми включват имплементирането на техники, използващи характерните за безжичната среда фадинг, интерференция и диверсификация на маршрутите, наблюдаваща се при системите с голям брой антени. Освен това, природата на безжичните канали има случаен характер, който може да бъде използван за

извеждане на споделен таен ключ от физическия слой, позволяващ прилагането на традиционни методи за защита на данните, елиминирайки проблема с обмен на ключове.

1.3. Подходи за сигурност на физическия слой

В съвременните безжични мрежи съществуват няколко широкоразпространени метода за подобряване на сигурността на физическия слой. В зависимост от характерните им свойства, тези методи могат да бъдат класифицирани в пет различни категории:

- сигурност, базирана на теория на информацията;
- сигурност чрез изкуствено добавен шум;
- сигурност чрез използване на устройство, формиращо диаграма за насочено действие;
- техники за сигурност, базирани на диверсификацията;
- генериране на таен ключ посредством характеристиките на физическия слой.

1.4. Атаки, насочени срещу сигурността на физическия слой

Въпреки технологичната гъвкавост, която предоставят безжичните мрежи, откритият характер на безжичната среда дава нови възможности за неоторизиран достъп до системните ресурси и атаки, насочени срещу сигурността, които могат да останат неразкрити.

Безжичните комуникационни системи са уязвими към два основни типа атаки на физическия слой – подслушване (eavesdropping) и заглушаване (jamming). Атаката подслушване се отнася до неоторизиран потребител, който се опитва да прихване данните, предавани между легитимните потребители. Докато подслушващия се намира в зоната на покритие на предавателя, безжичната комуникационна сесия може да бъде прихваната. За да подобри силата и качеството на прихванатия от него сигнал, по време на процеса на идентификация на канала между легитимния приемник и предавателя, подслушващият може да инициира т. нар. атака „пилотно замърсяване“.

Освен това, в безжичните мрежи неоторизиран приемник може лесно да генерира интерференция, за да заглуши комуникацията между легитимните възли, известно още като DoS атака. Целта на тази атака е да се възпрепятства достъпа на потребителите на мрежата до нейните ресурси чрез изпращане на теснолентови смущения.

1.5. Изводи след направения критичен анализ в Първа глава

В резултат от проведения обзор на литературата и научните изследвания, свързани с методи и алгоритми за сигурни комуникации в безжични телекомуникационни мрежи, могат да бъдат направени следните основни изводи:

- На всяко от нивата на слоестия архитектурен модел е заложено да отговаря на конкретни изисквания, свързани със сигурността, като долните два слоя – канален и физически, са най-слабо използвани за изграждане на сигурни комуникации.
- Традиционно използваните криптографски подходи не са в състояние да се справят с атаки, характерни за долните слоеве от референтния модел.
- Архитектурните и технологични особености на нововъзникващите безжични мрежи (като 5G и IoT) налагат нови изисквания към сигурността. Необходимо е разработването и изследването на методи за сигурни комуникации на физическо ниво, които да преодолеят проблемите на криптографията и да бъдат приложими в мрежи с ресурсни ограничения.

- Случайната природа на безжичния канал може да бъде използвана, за да повиши сигурността на системата, разгръщайки пълния потенциал на физическия слой.

- Освен че преодоляват сложността на традиционните криптографски техники, методите за сигурност на физическия слой са непробиваеми от гледна точка на теория на информацията и работят ефективно независимо от мощността и ресурсите, с които разполага злонамереният потребител.

- Срещу сигурността на физическия слой могат да бъдат предприети два основни типа атаки – подслушване и заглушаване.

- Обикновено в съвременните безжични мрежи подслушването се осъществява чрез атаката „пилотно замърсяване“, а заглушаването се реализира чрез сигнал, представляващ теснолентово смущение. Поради възможността атаките на физическия слой да останат неразкрити, е необходимо да се разработят и предложат методи за откриването им и средства за противодействие.

ГЛАВА 2. Подобряване на ефективността на методи за откриване на атаката „пилотно замърсяване“

2.1. Същност на атаката „пилотно замърсяване“

За да подобри условията на собствения си канал с базовата станция с цел подслушване на комуникацията, атакуващият може да се включи в тренировъчната фаза за оценка на канала, която е характерна за системите с дуплекс деление по време. Този тип атаката се нарича „пилотно замърсяване“ и се състои в изпращане на пилотни сигнали от атакуващия по същото време, по което легитимният потребител изпраща своите. В резултат BS оценява погрешно легитимния канал и проектира устройството си за предварително кодиране така, че да предава както по посока на LU, така и по посока на ED. Тъй като наличието на атаката „пилотно замърсяване“ не може да бъде установено от системата, се налага да бъдат предприети допълнителни мерки за нейното откриване.

Във Втора глава е направен сравнителен анализ на четири метода за откриване на PCA, които са се наложили в литературата [A1]. Първите два метода (*2-N-PSK* и *L-N-PSK*) откриват атаката чрез анализ на диаграмата на състоянията, предавайки съответно два или повече легитимни пилотни сигнали. Третият метод (*GLRT*) се базира на анализ на хипотези, а четвъртият (*SKs*) – на потвърждаване на тайни ключове. Методите са сравнени чрез някои техни основни характеристики, които са обобщени в Табл. 2.1, където степента на свързаност на всяка техника с дадените свойства е означена с *L* за ниска и *H* за висока. *N* е използвано, за да означи, че методът няма връзка със съответната характеристика.

	2-N-PSK	*L-N-PSK*	*GLRT*	*SKs*
Зависимост от SNR	*L*	*H*	*H*	*L*
Необходимост от познаване на едромащабния фадинг	*N*	*N*	*H*	*N*
Зависимост от фазов шум	*H*	*H*	*H*	*N*
Зависимост от броя антени	*H*	*H*	*H*	*H*
Необходимост от MaMIMO	*H*	*H*	*N*	*N*

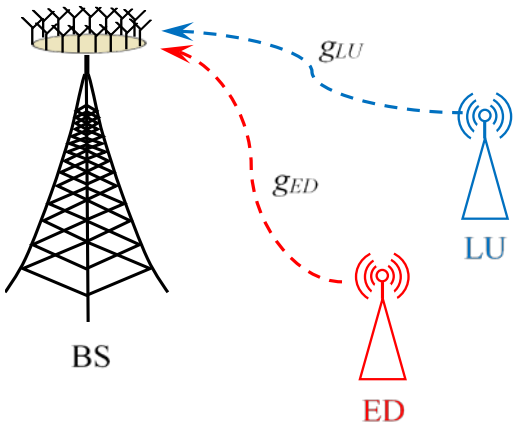
Необходимост от предварително познаване на канала	*N*	*N*	*H*	*N*
Необходимост от промени в системния модел	*H*	*H*	*N*	*H*
Сложност	*L*	*L*	*H*	*H*
Дълъг тренировъчен период	*L*	*L*	*H*	*H*
Увеличаване на заглавната информация	*L*	*L*	*N*	*H*
Устойчивост към вариации в предавателната мощност на ED	*H*	*H*	*H*	*H*
Устойчивост към атаки на заглушаване на сигнала на LU	*H*	*H*	*H*	*N*

Табл. 2.1. Сравнение на разгледаните методи за детекция на атаката „пилотно замърсяване“

Вследствие на сравнението един от методите, наречен накратко *2-N-PSK*, е избран за бъдещи изследвания поради благоприятните му свойства, но сравнително ниски стойности на вероятност за детекция на атаката, които постига.

2.2. Системен модел

Системният модел, състоящ се от една клетка, канали с адитивен бял Гаусов шум и без мобилност на абонатите, изследва ситуацията, изобразена на фиг. 2.1, където базова станция BS с голям брой антени – *M*, комуникира само с един легитимен потребител LU с една антена, докато един подслушващ ED, също с една антена, се опитва да долови информационния обмен.



Фиг. 2.1. Системен модел

Каналът за предаване в обратна посока от LU към BS е означен като g_{LU} и включва влиянието на мощността на предаване на LU - P_{LU}, едромащабния фадинг d_{LU}, и дребномащабния фадинг h_{LU}. По подобен начин, каналът от ED към BS е представен като g_{ED}, където P_{ED} е предавателната мощност на ED, d_{ED} е едромащабният фадинг и h_{ED} е дребномащабният фадинг. Каналите за предаване в обратна посока на LU и ED се изчисляват по израз (2.1):

$$\begin{aligned} g_{LU} &= \sqrt{P_{LU} d_{LU}}\, h_{LU}, \\ g_{ED} &= \sqrt{P_{ED} d_{ED}}\, h_{ED}. \end{aligned} \tag{2.1}$$

2.3. *2-N-PSK* метод за детекция на атаката „пилотно замърсяване“

2-N-PSK методът се състои в изпращане на два легитимни N-PSK пилотни сигнала по време на фазата за оценка на канала. В BS се пресмята корелацията z_{12} на двата приети сигнала според (2.4) и се анализира нейният фазов ъгъл. Ако ъгълът на резултата от корелацията не клони към ъгъл на валиден N-PSK символ, атаката е открита и комуникацията трябва да бъде преустановена. В противен случай, методът решава, че няма активна PCA.

$$\begin{aligned} z_{12} = \frac{1}{M}\Big(\sqrt{P_{LU} d_{LU}}\, h_{LU}\, p_1^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED}\, p_1^{ED}\Big)^H \times \\ \Big(\sqrt{P_{LU} d_{LU}}\, h_{LU}\, p_2^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED}\, p_2^{ED}\Big) + n_{12}, \end{aligned} \tag{2.4}$$

където ${p_1}^{LU}$ и ${p_1}^{ED}$ са сигналите, изпратени съответно от LU и ED по време на първото пилотно предаване, а ${p_2}^{LU}$ и ${p_2}^{ED}$ са сигналите през втория пилотен интервал. Означението $(\cdot)^H$ е за Ермитова матрица, а n_{12} е резултантният шум.

Вследствие провеждането на множество експериментални изследвания със случайни условия, са установени четири основни сценария на атаки, които *2-N-PSK* методът не е в състояние да открие. Описание на съответните сценарии е дадено по-долу, където с $\varphi(\cdot)$ е отбелязан ъгълът на всеки пилот.

Сценарий 1

И двата нелегитимни пилота съвпадат по фаза с легитимните:

$$\varphi\left(p_1^{ED}\right) = \varphi\left(p_1^{LU}\right) \quad \text{и} \quad \varphi\left(p_2^{ED}\right) = \varphi\left(p_2^{LU}\right).$$

Сценарий 2

Един от нелегитимните пилоти е реципрочен, а другият е равен или и двата са реципрочни по фаза на съответните легитимни сигнали:

$$\varphi\left(p_1^{ED}\right) = \varphi\left(p_1^{LU}\right) \quad \text{и} \quad \varphi\left(p_2^{ED}\right) = \varphi\left(p_2^{LU}\right) + 180^\circ.$$

или

$$\varphi\left(p_1^{ED}\right) = \varphi\left(p_1^{LU}\right) + 180^\circ \quad \text{и} \quad \varphi\left(p_2^{ED}\right) = \varphi\left(p_2^{LU}\right).$$

или

$$\varphi\left(p_1^{ED}\right) = \varphi\left(p_1^{LU}\right) + 180^\circ \text{ и } \varphi\left(p_2^{ED}\right) = \varphi\left(p_2^{LU}\right) + 180^\circ.$$

Сценарий 3

Атаката започва по време на второто пилотно предаване и нелегитимният пилот съвпада по фаза със съответния легитимен или неговия реципрочен сигнал:

$p_1^{ED} = 0$ и $\varphi\left(p_2^{ED}\right) = \varphi\left(p_2^{LU}\right)$.

или

$p_1^{ED} = 0$ и $\varphi\left(p_2^{ED}\right) = \varphi\left(p_2^{LU}\right) + 180^{\circ}$.

Сценарий 4

Фазите на двата нелегитимни пилота се различават от тези на съответните им легитимни сигнали с един и същи ъгъл:

$\varphi\left(p_1^{ED}\right) = \varphi\left(p_1^{LU}\right) + \varphi_x(N-PSK)$ и $\varphi\left(p_2^{ED}\right) = \varphi\left(p_2^{LU}\right) + \varphi_x(N-PSK)$.

2.4. Допълнителна техника за подобряване на ефективността на *2-N-PSK* метода

За подобряване на ефективността на *2-N-PSK* метода, във Втора глава е предложена техника, която да се използва като допълнение към оригиналния метод [A2]. Техниката е насочена най-вече към атака от типа на ***Сценарий 3***, инициирана по време на предаването на втория легитимен пилот от двойката, когато ED дублира пилотния сигнал на LU или изпраща неговата реципрочна стойност.

В случай, че фазовият ъгъл на корелацията z_{12} съвпада с ъгъл от N-PSK съзвездието, в BS се изчислява ПФ на канала по време на първото и второто пилотно предаване – g_1 и g_2, съответно. Ако двете ПФ се различават, това говори за евентуална нелегитимна намеса във втория тренировъчен времеинтервал. За да се потвърди, че тази разлика в ПФ не е вследствие на шум, се предава трети легитимен N-PSK пилот. Изчислява се корелацията z_{23} между втория и третия пилот. Ако и нейната фаза съвпада с ъгъл от N-PSK съзвездието, се изчислява ПФ на канала през третото пилотно предаване – g_3. Ако ПФ през второто и третото пилотно предаване е една и съща (g_2=g_3), атаката е потвърдена.

При атака от типа на ***Сценарий 3***, в която нелегитимните пилотни сигнали през втория и третия пилотен интервал съвпадат със съответните легитимни сигнали, приетите в BS сигнали за всяка от трите пилотни сесии – y_1, y_2 и y_3, се изчисляват съгласно (2.10), (2.12) и (2.14). ПФ на канала за първото, второто и третото пилотно предаване се изчислява посредством (2.11), (2.13) и (2.15), съответно.

$$y_1 = p_1^{LU} g_{LU} . \tag{2.10}$$

$$g_1 = g_{LU} = \frac{y_1}{p_1^{LU}}. \tag{2.11}$$

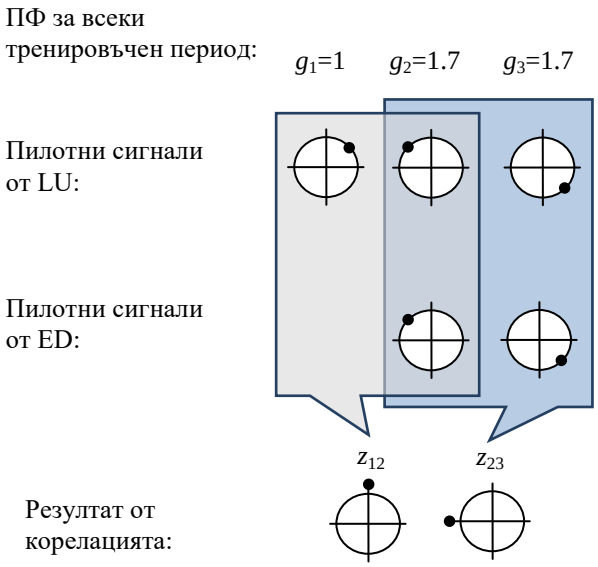
$$y_2 = p_2^{LU} g_{LU} + p_2^{ED} g_{ED} = p_2^{LU}\left(g_{LU} + g_{ED}\right). \tag{2.12}$$

$$g_2 = g_{LU} + g_{ED} = \frac{y_2}{p_2^{LU}}. \tag{2.13}$$

$$y_3 = p_3^{LU} g_{LU} + p_3^{ED} g_{ED} = p_3^{LU}\left(g_{LU} + g_{ED}\right). \tag{2.14}$$

$$g_3 = g_{LU} + g_{ED} = \frac{y_3}{p_3^{LU}}. \tag{2.15}$$

На фиг. 2.9 е представена интерпретация на предложената техника, където заедно с резултатите от корелацията е показано и геометричното представяне на 8-PSK пилотните символи.

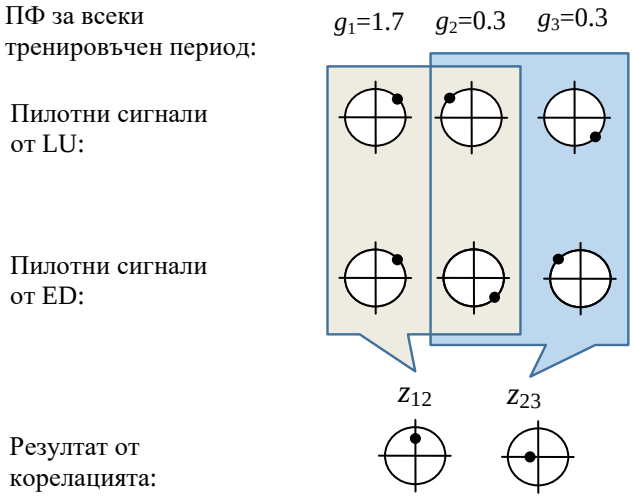


Фиг. 2.9. Примерна интерпретация на предложената техника при атака, инициирана по време на второто пилотно предаване

С цел намаляване на сложността на системата, симулацията е проведена с една антена на BS, каналът е приет за статичен и влиянието на шума е пренебрегнато. Стойността на амплитудите на пилотните сигнали на LU и ED е зададена да бъде единица. За целите на симулацията, каналът между BS и LU е приет да бъде g_{LU} =1, а този между BS и ED – g_{ED} =0.7.

Както може да бъде видяно от примера на фиг. 2.9, когато ED не участва в комуникацията, ПФ, изчислена в BS, е равна на ПФ на легитимния канал. Когато има налична атака, резултантната ПФ се променя и продължава да се появя по време на следващите пилотни сесии. Дори в най-лошия случай, когато пилотите на ED съвпадат с тези на LU и резултатът от корелацията има валиден 8-PSK ъгъл, повторната поява на стойност на ПФ g_2 показва присъствието на нелегитимен потребител.

Предложеното подобрение към *2-N-PSK* метода може да бъде използвано за откриване на атакуващ, чийто първи пилот повтаря този на LU и чиито втори и трети пилотни сигнали са реципрочни на съответните пилоти на LU (***Сценарий 2***). В тази ситуация, фиг. 2.10, атаката не може да бъде открита от оригиналния *2-N-PSK* метод, тъй като аргументът на корелацията съвпада с ъгъл на символ от N-PSK съзвездието.



Фиг. 2.10. Примерна интерпретация на предложената техника при атака, инициирана по време на първото пилотно предаване

Поради значителната разлика в стойностите на ПФ от първото пилотно предаване с тези от второто и третото, *2-N-PSK* методът с предложеното подобрение успешно разкрива присъствието на злонамерения потребител.

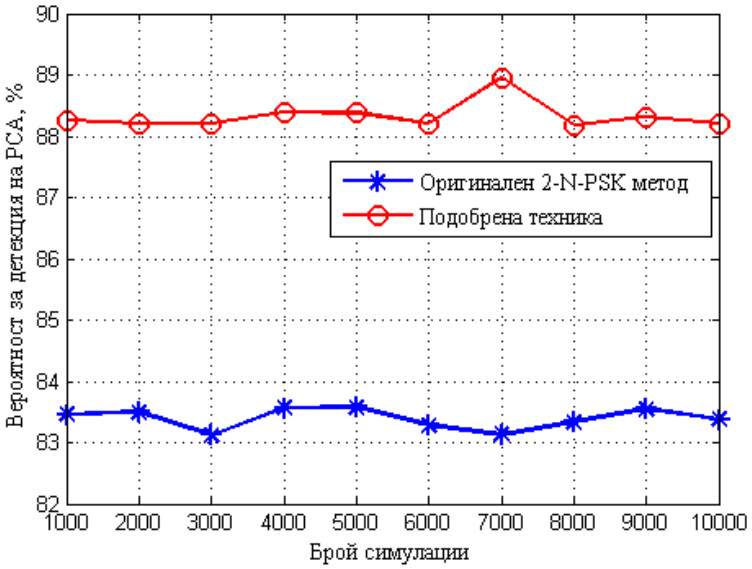
Условията, при които е проведен експериментът от фиг. 2.10, са аналогични на тези от фиг. 2.9, като разликата е само в изпратените от ED пилотни сигнали. Както се вижда от фиг. 2.9, когато нелегитимният потребител изпрати пилотен сигнал със същия аргумент като на LU, ПФ g_1 е сума от ПФ на легитимния и нелегитимния канал. Когато вторият и третият нелегитимни пилотни сигнали са реципрочни на легитимните (фиг. 2.10), g_2 и g_3 представляват разликата от ПФ на легитимния и нелегитимния канал, което е предпоставка за откриване на такъв тип атака от подобрения *2-N-PSK* метод.

Вероятностите за детекция на оригиналния и подобрения метод са анализирани чрез провеждането на голям брой експерименти, разделени в симулационни групи със случайни условия [А3]. За всяка от симулационните групи са проведени по десет независими експеримента. Средните аритметични стойности на резултатите са графично представени на фиг. 2.11.

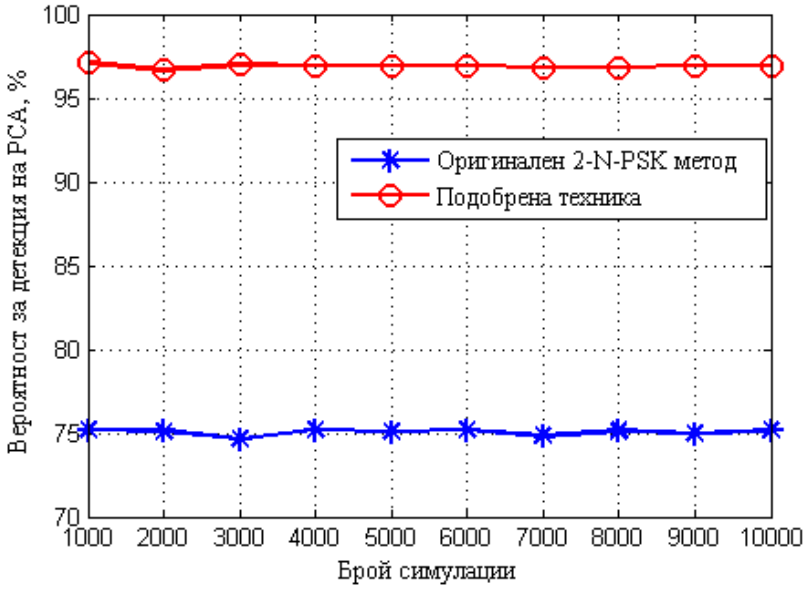
Както може да бъде видяно на фиг. 2.11, средната вероятност за детекция на различните симулационни групи е приблизително константна. При прилагане на предложеното допълнение към *2-N-PSK* метода, вероятността за успешна детекция на атаката „пилотно замърсяване“ се подобрява с около 5% в сравнение с резултатите от оригиналния *2-N-PSK* метод.

Основна цел на подобрената техника е да реши проблема на оригиналния метод с детекцията на атаки, започнали по време на втория тренировъчен период, т.е. ситуацията, описана като ***Сценарий 3*** по-горе. Поради тази причина е проведена друга група от експерименти [А3], в която отново пилотните сигнали са случайни, но ED винаги отсъства от първото пилотно предаване. Резултатите от вероятността за детекция на оригиналния метод и на подобрената техника при атаки, започнали с предаването на втория легитимен пилот, са изобразени на фиг. 2.12.

Графиките показват, че докато оригиналният *2-N-PSK* метод разкрива този тип атака с вероятност около 75%, подобрената техника постига успешна детекция за повече от 96% от случаите. Експерименталните резултати демонстрират значително подобрение в ефективността на *2-N-PSK* метода, когато предложената техника също е приложена.



Фиг. 2.11. Вероятност за детекция на оригиналния 2-N-PSK метод и на подобрената техника



Фиг. 2.12. Вероятност за детекция на оригиналния 2-N-PSK метод и на подобрената техника, когато ED изпуска първото пилотно предаване

2.5. Изводи и приноси към Втора глава

1. Предложена е нова техника, подобряваща ефективността на работа на *2-N-PSK* метода. Експериментално е потвърдено, че предложената нова техника повишава ефективността на *2-N-PSK* метода за детекция на атаката „пилотно замърсяване“.

2. Формулирани са и аналитично са описани случаите, в които *2-N-PSK* методът не успява успешно да открие атаката „пилотно замърсяване“.

ГЛАВА 3. Методи за откриване на атаката „пилотно замърсяване“ чрез анализ на диаграмата на състоянията

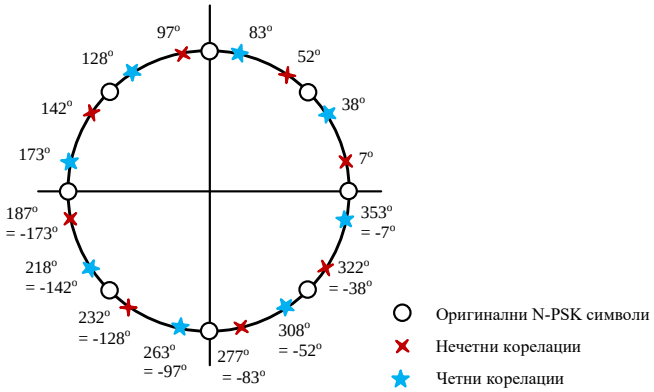
3.1. *Shifted 2-N-PSK* метод за откриване на атаката „пилотно замърсяване“ посредством отместени съзвездия

Въпреки че предложената техника успешно открива голяма част от атаките от ***Сценарий 3***, както и някои от ***Сценарий 2***, проблемните атаки от ***Сценарий 1*** и ***Сценарий 4*** остават неоткриваеми за метода. Това налага разработването на нов метод за откриване на атаката „пилотно замърсяване“, който е в състояние да открие всички възможни типове атака. Такъв метод е разработен в Трета глава на дисертационния труд.

Основната идея на новопредложения метод, наречен *Shifted 2-N-PSK* метод, се състои в това, че LU изпраща на BS пилотни сигнали, които не принадлежат на оригиналната и публично известна N-PSK диаграма на състоянията, наричана още съзвездие, а са част от две различни съзвездия, отместени от оригиналното с предварително определени градуси [A4].

Алгоритъмът се състои в отместване на всеки нечетен подред пилот на LU от неговата оригинална N-PSK стойност с x_1 градуса и всеки четен подред пилотен сигнал – с x_2 градуса. Също като при оригиналния *2-N-PSK* метод, резултатът от корелацията между двата приети сигнала се изчислява в BS и нейният ъгъл се сравнява с тези от референтно съзвездие. Ако аргументът на корелацията не съвпада с нито един от референтните ъгли, се счита че има налична атака.

Специфична особеност на *Shifted 2-N-PSK* метода е това, че референтните ъгли се различават от N-PSK ъглите. Освен това, съществуват две отделни референтни съзвездия – едно за нечетните подред корелации и едно за четните (фиг. 3.2). По този начин ъгълът на всяка нечетна корелация – като първата корелация z_{12} между първия и втория приет сигнал, се изчислява и сравнява с така нареченото нечетно референтно съзвездие, получено чрез добавяне на $y_1=x_2-x_1$ градуса към оригиналните N-PSK ъгли. Аналогично, всяка четна корелация, като втората z_{23} между втория и третия приет сигнал, се сравнява с четното референтно съзвездие, чиито ъгли са равни на N-PSK ъглите плюс $y_2=x_1-x_2$ градуса. Когато по време на процеса на оценка на канала в системата няма интрузия, ъгълът на резултата от корелацията принадлежи на съответното четно или нечетно референтно съзвездие [A4].



Фиг. 3.2. Четно и нечетно референтни съзвездия, когато $x_1=11°$ и $x_2=18°$

Тъй като при *Shifted-2-N-PSK* метода легитимният потребител изпраща пилотни сигнали от отместени съзвездия, е невъзможно дублирането или изпращането на реципрочните им стойности от ED, чиито нелегитимни сигнали са оригинални N-PSK символи. Затова при изследванията и анализа на ефективността на работа на *Shifted-2-N-PSK* метода, условията за успешна атака на отделните сценарии се модифицират. Атаката би могла да остане неразкрита, ако ED изпрати сигналът с този N-PSK ъгъл, който е най-близък по стойност до аргумента на отместения легитимен пилот или неговия реципрочен сигнал за ***Сценарий 1***, ***Сценарий 2*** и ***Сценарий 3***. За да атакува успешно системата според ***Сценарий 4***, ED трябва да изпрати в двата пилотни интервала тези N-PSK символи, които са най-близки по фаза до отместените пилоти на LU, плюс един и същи ъгъл. Следователно, за да атакува системата според описаните сценарии, ED трябва да се стреми не да открие пилотните сигнали на LU преди отместването, а да се доближи максимално до отместените легитимни пилоти според формула (3.1) и да изпрати N-PSK сигналите, които са в съответната връзка от сценария с отместените легитимни фазови ъгли.

$$\varphi^*\left(p_i^{LU}\right)+\frac{360^\circ}{2N}\geq\varphi_{xi}\left(N-PSK\right)\geq\varphi^*\left(p_i^{LU}\right)-\frac{360^\circ}{2N}. \qquad (3.1)$$

където с i е означен поредният номер на пилотния сигнал от двойката, т.е. $i = 1$ за първия пилот или $i = 2$ за втория пилот от двойката, а аргументите на легитимните пилоти след отместването са отбелязани с $\varphi^*(\cdot)$.

Аналитичното описание на модифицираните форми на четирите сценария, които се изследват при анализа на *Shifted-2-N-PSK* метода, наименувани съответно като ***Сценарий 1****, ***Сценарий 2****, ***Сценарий 3**** и ***Сценарий 4****, е както следва:

Сценарий 1*

$$\varphi\left(p_1^{ED}\right)=\varphi_{x1}\left(N-PSK\right) \quad \text{и} \quad \varphi\left(p_2^{ED}\right)=\varphi_{x2}\left(N-PSK\right).$$

Сценарий 2*

$$\varphi\left(p_1^{ED}\right)=\varphi_{x1}\left(N-PSK\right) \quad \text{и} \quad \varphi\left(p_2^{ED}\right)=\varphi_{x2}\left(N-PSK\right)+180^{\circ}.$$

или

$$\varphi\left(p_1^{ED}\right)=\varphi_{x1}\left(N-PSK\right)+180^{\circ} \quad \text{и} \quad \varphi\left(p_2^{ED}\right)=\varphi_{x2}\left(N-PSK\right).$$

или

$$\varphi\left(p_1^{ED}\right)=\varphi_{x1}\left(N-PSK\right)+180^{\circ} \text{ и } \varphi\left(p_2^{ED}\right)=\varphi_{x2}\left(N-PSK\right)+180^{\circ}.$$

Сценарий 3*

$$p_1^{ED}=0 \quad \text{и} \quad \varphi\left(p_2^{ED}\right)=\varphi_{x2}\left(N-PSK\right).$$

или

$$p_1^{ED}=0 \quad \text{и} \quad \varphi\left(p_2^{ED}\right)=\varphi_{x2}\left(N-PSK\right)+180^{\circ}.$$

Сценарий 4*

$$\varphi\left(p_1^{ED}\right)=\varphi_{x1}\left(N-PSK\right)+\varphi_x\left(N-PSK\right) \quad \text{и} \quad \varphi\left(p_2^{ED}\right)=\varphi_{x2}\left(N-PSK\right)+\varphi_x\left(N-PSK\right).$$

Успешната PCA детекция на схемата зависи от избора на стойности на отместванията и по-конкретно – от тяхната взаимовръзка [A5], [A6]. В някои случаи техниката преодолява само част от проблемите на оригиналния *2-N-PSK* метод, докато в други ситуации демонстрира способности за откриване на всеки тип атака на „пилотно замърсяване“. Ефективността на работа на метода в различните ситуации е представена в подточки *A, B* и *C*:

A. Отместванията на нечетните легитимни пилоти се различават от тези на четните легитимни пилоти с градуси, които не са равни на N-PSK ъгъл. Стойностите на отместванията не съвпадат с никой от N-PSK символите:

$$\varphi^*\left(p_1^{LU}\right)=\varphi\left(p_1^{LU}\right)+x_1 \quad \text{и} \quad \varphi^*\left(p_2^{LU}\right)=\varphi\left(p_2^{LU}\right)+x_2,$$

където $\left|x_1-x_2\right|\neq\varphi_x\left(N-PSK\right)$ и $x_1\neq x_2\neq\varphi_x\left(N-PSK\right)$.

В случаите, когато двете легитимни съзвездия се различават едно от друго с ъгъл, различен от N-PSK фаза, и нито едно от отместванията не е равно на N-PSK ъгъл, независимо от стойностите на пилотите, които неоторизираният потребител изпраща, аргументът на корелацията не принадлежи на референтното съзвездие и *Shifted 2-N-PSK* методът открива всички типове PCAs. Следователно, важно условие за успешното представяне на метода е нито легитимните, нито референтните съзвездия да не съвпадат с оригиналното N-PSK съзвездие.

B. Отместването на един от легитимните пилотни сигнали от двойката, нечетния или четния, не е N-PSK ъгъл, докато другото отместване е равно на аргумент от N-PSK съзвездието, т.е. или $x_1=\varphi_x$(N-PSK), или $x_2=\varphi_x$(N-PSK):

$$\varphi^*\left(p_1^{LU}\right)=\varphi\left(p_1^{LU}\right)+\varphi_x\left(N-PSK\right) \quad \text{и} \quad \varphi^*\left(p_2^{LU}\right)=\varphi\left(p_2^{LU}\right)+x_2 \text{ или}$$

$$\varphi^*\left(p_1^{LU}\right)=\varphi\left(p_1^{LU}\right)+x_1 \quad \text{и} \quad \varphi^*\left(p_2^{LU}\right)=\varphi\left(p_2^{LU}\right)+\varphi_x\left(N-PSK\right).$$

В този случай *Shifted 2-N-PSK* методът работи с двойки легитимни пилоти, един от които е отместен с определен ъгъл, докато другият принадлежи на оригиналното N-PSK съзвездие. Това означава, че стойността на отместването на всеки нечетен или на всеки четен пилот е равна на N-PSK ъгъл. В тази ситуация всички типове PCAs, с изключение на една, се разкриват от *Shifted 2-N-PSK* метода. При атака от типа на ***Сценарий 3****, възникнала по време на предаването на легитимен пилот, отместен с φ_x(N-PSK), методът не е способен да открие неоторизираната намеса. В случай че нечетните легитимни отместени пилоти не съвпадат с оригиналното съзвездие, докато четните съвпадат с него, „замърсяването“ е успешно, ако е инициирано заедно с втория пилот на всяка нечетна подред корелация. В противен случай, когато само четните легитимни пилотни сигнали са отместени, всяка четна подред корелация е уязвима към PCAs от типа на ***Сценарий 3****.

C. Отместванията на нечетните и на четните легитимни пилоти се различават едно от друго с N-PSK ъгъл, т.е. $|x_1\text{-}x_2| = \varphi_x(N\text{-}PSK)$:

$$\varphi^*\left(p_1^{LU}\right)=\varphi\left(p_1^{LU}\right)+x_1 \quad \text{и} \quad \varphi^*\left(p_2^{LU}\right)=\varphi\left(p_2^{LU}\right)+x_1+\varphi_x\left(N-PSK\right) \text{ или}$$

$$\varphi^*\left(p_1^{LU}\right)=\varphi\left(p_1^{LU}\right)+x_2+\varphi_x\left(N-PSK\right) \quad \text{и} \quad \varphi^*\left(p_2^{LU}\right)=\varphi\left(p_2^{LU}\right)+x_2.$$

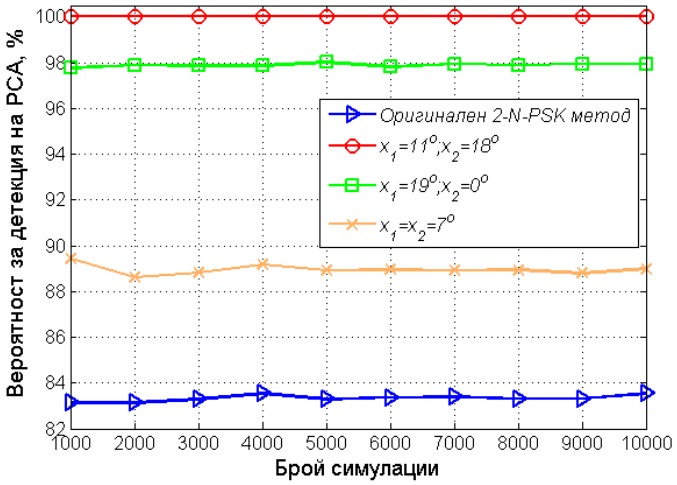
Когато стойностите на отместванията на двата пилота от легитимната двойка се различават с N-PSK ъгъл, т.е. по същия начин, по който в оригиналния *2-N-PSK* метод, съществува само едно референтно съзвездие, чиито ъгли съвпадат с оригиналните N-PSK фазови ъгли. Въпреки че използването на едно единствено съзвездие за анализа в BS редуцира сложността на системата, способностите за детекция на *Shifted 2-N-PSK* метода значително намаляват. В сравнение с ефективността на работа на *2-N-PSK,* методът с отместените съзвездия в случай *C* преодолява атаки от типа на ***Сценарий 2**** и ***Сценарий 3****, но остава уязвим към атаките от типа на ***Сценарий 1**** и ***Сценарий 4****.

3.2. Вероятност за детекция на атаката „пилотно замърсяване“ на *Shifted 2-N-PSK* метода

Качеството на работа на *Shifted 2-N-PSK* метода може най-добре да бъде оценено чрез анализ на неговата вероятност за детекция на PCAs. Трите различни сценария на *Shifted 2-N-PSK – A, B* и *C,* заедно с оригиналния *2-N-PSK* метод, са разгледани поотделно, така че ефективността им на работа да може да бъде сравнена. Първоначално отделните подходи са изследвани в отсъствие на шум, впоследствие вероятността им за детекция на PCA е измерена във функция на SNR [A5], след което е разгледан и ефектът от наличието на междуклетъчна интерференция в системата [A6].

Експериментите, изследващи вероятността за откриване на PCA при канали без шум, са разделени в групи в зависимост от броя на проведените симулации, като се използва системният модел, описан в т. 2.2. Пилотните сигнали на LU и ED във всяка симулация са избрани на случаен принцип, така че всички типове PCAs, независимо дали са откриваеми или не от оригиналния *2-N-PSK* метод, да могат да бъдат генерирани. Съответният брой симулации за всяка от групите са проведени множество пъти и осреднените резултати са представени графично на фиг. 3.10.

Графиките, илюстрирани на фиг. 3.10, потвърждават постигането на отлични резултати от *Shifted 2-N-PSK* метода в интерпретация на случай *A*. Вероятността за детекция на PCA е около 98% и 89% съответно в случаи *B* и *C*. Тези резултати са значително по-добри от резултатите, постигнати от *2-N-PSK* метода, който е ефективен в около 83% от атаките.



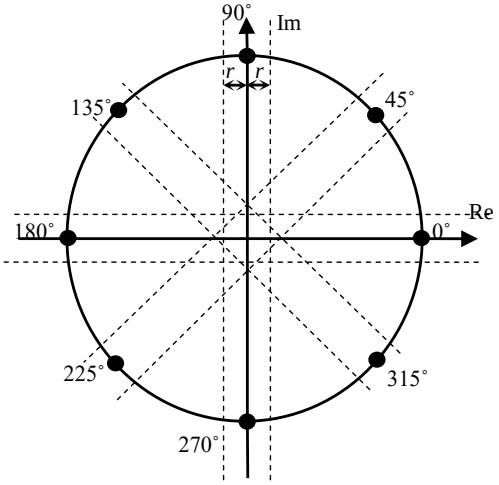
Фиг. 3.10. Вероятност за детекция на PCA на оригиналния 2-N-PSK и на Shifted 2-N-PSK метод при липса на шум и интерференция

Поради ефекта на шума аргументът на корелацията може да се различава от референтния фазов ъгъл с определена допустима стойност както в положителна, така и в отрицателна посока и по този начин регионът за детекция се формира във форма, подобна на тунел, около референтния ъгъл [А5], както е изобразено на фиг. 3.11.

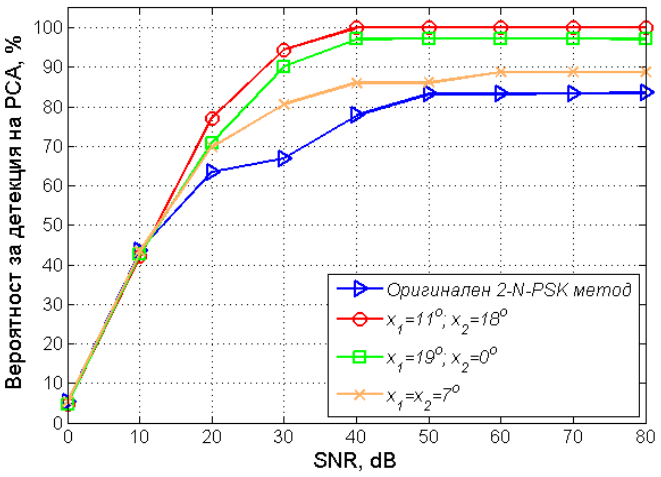
В [114] е предложена формула за дефиниране на регионите за детекция във функция от ПФ на легитимния канал - $\sqrt{P_{LU}}d_{LU}h_{LU}$, броя антени – M, и мощността на шума – N_0. Аналитичният израз (3.2) формира големината на региона за детекция във всяка посока – положителна и отрицателна. Разстоянието r се регулира чрез мащабираща константа c.

$$r = c\frac{\sqrt{N_0\left(MN_0 + 2\dfrac{P_{LU}d_{LU}\left\|h_{LU}\right\|^2}{M}\right)}}{M}. \tag{3.2}$$

Оригиналният *2-N-PSK* и трите разновидности на *Shifted 2-N-PSK* се тестват при наличие на шум и вероятността за детекция на PCA отново се анализира. Проведени са множество независими експерименти, всеки от които се състои от хиляди симулации, и резултатите са представени във фиг. 3.12.



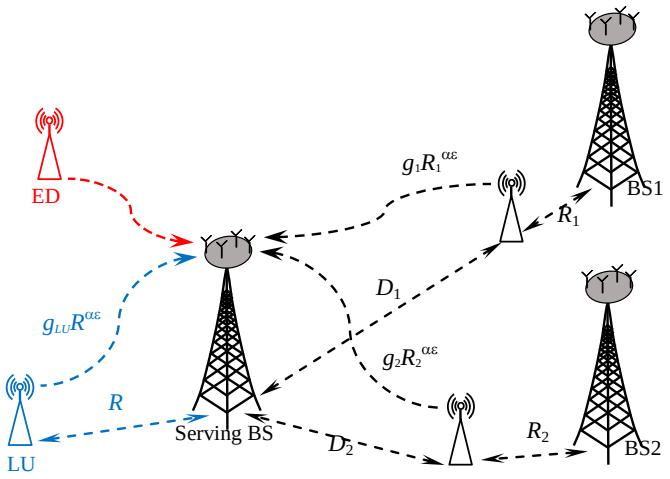
Фиг. 3.11. Региони за детекция около 8-PSK символите



Фиг. 3.12. Вероятност за детекция на PCA във функция от SNR на оригиналния 2-N-PSK и на Shifted 2-N-PSK метод

Въпреки сходството между четирите графики в областта на ниските стойности на SNR, при *Shifted 2-N-PSK* метода се наблюдава значително подобрение във вероятността за детекция на PCA, когато мощността на сигнала превишава тази на шума.

Подобни експерименти са проведени и когато системата се разглежда като разширен многоклетъчен модел като този, изобразен на фиг. 3.13, и влиянието на интерференцията върху вероятността за детекция на PCA също е изследвано [A6].



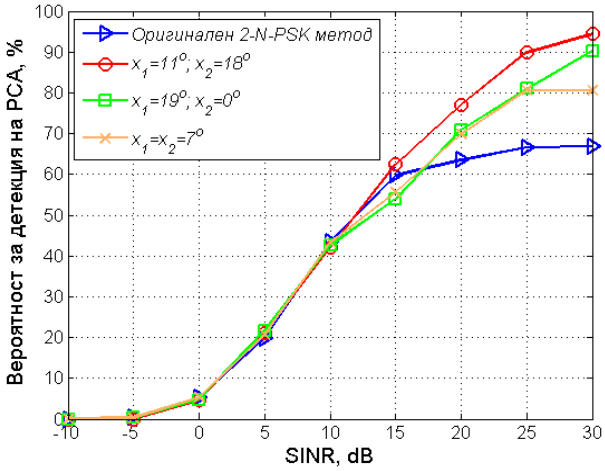
Фиг. 3.13. Многоклетъчен модел на система, включваща двама интерфериращи потребители от съседни клетки

Тъй като интерференцията възпрепятства ефективната работа на методите за детекция на PCAs, влиянието ѝ трябва да бъде оценено. За експериментални цели нивото на сигнал-към-интерференция-плюс-шум – SINR, се получава в съответствие с формула (3.3):

$$SINR = \frac{g_{LU} R^{\alpha(\varepsilon-1)}}{\sigma^2 + \sum_{u \in U} \left(R_u^{\alpha}\right)^{\varepsilon} g_u D_u^{-\alpha}}, \tag{3.3}$$

където U е множеството интерфериращи потребители, R е разстоянието между LU и основната BS (Serving BS), R_u е разстоянието от интерфериращ потребител $u \in U$ до обслужващата го базова станция, и D_u е разстоянието на интерфериращия потребител $u \in U$ до основната базова станция BS. Приетата мощност на желания сигнал в основната

BS се изразява като $g_{LU}R^{-\alpha}$. Мощността на шума е σ^2, α е експонента на загубите при разпространение, а с ε е означен коефициентът за контрол на мощността.



Фиг. 3.14. Вероятност за детекция на PCA във функция от SINR на оригиналния 2-N-PSK и на Shifted 2-N-PSK метода

Както показват графиките на фиг. 3.14, при ниски стойности на SINR, които се отнасят до потребителите около периферията на клетката, оригиналният *2-N-PSK* метод и трите разновидности на *Shifted -2-N-PSK* се държат приблизително по един и същи начин. При стойности на SINR, по-големи от 10 dB, графиките на вероятността за детекция на PCA започват да се различават една от друга и най-добри резултати се демонстрират от *Shifted 2-N-PSK* метода в случай *A*, който описва препоръчителния подход за реализация на схемата.

3.3. Връзка между отместванията на легитимните съзвездия при *Shifted 2-N-PSK* метода за детекция на атаката „пилотно замърсяване“

Както е отбелязано в предходните точки от настоящата глава на дисертационния труд, вероятността за детекция на PCA, демонстрирана от *Shifted 2-N-PSK* метода, се различава в зависимост от избора на стойности на отместванията на легитимните съзвездия.

Различаващата се ефективност, постигната в ситуации *A*, *B* и *C*, е основание за изследване на стойностите на отместванията на легитимните пилоти с цел откриване дали вероятността за детекция на PCA зависи от някаква взаимовръзка между четното и нечетно отместени легитимни съзвездия. За целите на този експеримент са проведени множество симулации със случайно избрани отмествания, но не е открита никаква закономерна зависимост между ефективността на метода и избора на стойности на отместванията. Въпреки това се забелязва, че при използването на някои двойки (x_1, x_2), съществуват корелации, чиито фазови ъгли са много близки по стойност до тези от съответното референтно съзвездие [А6]. Такъв сценарий би могъл да доведе до неспособност на метода да открие атаката, вследствие въздействието на шума и интерференцията или грешки от закръгление в резултат от ограничената точност на системата.

Тъй като вероятността за детекция на PCA зависи от избора на отместванията на легитимните пилотни сигнали, е проведено друго изследване, което се основава на следните аргументи: в случай, че пилотните отмествания могат да заемат само целочислени стойности, броят на всички възможни комбинации (x_1, x_2) е 360×360=129 600, понеже за всеки от двата пилота на легитимната двойка са възможни 360 варианта на отместване. За всяко $x_1 \in [0°, 359°]$, стойността на x_2 се променя последователно в същия диапазон $x_2 \in [0°, 359°]$. За всяка възможна двойка (x_1, x_2) са

проведени десет хиляди случайни симулации и в резултат от експериментите е изчислена вероятността за детекция на PCA. Ако вероятността за детекция на PCA клони към 100%, съответната тествана комбинация (x_1, x_2) се приема за една от оптималните. Тези оптимални комбинации са изброени за различни стойности на разграничаващия ъгъл [A6]. Терминът „разграничаващ ъгъл" означава максималните градуси, с които ъгълът на корелацията може да се различава от референтен ъгъл, но въпреки това се приема за равен на него. Това внася неточност в системата, зависеща от големината на разграничаващия ъгъл. Същите експерименти са изпълнени и с изброяване на двойките (x_1, x_2), които постигат вероятност за детекция на PCA по-голяма или равна на 98%. Обобщените резултати са представени в Табл. 3.25.

Разграничаващ ъгъл	Брой двойки (x_1, x_2), даващи вероятност за детекция на PCA 100%	Брой двойки (x_1, x_2), даващи вероятност за детекция на PCA ≥98%
0.005°	121 408	125 260
0.125°	91 369	123 224
0.25°	65 775	117 167
0.5°	34 959	97 616
1°	5 951	45 662

Табл. 3.25. Брой на оптималните двойки отмествания за Shifted 2-N-PSK при различни разграничаващи ъгли

Колкото по-малък е разграничаващият ъгъл, толкова е по-добра точността на системата и оттам броят на благоприятните комбинации на стойности на отместванията е по-голям. Резултатите в таблицата показват, че при много прецизна система, 100% вероятност за детекция на PCA се постига от 121 408 на брой комбинации на отместванията, което е около 93.7% от всички възможни двойки (x_1, x_2). При използване на много непрецизна скала, където разграничаващият ъгъл е 1°, само 5 951 на брой комбинации са препоръчителни, т.е. около 4.6% от всички възможни.

В зависимост от изискванията, когато за нуждите на системата е приемлива вероятност за детекция на PCA по-голяма или равна на 98%, се наблюдава значително увеличение на броя възможни двойки (x_1, x_2), постигащи благоприятни резултати. От всички възможни комбинации, около 95.1% и 35.2% удовлетворяват изискванията за разграничаващ ъгъл, съответно 0.005° и 1°.

Примери за вероятността за детекция на PCA, която постигат някои двойки стойности на отместванията при различни точности на системата, са дадени в Табл. 3.26. Представените резултати показват, че въпреки че двойката (x_1=9°, x_2=36°) постига вероятност за детекция на PCA от 100% при системи с разграничаващ ъгъл 0.25° или по-малък, което подобрява резултата на (x_1=13°, x_2=20°) за същата точност, при разграничаващи ъгли от 0.5° и 1°, по-добри резултати се получават с комбинацията (x_1=13°, x_2=20°). Въпреки че в последните три колони на Табл. 3.26 $|x_1-x_2|$=7°, тези три комбинации отмествания (x_1, x_2) постигат различна вероятност за детекция на PCA. Резултатите в Табл. 3.26 потвърждават, че не може да бъде открита никаква взаимовръзка между стойностите на двете отмествания в легитимната двойка, която оказва влияние върху способностите за детекция на *Shifted 2-N-PSK* метода.

Разграничаващ ъгъл	Вероятност за детекция на PCA, %					
	x_1=67° x_2=23°	x_1=32° x_2=19°	x_1=9° x_2=36°	x_1=13° x_2=20°	x_1=71° x_2=78°	x_1=11° x_2=18°
0.005°	100	100	100	100	100	100
0.125°	100	98.98	100	98.63	100	100
0.25°	97.81	97.95	100	98.59	100	100
0.5°	93.85	97.94	97.21	98.66	100	100
1°	91.69	95.79	97.31	98.65	98.60	100

Табл. 3.26. Примерни двойки отмествания за Shifted 2-N-PSK при различни разграничаващи ъгли

3.4. Алгоритъм за изчисляване на отместванията на легитимните съзвездия

В Трета глава от дисертационния труд е предложен алгоритъм, който може да бъде приложен при всеки от легитимните участници в комуникацията за изчисляване на стойностите на отместванията на легитимните съзвездия в следващия тренировъчен интервал. Тъй като преди първото пилотно предаване няма обмен на информация между LU и BS, алгоритъмът не може да бъде използван за определяне на стойностите на x_1 и x_2, затова се приема, че те са предварително договорени по защитен канал. Цялостният тренировъчен процес се състои в следните няколко основни етапа:

1) LU изпраща на BS по защитен канал стойностите на отместванията x_1 и x_2, които да бъдат използвани при предаването на първата двойка пилотни сигнали. x_1 и x_2 се генерират от генератор на случайни числа в LU и са стойности, които отговарят на изискванията за оптимална работа на работа на *Shifted 2-N-PSK* метода, т.е. $|x_1 - x_2| \neq \varphi_x(N - PSK)$ и $x_1 \neq x_2 \neq \varphi_x(N - PSK)$.

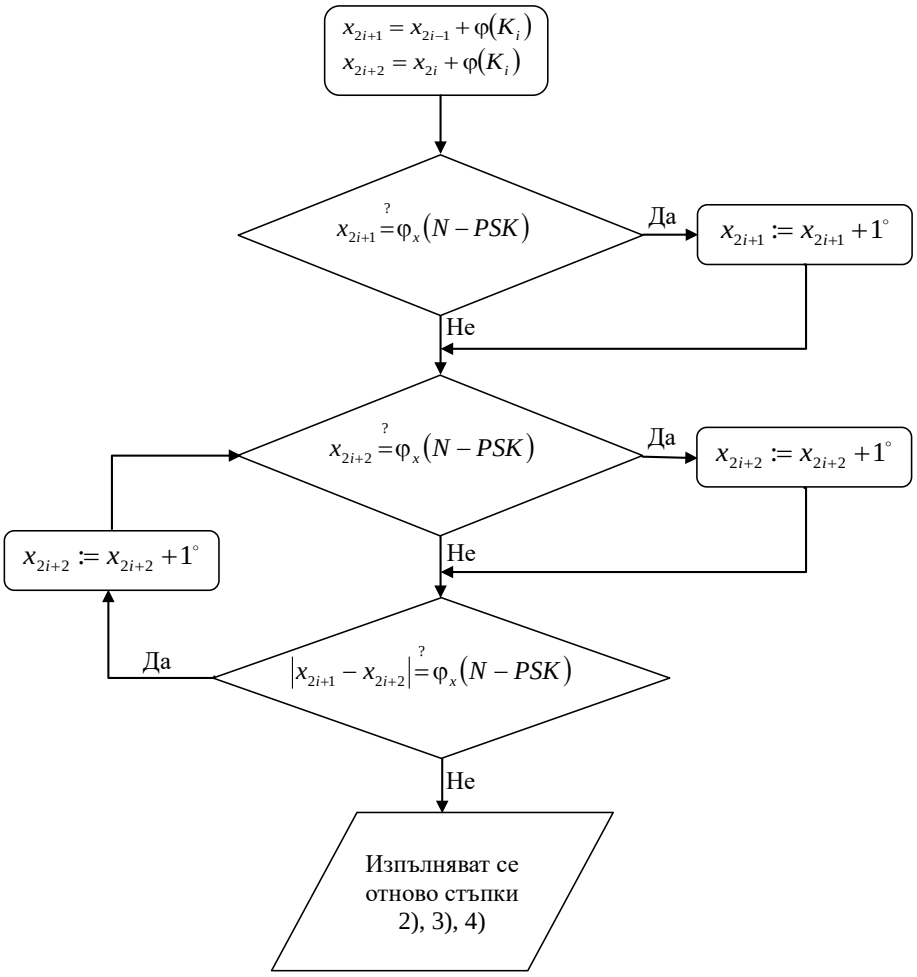
2) По време на първата тренировъчна фаза LU изпраща на BS два пилотни сигнала – ${p_1}^{LU}$ и ${p_2}^{LU}$, отместени от оригиналното N-PSK съзвездие, съответно с x_1 и x_2 градуса.

3) BS оценява легитимния канал K_1 и уведомява LU за състоянието на канала чрез протокол от по-високо ниво. Същевременно се прилага *Shifted 2-N-PSK* методът за детекция на атаката „пилотно замърсяване“ и BS сравнява корелацията на приетите пилотни сигнали с референтното съзвездие. В случай на атака, комуникацията се преустановява.

4) Както LU, така и BS самостоятелно изчисляват стойностите на отместванията x_3 и x_4, следвайки новопредложения алгоритъм. Стъпките 2), 3) и 4) се повтарят за всяка следваща оценка на канала K_i, изчислена през i-тата тренировъчна фаза: в етап 2) се предават сигналите ${p_{2i\text{-}1}}^{LU}$ и ${p_{2i}}^{LU}$, отместени съответно с $x_{2i\text{-}1}$ и x_{2i}; в етап 3) се оценява канала K_i; в етап 4) се изчисляват стойностите на отместванията x_{2i+1} и x_{2i+2}.

Алгоритъмът, използван на етап 4) за изчисляване на отместванията за следващия тренировъчен интервал, е представен систематизирано на блок-схемата на фиг. 3.15. По време на i-тата подред тренировъчна фаза, BS оценява канала в настоящия момент K_i. Тъй като нелегитимният потребител е разположен на място, различно от това на LU, то комуникационният канал между ED и BS е слабо корелиран с легитимния канал, атакуващият изпитва различно влияние на средата и няма информация за ПФ K_i, чийто характер е случаен. Поради тази причина фазата на канала $\varphi(K_i)$, която е известна само на BS и LU, може да бъде използвана от всеки от тях за изчисляване на ъглите на

отместванията на легитимните съзвездия x_{2i+1} и x_{2i+2}, предназначени за пилотното предаване в тренировъчен интервал i+1. Случайната природа на канала K_i, заедно с допускането, че стойностите на x_1 и x_2 са споделена тайна между LU и BS, определят сигурността на изчислените отмествания и дават възможност алгоритъмът да бъде публично известен и да се основава на елементарни математически операции. С цел опростяване на цифровите обработки и възможност за интегриране на алгоритъма в системи с ограничени изчислителни ресурси, е избрано x_{2i+1} и x_{2i+2} да бъдат получени като сума на отместванията от тренировъчна фаза i – x_{2i-1} и x_{2i}, и аргумента на ПФ на канала – $\varphi(K_i)$.



Фиг. 3.15. Блок-схема на алгоритъм за изчисляване на отместванията на легитимните съзвездия x_{2i+1} и x_{2i+2}

Според теоретичното описание на *Shifted 2-N-PSK* метода, най-ефективна е неговата работа в случай *A*, когато нито легитимните съзвездия, нито референтните не съвпадат с оригиналното N-PSK съзвездие, т.е. когато са спазени условията $|x_1 - x_2| \neq \varphi_x(N-PSK)$ и $x_1 \neq x_2 \neq \varphi_x(N-PSK)$. Това е доказано и от експерименталните резултати, представени в настоящата глава от дисертационния труд. Следователно, за оптимална работа на системата е необходимо стойностите на отместванията x_{2i+1} и x_{2i+2}, които алгоритъмът изчислява, също да отговарят на гореспоменатите условия.

Изпълнението на условието $|x_{2i+1} - x_{2i+2}| \neq \varphi_x(N-PSK)$ е гарантирано, в случай че $|x_{2i-1} - x_{2i}| \neq \varphi_x(N-PSK)$ е в сила, и x_{2i+1} и x_{2i+2} се изчисляват както следва: $x_{2i+1} = x_{2i-1} + \varphi(K_i)$ и $x_{2i+2} = x_{2i} + \varphi(K_i)$. Необходима е проверка на условията

$x_{2i+1} \neq \varphi_x(N-PSK)$ и $x_{2i+2} \neq \varphi_x(N-PSK)$. Ако някое от новоизчислените отмествания е ъгъл, равен на фаза от N-PSK съзвездието, му се присвоява стойност, увеличена с един градус. В резултат на изпълнението на условията $x_{2i+1} \neq \varphi_x(N-PSK)$ и $x_{2i+2} \neq \varphi_x(N-PSK)$ е възможно стойностите на x_{2i+1} и x_{2i+2} да бъдат променени така, че вече да не отговарят на условието $|x_{2i+1} - x_{2i+2}| \neq \varphi_x(N-PSK)$, поради което е необходима съответната проверка. Ако полученото референтно съзвездие съвпада с N-PSK символите, стойността на отместването на четния подред пилотен сигнал – x_{2i+2}, се увеличава с един градус и отново се проверява да не бъде равна на N-PSK аргумент. Когато всички условия за оптимален избор на изчислените стойности x_{2i+1} и x_{2i+2} са удовлетворени, може да се премине към изпълнението на етапи 2), 3) и 4) за следващата тренировъчна фаза – тази с пореден номер $i + 1$.

3.5. Изводи и приноси към Трета глава

1. Предложен е нов метод – *Shifted 2-N-PSK*, който преодолява проблемите на оригиналния *2-N-PSK* метод, свързани с неуспешна детекция на атаката „пилотно замърсяване“. Посредством задълбочени експериментални изследвания е доказана ефективността на предложения нов *Shifted 2-N-PSK* метод в случаите на неоткриваеми за оригиналния метод атаки. Експериментите са проведени при различни условия на средата за предаване: при липса на шум и интерференция в канала за връзка, в зашумена среда и когато каналът е под влиянието на шум и междуклетъчна интерференция.

2. Изследвана е връзката между отместванията на легитимните съзвездия на *Shifted 2-N-PSK* метода и са формулирани условията за оптимална работа на метода: *Shifted 2-N-PSK* методът постига най-голяма вероятност за детекция на атаката, когато нито отместените пилотни съзвездия, нито референтните не съвпадат с оригиналното N-PSK съзвездие. Броят оптимални двойки отмествания е експериментално получен за системи с различна точност.

3. Разработен е алгоритъм за изчисляване на отместванията на легитимните съзвездия. Отместванията, използвани за първото пилотно предаване, се обменят по защитен канал, а тези за всяка следваща тренировъчна фаза се изчисляват поотделно от базовата станция и от легитимния потребител. Това става посредством стойностите на отместванията и оценката на канала от предходната тренировъчна фаза.

ГЛАВА 4. Методи с ниска изчислителна сложност за потискане на ефекта от атаката на заглушаване

4.1. Същност на атаката на заглушаване

Друг вид атака, която може а бъде предприета срещу сигурността на физическия слой на безжичните комуникационни системи, е атаката на заглушаване. Заглушаването представлява умишлено генериране на радиосигнали от злонамерен потребител, които интерферират със сигналите, предавани между легитимните участници в комуникацията, и по този начин понижават качеството на комуникацията. По този начин атакуващият окупира ресурсите на безжичния канал и предотвратява достъпа на потребителите до мрежата, което представлява DoS атака на физическия слой. Заглушаването най-често се реализира чрез сигнал, представляващ теснолентово смущение.

В Четвърта глава от дисертационния труд е направен критичен анализ на основните методи, които могат да бъдат използвани на физическия слой за потискане на ефекта от атака на заглушаване. Методите са разделени в две основни групи – техники с разширяване на спектъра (FHSS и DSSS) и филтрация на заглушаващия сигнал в

приемника (MMSE, ZF, BJM и цифров филтър за IEEE 802.15.4). Разгледаните методи са сравнени посредством някои техни основни предимства и недостатъци, които могат да окажат влияние на реализацията им в различни типове мрежи в зависимост от инфраструктурните особености и наличните ресурси. Резултатите от сравнението са обобщени в Табл. 4.1 [A7].

Въпреки че методите за филтрация в приемника преодоляват недостатъците на техниките за разширяване на спектъра, нито един от подходите, участващи в сравнението, не е подходящ за филтрация на заглушаващи сигнали, чиято честота се мени с времето. За този специфичен сценарий на атаката на заглушаване, метод, който заслужава внимание, е адаптивната филтрация. Няколко такива решения са предложени в литературата, но повечето от тях са подходящи за употреба само в конкретни приложения и са прекалено сложни, за да бъдат използвани в мрежи с ограничени ресурси.

No	Сравнявани характеристики	Техники за намаляване на ефекта от атака на заглушаване					
		Подходи за разширяване на спектъра		Подходи за неадаптивна филтрация в приемника			
		FHSS	DSSS	MMSE	ZF	BJM	Цифров филтър за IEEE 802.15.4
1	Необходимост от допълнителни обработки в приемника	✓	✓	✓	✓	✓	✓
2	Необходимост от допълнителни обработки в предавателя	✓	✓	✗	✗	✗	✗
3	Необходимост от синхронизация	✓	✓	✗	✗	✗	✗
4	Необходимост от обмен на таен ключ	✓	✓	✗	✗	✗	✗
5	Неефективно използване на честотната лента	✓	✓	✗	✗	✗	✗
6	Влошаване на предаването при липса на атака	✗	✗	✗	✗	✗	✓
7	Висока изчислителна сложност	✓	✓	✓	✗	✗	✗
8	Необходимост от изчисляване на CSI	✗	✗	✓	✓	✗	✗
9	Необходимост от голям брой пилоти	✗	✗	✓	✓	✓	✗
10	Необходимост от запазване на неизползвана пилотна последователност	✗	✗	✓	✓	✗	✗

Табл. 4.1. Сравнение на разгледаните техники за намаляване на ефекта от атака на заглушаване

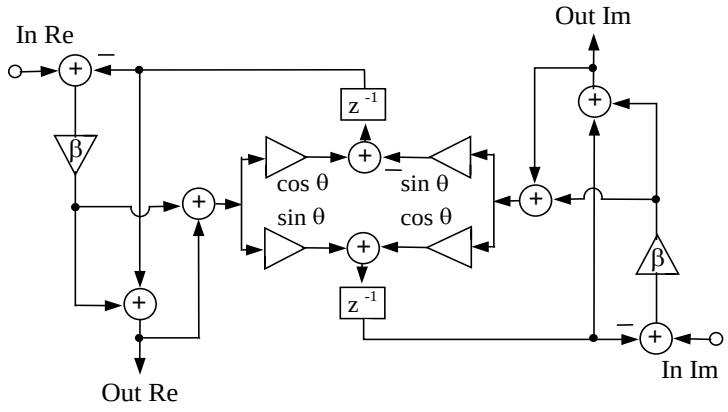
4.2. Метод за потискане на заглушаващия сигнал в приемника чрез използване на адаптивен комплексен теснолентов филтър

В Четвърта глава от дисертационния труд, за противодействие на атаката на заглушаване е предложено филтърно звено с комплексни коефициенти и независима настройка на централната честота и честотната лента, което се използва за създаването на адаптивен филтър [A8]. Реализацията, която се използва, е от първи ред, с ниска изчислителна сложност и с много ниска чувствителност, поради което е наречена LS1 – фиг. 4.4.

Предавателните функции на LS1 звеното, всяка от които е от лентов тип, имат вида:

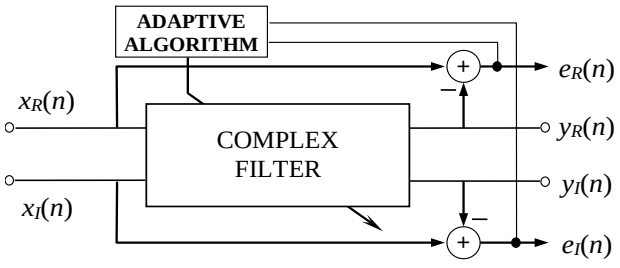
$$H_{RR}(z)=H_{II}(z)=\beta\frac{1+2\beta\cos\theta z^{-1}+(2\beta-1)z^{-2}}{1+2(2\beta-1)\cos\theta z^{-1}+(2\beta-1)^2 z^{-2}};$$
$$H_{RI}(z)=-H_{IR}(z)=\beta\frac{2(1-\beta)\sin\theta z^{-1}}{1+2(2\beta-1)\cos\theta z^{-1}+(2\beta-1)^2 z^{-2}}. \quad (4.9)$$

Ширината на честотната лента на филтъра може да бъде настроена чрез промяна само на един коефициент – β, а коефициентът θ контролира централната честота.



Фиг. 4.4. LS1 филтър от първи ред с комплексни коефициенти

Тази реализация се характеризира с две много важни предимства: първо, изключително ниската чувствителност в лентата на пропускане увеличава устойчивостта към ефектите на квантуване; второ, централната честота и ширината на честотната лента (на задържане, ако филтърът е режекторен, и на пропускане – ако е лентов) на филтъра могат да бъдат независимо контролирани, практически в целия работен честотен диапазон. На фиг. 4.5 е показана блокова схема на адаптивна теснолентова система с комплексни коефициенти, състояща се от режекторено и лентово LS1 комплексно филтърно звено.



Фиг. 4.5. Блок-схема на режекторен / лентов адаптивен комплексен филтър

Следва описание на входно-изходните уравнения на съответните режекторен и лентов филтър (4.10) - (4.16). Входно-изходното уравнение на реалния изход на лентовия филтър има вида:

$$y_R(n) = y_{R1}(n) + y_{R2}(n), \tag{4.10}$$

$$\begin{aligned} y_{R1}(n) = &-2(2\beta-1)\cos\theta(n)\,y_{R1}(n-1) - \\ &-(2\beta-1)^2\,y_{R1}(n-2) + 2\beta x_R(n) + \\ &+4\beta^2\cos\theta(n)\,x_R(n-1) + 2\beta(2\beta-1)\,x_R(n-2), \end{aligned} \tag{4.11}$$

$$\begin{aligned} y_{R2}(n) = &-2(2\beta-1)\cos\theta(n)\,y_{R2}(n-1) - \\ &-(2\beta-1)^2\,y_{R2}(n-2) - \\ &-4\beta(1-\beta)\sin\theta(n)\,x_I(n-1), \end{aligned} \tag{4.12}$$

където y_R е сигналът на реалния изход, а x_R е сигналът на реалния вход.

Имагинерният изход се представя чрез следната формула:

$$y_I(n) = y_{I1}(n) + y_{I2}(n), \tag{4.13}$$

$$\begin{aligned} y_{I1}(n) = &-2(2\beta-1)\cos\theta(n)\,y_{I1}(n-1) - \\ &-(2\beta-1)^2\,y_{I1}(n-2) + \\ &+4\beta(1-\beta)\sin\theta(n)\,x_R(n-1), \end{aligned} \tag{4.14}$$

и

$$\begin{aligned} y_{I2}(n) = &-2(2\beta-1)\cos\theta(n)\,y_{I2}(n-1) - \\ &-(2\beta-1)^2\,y_{I2}(n-2) + 2\beta x_I(n) + \\ &+4\beta^2\cos\theta(n)\,x_I(n-1) + 2\beta(2\beta-1)\,x_I(n-2), \end{aligned} \tag{4.15}$$

където y_I е сигналът на имагинерния изход, а x_I е сигналът на имагинерния вход.

Реалният и имагинерният изход на режекторния филтър са както следва:

$$e_R(n) = x_R(n) - y_R(n), \quad e_I(n) = x_I(n) - y_I(n). \tag{4.16}$$

Тегловната функция представлява мощността на сигнала на изхода на режекторния филтър:

$$[e(n)\,e^*(n)], \tag{4.17}$$

където $e(n) = e_R(n) + je_I(n)$.

Коефициентът на филтъра, който отговаря за централната честота, се актуализира да съответства на честотата на смущаващия сигнал посредством алгоритъма на най-малките средни квадрати LMS:

$$\theta(n+1) = \theta(n) + \mu\,\mathrm{Re}[e(n)\,y'^*(n)]. \tag{4.18}$$

μ е размерът на стъпката, който контролира скоростта на сходимост, $y'(n)$ е първата производна на $y(n) = y_R(n) + jy_I(n)$ спрямо коефициента на адаптация.

Реалната част на производната $y'(n)$ е:

$$
\begin{aligned}
y_R^{'}(n) = {} & 2(2\beta-1)\sin\theta(n)y_{R1}(n-1) - \\
& - 4\beta^2\sin\theta(n)x_R(n-1) + \\
& + 2(2\beta-1)\sin\theta(n)y_{R2}(n-1) - \\
& - 4\beta(1-\beta)\cos\theta(n)x_I(n-1).
\end{aligned}
\tag{4.19}
$$

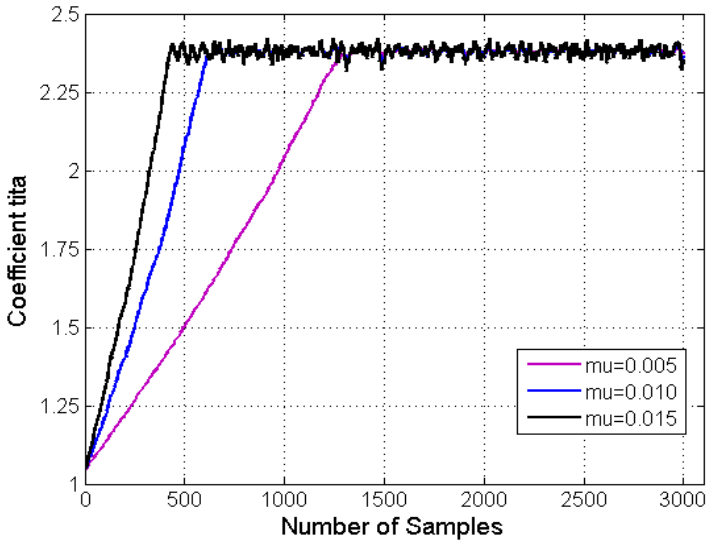
Имагинерната част на $y'(n)$ е:

$$
\begin{aligned}
y_I^{'}(n) = {} & 2(2\beta-1)\sin\theta(n)y_{I1}(n-1) + \\
& + 4\beta(1-\beta)\cos\theta(n)x_R(n-1) + \\
& + 2(2\beta-1)\sin\theta(n)y_{I2}(n-1) - \\
& - 4\beta^2\sin\theta(n)x_I(n-1).
\end{aligned}
\tag{4.20}
$$

4.3. Експериментални резултати, свързани с изследването на адаптивния комплексен LS1 филтър при наличие на атака на заглушаване

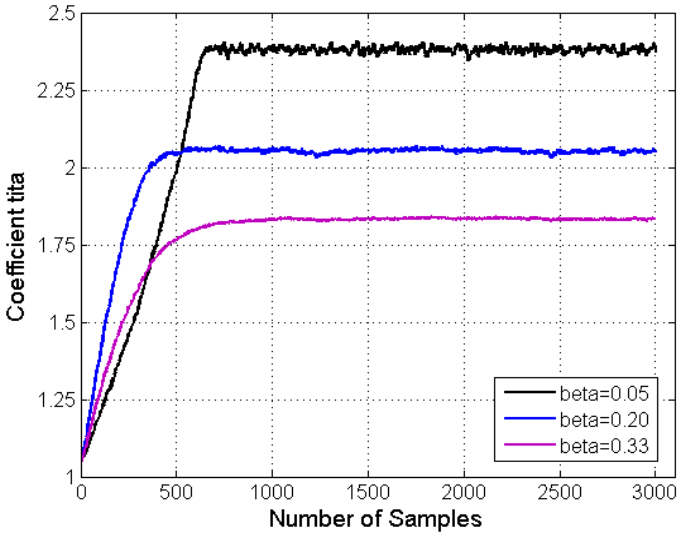
За целите на експериментите, легитимният информационен сигнал е моделиран като случаен широколентов сигнал, а теснолентовото смущение е представено чрез синусоида с определена централна честота, която може да бъде променяна. Първо е анализирано установяването на коефициента на филтъра, свързан с неговата централна честота, след което експериментално са демонстрирани отличните адаптивни свойства на филтъра и накрая е изследвана ефективността на предложеното решение за потискане на смущението, породено от атака на заглушаване [A8].

Проследен е адаптивният параметър θ, който контролира централната честота на филтъра. Поведението на филтъра е изследвано в сценариите с различен размер на стъпката μ и различна ширина на честотната лента, като резултатите са илюстрирани съответно на фиг. 4.6 и фиг. 4.7. От графиките на фиг. 4.6 се вижда, че колкото по-голям е размерът на стъпката, толкова по-бързо филтърът се установява в стабилно състояние, но това става за сметка на по-големите колебания, наблюдавани около установената стойност на централната честота, което може да доведе до известна неточност в работата на филтъра. Следователно, изборът на размер на стъпката на адаптация представлява компромис между времето, необходимо за установяване на системата в устойчиво работно състояние, и прецизността при детектирането на истинската стойност на централната честота на заглушаващия сигнал.



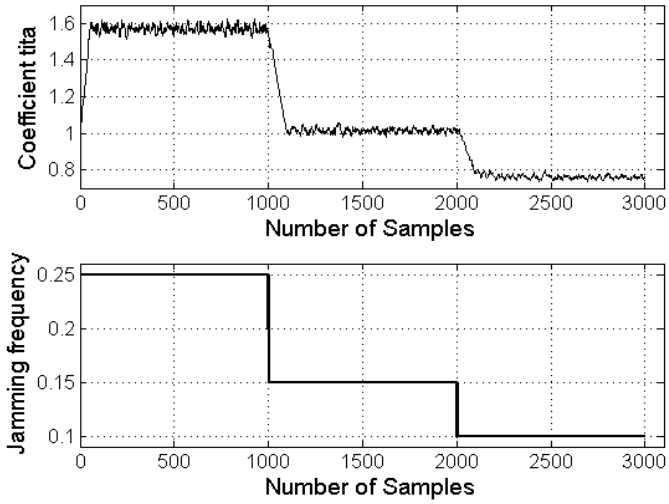
Фиг. 4.6. Обучаващи криви на адаптивния параметър θ при различен размер на стъпката μ

Проведени са също и симулации при фиксирана стойност на размера на стъпката μ=0.01 и различна ширина на честотната лента на филтъра. Както показват резултатите, изобразени на фиг. 4.7, колкото е по-широка честотната лента на филтъра, толкова по-голяма е разликата между стойността, в която се установява коефициентът θ, и действителната стойност, отговаряща на централната честота на теснолентовото смущение. Когато филтърът се установи в честота, различна от тази на смущението, тогава се потиска не само заглушаващият сигнал, а отчасти и легитимният широколентов сигнал, а това намалява качеството на предаване. Следователно, колкото по-тясна е ширината на честотната лента на филтъра, толкова централната честота, в която се установява филтърът е по-близка до тази на смущението и толкова по-малко е отклонението от истинската ѝ стойност.



Фиг. 4.7. Обучаващи криви на адаптивния параметър θ при различна ширина на честотната лента β

Адаптивните свойства на предложения комплексен филтър са експериментално изследвани чрез симулирането на заглушаващ сигнал, чиято честота се променя във времето. Резултатите са представени графично на фиг. 4.8, където се вижда, че промените в честотата на заглушаващия сигнал биват успешно проследени от теснолентовия адаптивен комплексен филтър.



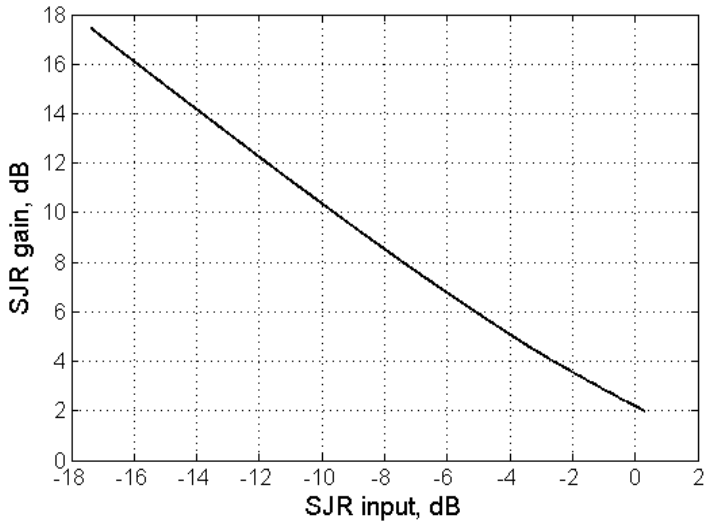
Фиг. 4.8. Проследяващи криви, показващи, че централната честота на предложения адаптивен комплексен теснолентов филтър се променя адаптивно в зависимост от честотата на заглушаващия сигнал

Качеството на работа на филтъра може да бъде най-добре оценено чрез сравнение на отношението сигнал-към-заглушаване SJR на входа на филтъра със стойността на SJR на изхода на филтъра. Подобряването на качеството на предаване може да бъде оценено чрез параметъра, наречен *SJR gain*, който се изчислява по формула (4.22):

$$SJR\ gain\,[dB] = SJR\ output\,[dB] - SJR\ input\,[dB], \tag{4.22}$$

където *SJR output* и *SJR input* са SJR отношенията, съответно на изхода и на входа на филтъра, които са експериментално получени.

Резултатите са представени графично на фиг. 4.9, където параметърът *SJR gain* е във функция от стойността на SJR на входа на филтъра. Тъй като при наличие на теснолентов заглушаващ сигнал с висока мощност, мощността на смущението е концентрирана в тесен спектър и надвишава спектралната плътност на мощността на широколентовия легитимен сигнал, SJR отношението преди филтрацията има отрицателна стойност. Колкото по-голяма е мощността на заглушаващия сигнал, толкова по-съществено е подобрението в качеството на предаване, което постига филтърът. Например, когато SJR на входа на филтъра клони към –18 dB, стойността на параметъра *SJR gain* е около 18 dB, докато при увеличаване на SJR на входа до –2 dB, стойността на *SJR gain* намалява приблизително до 3.8 dB. Освен това, може да се отбележи, че когато мощността на смущението се доближава до тази на легитимния сигнал, филтрацията не успява да постигне почти никакво потискане на заглушаването и стойността на *SJR gain* клони към едва 2 dB.



Фиг. 4.9. ***SJR gain*** *във функция от SJR на входа на филтъра*

4.4. Изводи и приноси към Четвърта глава

1. Предложен е нов метод за преодоляване на ефекта от атака на заглушаване с теснолентово смущение чрез използване на адаптивен комплексен теснолентов филтър в приемника.

2. Посредством експериментални изследвания е доказана ефективността на новопредложения адаптивен метод, в случай на атака със заглушаващи теснолентови сигнали, чиято честота се мени във времето.

НАУЧНО-ПРИЛОЖНИ И ПРИЛОЖНИ ПРИНОСИ

В дисертационния труд са постигнати следните значими резултати с научен и научно-приложен характер:

- Предложена е нова техника, подобряваща ефективността на работа на *2-N-PSK* метода. Експериментално е потвърдено, че предложената нова техника повишава ефективността на *2-N-PSK* метода за детекция на атаката „пилотно замърсяване“. Формулирани са и аналитично са описани са случаите, в които *2-N-PSK* методът не успява успешно да открие атаката „пилотно замърсяване“.
- Предложен е нов метод – *Shifted 2-N-PSK*, който преодолява проблемите на оригиналния *2-N-PSK* метод, свързани с неуспешна детекция на атаката „пилотно замърсяване“. Посредством задълбочени експериментални изследвания е доказана ефективността на предложения нов *Shifted 2-N-PSK* метод в случаите на неоткриваеми за оригиналния метод атаки. Експериментите са проведени при различни условия на средата за предаване: при липса на шум и интерференция в канала за връзка, в зашумена среда и когато каналът е под влиянието на шум и междуклетъчна интерференция.
- Изследвана е връзката между отместванията на легитимните съзвездия на *Shifted 2-N-PSK* метода и са формулирани условията за оптимална работа на метода: *Shifted 2-N-PSK* методът постига най-голяма вероятност за детекция на атаката, когато нито отместените пилотни съзвездия, нито референтните не съвпадат с оригиналното N-PSK съзвездие. Броят оптимални двойки отмествания е експериментално получен за системи с различна точност.
- Разработен е алгоритъм за изчисляване на отместванията на легитимните съзвездия. Отместванията, използвани за първото пилотно предаване, се обменят по защитен канал, а тези за всяка следваща тренировъчна фаза се изчисляват поотделно от базовата станция и от легитимния потребител. Това става посредством стойностите на отместванията и оценката на канала от предходната тренировъчна фаза.
- Предложен е нов метод за преодоляване на ефекта от атака на заглушаване с теснолентово смущение чрез използване на адаптивен комплексен теснолентов филтър в приемника. Посредством експериментални изследвания е доказана ефективността на новопредложения адаптивен метод, в случай на атака със заглушаващи теснолентови сигнали, чиято честота се мени във времето.

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

ПФ – Предавателна Функция
BJM – Blind Jamming Mitigation
BS – Base Station
DoS – Denial-of-Service
DSSS – Direct Sequence Spread Spectrum
ED – Eavesdropper
FHSS – Frequency Hopping Spread Spectrum
GLRT – Generalised Likelihood Ratio Test
IoT – Internet of Things
IPv6 – Internet Protocol version 6
LMS – Least mean squares
LS – Low Sensitivity
LU – Legitimate User
M2M – Machine-to-Machine

MaMIMO – Massive Multiple Input Multiple Output
MMSE – Minimum Mean Square Error
N-PSK – Phase-Shift Keying of N^{th} order
PCA – Pilot Contamination Attack
PLS – Physical Layer Security
SINR – Signal-to-Interference-plus-Noise Ratio
SJR – Signal-to-Jamming-Ratio
SKs – Secret Keys
SNR – Signal-to-Noise-Ratio
ZF – Zero-Forcing
4G – Fourth Generation
5G – Fifth Generation

СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД

[A1] D. Mihaylova, G. Iliev, and Z. Valkova-Jarvis, „Comparison of Methods for the Detection of Pilot Contamination Attacks," Proceedings of First International Balkan Conference on Communications and Networking (BalkanCom 2017), May 30 – June 2, 2017, Tirana, Albania, pp. 1-5.

[A2] D. Mihaylova, Z. Valkova-Jarvis, and G. Iliev, „An improved technique for the detection of pilot contamination attacks in TDD wireless communication systems," MATEC Web of Conferences, Proceedings of 21st International Conference on Circuits, Systems, Communications and Computers (CSCC 2017), vol. 125, art. no. 03007, 14-17 July 2017, Crete Island, Greece, pp. 1-4.

[A3] D. Mihaylova, Z. Valkova-Jarvis, and G. Iliev, „A New Technique to Improve the 2-N-PSK Method for Detecting Wireless Pilot Contamination Attacks," WSEAS Transactions on Communications, vol. 16, art. no. 21, pp. 176-183, 2017.

[A4] D. Mihaylova, Z. Valkova-Jarvis, G. Iliev, and V. Poulkov, „Shifted constellation-based detection of pilot contamination attacks," Proceedings of 2017 Global Wireless Summit (GWS 2017), 15-18 Oct. 2017, Cape Town, South Africa, pp. 83-86.

[A5] D. Mihaylova, Z. Valkova-Jarvis, and G. Iliev, „Detection capabilities of a shifted constellation-based method against pilot contamination attacks", in Proceedings of 2017 Advances in Wireless and Optical Communications (RTUWO 2017), 2-3 Nov. 2017, Riga, Latvia, pp. 56-60.

[A6] D. Mihaylova, Z. Valkova-Jarvis, and G. Iliev, „Relation of Optimal Pilot Offsets in the Shifted Constellation-Based Method for the Detection of Pilot Contamination Attacks," World Academy of Science, Engineering and Technology, International Journal of Computer and Information Technology (IJCIT), vol. 12, no. 8, 30-31 July 2018, Zurich, Switzerland, pp. 649-653, 2018.

[A7] D. Mihaylova, „An overview of methods of reducing the effect of jamming attacks at the physical layer of wireless networks," 4th EAI International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures (Fabulous 2019), 28-30 March 2019, Sofia, Bulgaria, (*accepted*).

[A8] Z. Valkova-Jarvis, D. Mihaylova, A. Mihovska, and G. Iliev, „Adaptive complex filtering for narrowband jamming mitigation in resource-constrained wireless networks," Wireless Telecommunications Symposium (WTS 2019), 9-12 April 2019, New York City, USA, (accepted).

SUMMARY

Methods and Algorithms for Secure Communications at the Physical Level of Wireless Telecommunication Networks

Dimitriya Angelova Mihaylova, M. Sc.

Abstract of Ph.D. Thesis

A major concern in contemporary wireless communication systems relates to their security and privacy provisioning. Over the last decade, physical layer security has drawn significant research attention as a means of protecting the network from unauthorized access. Despite its numerous advantages, PLS is still vulnerable to certain malicious user interventions. Two commonly used attacks that can be launched against security at the physical layer are jamming and eavesdropping. Due to the broadcast nature of their interface, wireless systems are especially at risk from these types of intrusion.

The goal of this PhD thesis is to improve the security of modern wireless communication systems through optimization and development of methods, techniques and algorithms for secure communications at the physical layer with low computational complexity.

The first chapter presents a critical overview of traditional security approaches. The security issues of contemporary wireless networks are discussed, and the principles and vulnerabilities of physical layer security are described. Finally, the main tasks to be solved further in the thesis are summarized in this chapter.

In the second chapter, four different methods for the detection of pilot contamination attacks are analysed and compared and one of them, named *2-N-PSK*, is chosen for future research. The scenarios in which the *2-N-PSK* method is not able to detect the attack are formulated and analytically described. A new technique to improve the performance of the *2-N-PSK* method is proposed. It is experimentally confirmed that the proposed new technique increases the efficiency of the *2-N-PSK* method for detecting pilot contamination attacks.

In the third chapter, a new method is proposed - *Shifted 2-N-PSK*, which overcomes the problems of the original *2-N-PSK* method related to unsuccessful detection of pilot contamination attacks. Through in-depth experimental research, the effectiveness of the proposed new *Shifted 2-N-PSK* method is demonstrated in the attacks scenarios that are undetectable by the original method. The experiments are conducted under different transmission medium conditions: in the absence of noise and interference in the communication channel, in a noisy environment, and when the channel is under the influence of noise and intercell interference.

The relationship between the legitimate constellations' shift values of the *Shifted 2-N-PSK* method is investigated and conditions are formulated for the method's optimal efficiency: best detection probability is achieved by the *Shifted 2-N-PSK* method when neither the legitimate nor the reference constellations coincide with the original N-PSK constellation. The number of optimal offset pairs is experimentally obtained for systems with different accuracy. An algorithm to compute the legitimate constellations' shift values is developed. Those used for the first pilot transmission are exchanged over a secure channel, while those for each subsequent training phase are calculated separately at the base station and legitimate user through the offset values and channel estimate from the previous training phase.

In the fourth chapter, existing jamming mitigation techniques used at the physical layer are compared. A new method is proposed to overcome the effect of a narrowband jamming by using an adaptive complex narrowband filter at the receiver. The effectiveness of the newly proposed adaptive method is experimentally investigated in the case of narrowband jamming whose frequency varies over time.