WorldWideWeb

https://doi.org/10.1007/s11280-018-0654-2

ASDR-basedveriﬁcationplatformfor802.11PHYlayer

securityauthentication

XiaoguangLi1·JunLiu1 ·BoyanDing1·ZhiweiLi1·HaoyangWu1·TaoWang1

Received:3October2018/Revised:7November2018/Accepted:26November2018/

©SpringerScience+BusinessMedia,LLC,partofSpringerNature2019

Abstract

TheWiFisecurityauthenticationmechanismcombinedwiththePHYlayerinformationhas

becomeahotspotofWiFisecurityresearch.ThePHYlayercontainsrichinformationsuch

aswirelesschannel,devicelocation,andsignalquality.HighperformanceWiFiverification

thatsupportsPHYlayerprogramminghasbecomeanindispensabletoolforWiFisecurity

research.ThispaperdesignsandimplementsaverificationplatformTickSECthatsupports

theresearchofWiFisecurityauthenticationatthePHYlayer.Itsupportsreal-timeacqui-

sitionofPHYlayerinformation,andofferstheprogrammabilitywithinthePHYlayer.We

alsogiveacasestudyofWiFideviceidentificationusingPHYlayerinformation.Exper-

imentalresultsshowthatTickSECcanmeettheneedsofPHYlayerWiFiauthentication

verification.

Keywords Softwaredefinedradio·WiFisecurity·PHYlayer·FPGA

ThisarticlebelongstotheTopicalCollection:SpecialIssueonSecurityandPrivacyinNetwork

Computing

GuestEditors:XiaohongJiang,YongzhiWang,TarikTaleb,andHuaWang

NaNA2018conference’srecommendationpaper

JunLiu

juneliu@pku.edu.cn

TaoWang

wangtao@pku.edu.cn

XiaoguangLi

lixiaoguang@pku.edu.cn

BoyanDing

dboyan@pku.edu.cn

ZhiweiLi

lizhiwei@pku.edu.cn

HaoyangWu

wuhaoyang@pku.edu.cn

1

PekingUniversity,Beijing,China

WorldWideWeb

1 Introduction

Inmodernsociety,thepopularityofWiFifacilitatespeople’slife.Inthemeantime,ithas

alsobroughtsecurityrisks.ThesecuritymechanismofthePHYlayerhasbecomeahot

topicinWiFisecurityresearch.ThePHYlayercontainsrichinformationonwirelesschan-

nels,such as equipment locations and signal quality, and researchers have sought to use

thesetoenhancethesecurityofWiFi.Examplesofinformationthatresearchershaveused

includeRSS(ReceivedSignalStrength)[37], CIR(ChannelImpulseResponse)[20, 21],

CSI(ChannelStateInformation)[22]andsoon.

WiFisecurityresearchrequiresaverificationplatformtoimplementandevaluatesecu-

rity mechanism. Compared with the security research of the upper layers (e.g. TCP/IP),

PHYlayersecurityresearchplaceshigherrequirementsontheverificationplatform.The

PHY layer data transmission rate specified in the 802.11ac protocol is 433Mbps (single

antenna,80MHzbandwidth),withPHYlayerdelaynotexceedingseveralmicroseconds.

PHYlayerimplementedwithsoftwarecannotmeettherequirementsintermsofthroughput

andlatency.Whilehardwareimplementationsareoftennotprogrammableenoughtofitthe

needsofsecurityresearch.

Thispapermainlyhasthefollowingcontributions:

–

–

ThoughanalysisofcommonWiFiattackandthreestrategiesofusingthePHYlayer

informationtodealwithWiFiattack,wechoosethePHYlayerinformation(suchas

CSI,RSSIandfrequencyoffset)forsecurityauthentication;

Based on previous work Tick [31], we design and implement TickSEC (Tick for

Security)platformthatsupportsPHYlayersecurityauthentication.Differentfromcom-

mercialnetworkcards,itcanobtainPHYlayerinformationinrealtimewhileproviding

programmability,convenientforPHYlayersecurityverification.

–

Asacasestudy,anapproachforidentifyingdifferentWiFidevicesusingPHYlayer

information is proposed. We verify the effectiveness of TickSEC and introduce a

machinelearningmethodtoanalyzetheresultsofsecurityauthentication.

Theremainderofthispaperisorganizedasfollows.Section2introducesthePHYlayer

of802.11andPHYLayerSecurityResearch.Section3presentsrelatedworkinWiFisecu-

rityresearchandseveralstate-of-the-artSDRplatformsforWiFiresearch.Sections4and5

analyzethedesignandimplementationofTickSECrespectively,highlightingitssupportfor

WiFisecurityresearchatPHYlayer.Section6proposesacasestudyandtheevaluationof

platform.Section7isthesummarythispaper.

2 Background:The802.11PHYlayer

The802.11PHYlayerspecifiesthemodeofmodulation,demodulation,coding,andradio

frequency parameters of data transmission and constitutes the lowest layer of the OSI

network model.Exceptthelegacy802.11b,whichusesdirect-sequencespreadspectrum

(DSSS) modulation techniques, other 802.11 standards, i.e. 802.11a/g/n/ac, use OFDM

(orthogonalfrequency-divisionmultiplexing)astheirmodulationtechnique.Soourwork

focusesonthemorecontemporaryOFDM.

2.1 The802.11processingpipeline

Figure1depictsablockdiagramofthe802.11PHYlayerprocessingpipeline.

WorldWideWeb

Figure1 Transmitterandreceivermodulesfor802.11a/g/n/ac

Onthetransmitterend,thePHYlayerobtainsaframeofbinarydatafromtheMAClayer.

Theframedatapassesthroughsourcecoding,constellationmappingandIFFT(InverseFast

FourierTransform).Thenguardintervals(GI)areinsertedineachsymbol,andapreamble

isprependedbeforetheframe.Finallythedatasamplesaresendedtoradiofrequency(RF)

frontendreachestheair.

Thereceivingend,ontheotherhand,convertsRFsignalreceivedintheairbackinto

framedata.ThePHYfirstacquireswirelesssignalfromtheairintheformofI/Qcom-

plexsamplesfromtheRFfrontend.Thesamplesaretrackedinthetimesynchronization

modules,whichdeterminesthestartofaframe.Whentimesynchronizationsucceeds,the

samplesarepassedthroughthefollowingmodules,includingfrequencysynchronization,

GIremovalandFFT,whichconvertstimedomainsignalbackintofrequencydomain.After

FFT,thechannelestimationmoduledoesequalization,removingtheinfluenceofthechan-

nel on the signal. Then the frame data is solved with a process that is a inverse of the

transmitter.

The802.11PHYlayercontainsaconsiderableamountofvaluableinformationforWiFi

securityresearch,especiallyatthereceivingside.CSIcanbeobtainedfromthechannelesti-

mationmodule,reflectingthelocationofthetransmitter,thesurroundingenvironment,etc.

Otherinformation,suchasRSSI,frequencyoffset[29],errorvectormagnitude(EVM)[28],

can be acquired from time synchronization, frequency synchronization and constellation

modulesrespectively.

2.2 Informationfrom802.11PHYlayer

This section describes some PHY layer information that is common in WiFi security

research.

RSSI (Received Signal Strength Indicator) is a measurement of the power present in

areceivedradiosignal,relatedtowirelesstransmitterpower,transmissionandreception

distance,andsurroundingobstacleenvironment.ResearchersoftenuseRSSItodistinguish

betweendifferentdevicesortoobtainchangesinthesurroundingenvironment.

CSI(ChannelStateInformation)referstoknownchannelpropertiesofacommunication

link.Thisinformationdescribeshowasignalpropagatesfromthetransmittertothereceiver

and represents the combined effect of, for example, scattering, fading, and power decay

withdistance.CSIhasawealthofphysicalubiquitythatisoftenusedtoextrapolateother

information,suchaslocationandmovement.

Frequencyoffset isanoffsetbetweenthecarrierfrequencyofthereceivedsignaland

thetransmittedsignal.Inradioengineering,afrequencyoffsetisanintentionalslightshift

ofbroadcastradiofrequency(RF),toreduceinterferencewithothertransmitters.Thefre-

quencyoffsetisestimatedbasedontheoffsetoftheperiod,andthenthefrequencyoffset

compensationisperformed.

WorldWideWeb

3 Relatedwork

3.1 WiFiPHYlayersecurityresearch

3.1.1 Hardwareﬁngerprint

Hardwarefingerprintreferstothetechnologyofidentifyingandauthenticatinghardware-

related PHY layer information. The hardware related PHY layer information in WiFi

include clock offset, clock fluctuation, and radio frequency characteristics. The PAR-

ADIS [8] system uses a variety of PHY layer information combined with the machine

learningmodeltoidentify802.11wirelessdevices.ThispapercollectsPHYlayerinforma-

tionrelatedtothehardware,includingfrequencyoffsetandoffsetofconstellationpoints.

TheexperimentsinthisarticleshowthatthePARADISsystemcanidentifymorethan130

commercialNICswithanaccuracyofover99Therearealsootherwirelesssystems,suchas

Bluetooth,whichusehardwarefingerprinttechnologyforidentification.Forexample,the

BlueID[13]systemusesclockcharacteristicsofBluetoothdevicesfordeviceidentification.

3.1.2 Channelﬁngerprint

Channel fingerprint refers to the technology of identifying and authenticating by using

channel-relatedPHYlayerinformation.Thechannel-relatedphy-layerinformationisoften

usedtolocateandjudgewhetherthedeviceismoved.TheinformationincludesCSI,RSSI,

multi-antenna signal direction matrix, et.al. Faria [9] used RSSI to authenticate wireless

devices.Bagci[6]suggestedusingCSItodetectwhethertheInternetofDevicesisunlaw-

ful.ThisarticleusesthechangeofCSItojudgewhetherthedeviceismoved.Xiong[35]

usedCSItorecognizeavarietyofactiveattacks.Multi-daylinetechnologyisusedinthe

802.11n protocol to significantly increase system transfer rate and accuracy. This article

usesthemulti-antennaCSItoextractthesignaltotheangleofview,andproposesasetof

DataCheckprotocolsthatarecertifiedbytheangleofarrivaltoidentifyandauthenticatethe

device.Itispossibletoidentifydevicesthatare5cmapart,andtherecognitionaccuracyis

significantlyimprovedcomparedtothe5mbyusingRSSI.

Thephysicallayersecuritymechanismisbasedonthesecuritymechanismoftheencryp-

tion technology and the non-encrypted, also known as the authentication-based security

mechanisms.Thesecuritymechanismbasedonencryptionhascertainlimitations.Complex

encryptionalgorithmsaredifficulttoimplementintheactualcommunicationsystem[24].

Therefore, some researchers explore the authentication-based security mechanisms [37]

. Instead of encrypting data, works in this approach leverage PHY layer information to

check the authenticity of wireless frames and devices. Table 1 provides a summary of

existingworksinthisapproach.Accordingtothetable,thesesystemshavethefollowing

requirementsforanidealverificationplatform:

–

–

–

ProvidescommonPHYlayerinformation,suchasCSI,RSSI,etc.,inadditiontosup-

portingextendedPHYlayerinformationlikefrequencyoffset,signalcorrelation[11],

constellationpointoffset[12]andCIR[20].

CustomizethePHYlayerdataprocessing.Forexample,researchhasintroducedarti-

ficialfrequencyoffsetsatthePHYlayersendingend[23].Thiscanonlybedoneby

platformsthatsupportPHYlayerprogramming.

Communicates in real time with commercial devices, increasing the credibility of

verificationresults.

WorldWideWeb

Table1 SummaryofauthenticationsystemsbasedonPHYlayerinformation

Existingworks

PHYinfo

Verificationplatform

TPDS’13[36]

RSS

Orinocosilvercard,AtherosminiPCINIC

USRPN210

TVT’16[34]

RSSI

MobiSys’10[16]

MILCOM’11[20]

ICC’13[21]

RSS

NokiaN800Internettablets

Simulation

CIR

CIR

Simulation

INFOCOM’13[22]

AISACCS’14[23]

ICC’07[33]

CSI

IntelIWL5300NIC

USRP

Freq.offset

Freq.offset

Wise[10]

–

SupportprocessmodularityofPHYlayer.TheprocessingofthePHYlayerinforma-

tionrequiresintensivecalculations,andthesoftwarepartcanquicklyimplementthe

encryptionalgorithmwhilethehardwarepartcanimprovetheefficiencyandmeetthe

timingrequirementsoftheprotocol.

3.2 WiFiresearchplatforms

The existing wireless platforms that support WiFi research at the PHY layer are mainly

dividedintofourtypes:

1.

ComputersimulationsoftwareswithoutRFfrontend.Ontheseplatforms,PHYlayer

implementedwithpuresoftwareforsimulation.NotableexamplesofthistypeareMat-

lab [27] and Wise [10]. The former provides a programming language suitable for

scientific computing and a rich collection of tools for wireless algorithms develop-

ment,supportinganumberofWiFiresearches.Whilethelattercontainsmodelingand

simulationtoolsspecifictowirelesscommuncation.

2.

3.

CommercialnetworkcardswithRFfront-endandPHYlayerimplementedonASIC.

These platforms provide ideal performance for real-time communication and veri-

fication. However their programming capability is limited by their proprietary and

fixed-functionimplementationonhardware.IntelIWL5300isoneofthecommonNICs

usedbyvariousstudies[22,32].

Softwareradioplatform,withRFfront-end,PHYlayerimplementedbysoftware.A

famous representation of this type is the combination of National Instruments hard-

wareUSRPandtheopen-sourcesoftwareGNURadio[7].GNURadioallowsusersto

developtheirownPHYlayermodulesinsoftwareandalsoprovidesagraphicaldevel-

opmentenvionmenttofacilitatethecustomizationofdataprocessingflow.Compared

withpuresoftwaresimulation,itisadvantageousinitsabilitytocommunicateinthe

realwirelessenvironment.However,theperformancelimitationofsoftwaremakesit

impossibletoimplementhigh-throuputprotocolssuchas802.11inrealtime.

FPGA-based platforms with RF front-end and PHY layer implemented by FPGA

hardware.FPGAoffersboththehighperformanceofhardwareandprogrammability

throughhardwaredescriptionlanguages(HDL),idealforaccelerationofcustomized

applications.Severalplatformshavebeendevelopedtheseyearsinthefieldofwireless

research.RiceUniversity’sWARPplatform[17]isanexample.

4.

WorldWideWeb

These four types of wireless verification platforms have different characteristics and

advantages. However, currently none of the platform is ideal for PHY layer security

research.Computersimulationsoftwarehasthebestprogrammabilityandalargeamountof

publiccodeforresearch,butitcannotbeverifiedinarealwirelessenvironment.Theperfor-

manceofcommercialnetworkcardsisthebestandrealenvironmentverificationispossible,

buttheprogrammabilityistheworstinthefourtypes.Software-basedradioplatformshave

highPHYlayerprogrammabilityandcandowirelesscommunication,buttheircommu-

nicationperformanceislowandtheycannotmeettherequirementsoftheWiFiprotocol

standard.FPGA-basedradioplatformshavethebestpotential,withbothhighperformance

andreasonableprogrammability.However,theseplatformsarestillinearlystagesinterms

ofmaturityandtheyarenotoptimizedforsecurityresearch.Table2providesacomparison

ofthesetypesofplatforms.

Therefore, researchers at the PHY layer for WiFi security need a wireless open plat-

formthatsatisfiestheirneedsinbothperformanceandprogrammabilitytoimplementand

validatetheirresearch.

Our work is based upon the Tick [31] platform, which provides a high-performance

andprogrammableSDRimplementationthatsupports802.11a/g/acprotocol.Theoriginal

Tickisn’toptimziedforsecurityresearch,where[18]proposessomepreliminaryideason

theengineeringaspect.Wefurtherdevelopupontheideasofthelatterworkandformed

aarchitecturedesignandimplementation.Li[18]containsmoretechnologicaldetailsof

certainmodulesdescribedhere.

4 DesignofTickSEC

4.1 Designgoals

Basedontheaboverequirementsonverificationplatformsforauthentication,thefollowing

designgoalsoftheverificationplatformshouldbemet:

1.

2.

Realize802.11protocol,enablingreal-timecommunicationwithcommercialwireless

networkcard;

SupportcustomizationofdataprocessinginPHYlayer;

Table2 ComparisonofdifferenttypesofWiFiresearchplatforms

Platform

PHYinfo

extraction

PHYlayer

Interoprability

Performance

(example)

programmability

SimuationSW

(Matlab)

No

Good

No

No

Poor

Good

Poor

Good

WirelessNIC

(IntelIWL5300)

SW-basedSDR

(GNURadio)

FPGA-basedSDR

(WARP)

Partly

Yes

Yes

Good

Poor

Notrealtime

Yes

Yes

WorldWideWeb

3.

4.

Easyaccesstocommonly-usedPHYlayerinformation,suchasRSSI,CSI,frequency

offset,etc.,andsupportuserextensiontoacquireotherPHYlayerinformation;

Supportsoftwareandhardwareimplementationsofsecurityalgorithms,providingthe

abilitytointerchangebetweenhardwareandsoftwaremodules.

4.2 Designchallenges

thedesignchallengeTickSECfaceareasbelow:

1.

PHYlayerinformationextraction.WeneedtoobtainvariousinformationinPHYlayers

whileensuringhighperformance.HowtoobtainthespectruminformationfromPHY

layerinreal-timewithoutaffectingnormalcommunicationisachallenge.Wealsoneed

tosolvetheproblemsinanalysingspectrumconditionsfromtheseinformation.

Low-latencyandhighthroughputtransmission.Theextractionandtransmissionlatency

of PHY layer is very important for WiFi security applications. How to achieve low

latencyandhighthroughputtransmissionofPHYlayerinformationisachallenge.

Oneverificationplatformshouldnotonlysatisfytheexistingresearch,butalsopro-

videacertaindegreeofextensibilitytosupportfutureinnovations.Howtodesignthe

interfacetoimprovethescalabilityisanotherchallenge.

2.

3.

4.3 TickSECarchitecturedesign

Toovercometheabove-mentionedchallenges,weproposethecorrespondingarchitectural

designsofTickSECbasedupontheoriginalTick[31]system.ThearchitectureofTickSEC

extendsinthreeaspects:First,thescopeofsoftwareandhardwarecollaborationisextended,

andthePHYlayerisalsoconnectedtotheembeddedprocessorthroughtheAXIbus,sothat

userscandirectlyconfigurethePHYlayerandtoobtaindatafromtheit;second,TickSEC

providesuserswithsoftwareandhardwareprogramminginterfacetoextractthecommonly

usedPHYlayerinformation;third,extensiblehardwaremoduletoanalyzethePHYlayer

informationanditsinterfacewithsoftwareisdesigned.Theadvantageofthisapproachis

thatWiFisecurityresearcherscaneasilyobtaincommonPHYlayerinformationfromthe

softwaresideandexpandotherPHYlayerinformation,andcanchoosetoimplementtheir

ownsecuritymechanismsbyhardwareorsoftwareforverification.

4.3.1 OverviewofTickSEC

ThehardwarestructureofTickSECisillustratedinFigure2.Theblockdesigninthefigure

isthepartofthesoftwareandhardwareco-design.TheUSBcommunicationlibraryused

toprovideconnectionwiththehostPCisplacedoutsidetheblockdesign.Coremodulein

blockdesignisanembeddedMicroBlazeprocessor.LowMacTXandRXarethesender

andreceiverpartsoftheLowMAC,whichisresponsibleofthetiming-criticallogicofthe

MAClayers,andarereservedfromTickdesign.InTickSEC,wepackagePHYTXand

RXmodules,whichwereoutsideinTick,intoIPsandplacethemintoblockdesign.This

enablestheirconnectionwiththeembeddedprocessorthroughtheAXIbus,andtheradio

frequency(RF)supportlibraryalsomovesintotheblockdesign.ThePHYAnalyzermode

newlyaddedhardwareIPofTickSEC.ItisusedtoperformdataanalysisonthePHYlayer

informationobtainedfromthePHYlayermoduleandfeedtheanalysisresultbacktothe

embeddedprocessor.

WorldWideWeb

Figure2 TickSEChardwaremoduledesign

4.3.2 ExtractionofcommonPHYlayerinformation

Inthispart,severalcommonlyusedPHYlayerinformationextractionmethodswithframes

aredescribed,specificallyincludingCSI,RSSI,frequencyoffsetandclockoffset.Inabove,

wementionedthatCSIandRSSIarethemostcommonlyusedPHYlayerinformationin

securityresearch.Frequencyoffsetsareoftenusedinauthentication-basedsecuritymecha-

nisms.FortheAP,theprotocolspecifiesthatabeaconframeistransmittedevery100ms.We

canobtainthebeaconframebyreceivingthetimestampofthebeaconframethusclockoff-

setcanbecalculatedfromthebeacons.Thefollowingwillintroducetheextractionprocess

ofCSI,RSSIandfrequencyoffsetrespectively.

Before discussing ways to extract CSI and other PHY layer information, we’ll first

presentabriefintroductionof802.11frame,especiallyfieldsinthepreambletofacilitate

understandingoftheextractionalgoritms.

Figure3illustratesthestructureofthe802.11a/gframeatthePHYlayer.Thepreamble

at the beginning of the frame is prepended by the sender before the data and is known

to both parties. The receiver performs synchronization and channel estimation based on

preamble.Thepreamblein802.11a/gPHYlayercontainstwotrainingfields.Thefirstis

shorttrainingsequence(STS)of160samplingpoints,followedbylongtrainingsequence

(LTS)ofanother160samplingpoints.SIGNALfield(80samplingpoints)comesafterthese

trainingfields,specifyingtheframelengthandmodulationmethod.Theshorttrainingword

takes16samplingpointsasacycle,atotalof10cycles,samplingintervalis0.05μ s,used

todoAGC(automaticgaincontrol),timesynchronization,frequencysynchronization,etc.,

willbedescribedlaterwhenextractingfrequencydeviationandRSSI.Thefirst32sampling

pointsofthelongtrainingwordareguardintervals,whicharecomposedof16sampling

Figure3 802.11a/gFramestructure

WorldWideWeb

points T1 and T2. T1 and T2 are repeated. The long training words are used for channel

estimationandfine-grainedfrequencyoffsetestimation.

CSI TheCSIof802.11referstothecurrentchannelstatusofeachsubcarrier.Itisacommon

assumption that the CSI doesn’t change substantially within the reception process of an

802.11frame.Basedonthisassumption,the802.11implementationsoftenusestheLong

TrainingSequence(LTS)inthepreambletoestimatethechannel.TheextractionCSIis

donewithinthechannelestimationmodulewhichanalysestheLTS.

ThefrequencydomainvaluesoftheLTSisasequenceof1and−1s,asshowinFigure4,

withoutothervalues(the0inthemiddleistheDCcomponentwhichdoesn’tcarryinfor-

mation).SotoobtainCSIfromLTS,weonlyneedtoconvertthesignofeachsubcarrier

accordingtoFigure4.Ontheotherhand,theSTSisnotsuitableforCSIcalculationbecause

italsocontainsothervaluessuchas0and1+j.InthespecificimplementationofTick-

SEC,weprestorethetheoreticalvalueofthelongtrainingwordandcompareitwiththe

longtrainingwordreceived.Whenthetheoreticalvalueis−1,thesignofreceivedvalue

inverted,andthetheoreticalvalueis1whenitisunchanged.Afterthesignconversion,a

vectorof52samplesisobtained.ThisvectorcanrepresenttheCSIofthisframe.

RSSI The software driver of the Tick RF communication library provides a function to

directlycalculatetheRSSI.However,inpracticaltests,itisfoundthattheexecutionofthis

functionisrelativelyslow,lastingseveralmilliseconds,sotheresultdoesnotrepresentthe

RSSIofthecurrentframe.InordertoextracttheRSSImoreaccurately,TickSECcalculates

thepowersumoftheshorttrainingwordsinthesynchronizationmodule,becausethethe-

oreticalpowervalueoftheshorttrainingwordsofdifferentframesisfixed,andunlikethe

longtrainingwords,whichhasalargesubcarrierspan.However,theautomaticgaincon-

trol(AGC)attheRFfrontendwillaffectthevaluereceivedatPHYlayer.Thusthegainat

AGC,canbereadfromRFfrontendwithlowlatency,shouldalsobetakenintoaccountin

RSSIcalculation.

Frequencyoﬀset Thefrequencyoffsetisextractedinthefrequencyoffsetestimationmod-

uleandutilizestheperiodicityoftheSTS,specifically,thelast64samplingpoints(4outof

10cycles)oftheshorttrainingwordisused.Therearetworeasonsforthispartialutilization.

First,theprevioussamplepointsareaffectedbyAGCmentionedabove,andtheiramplitude

fluctuates.Usingthemmightdegradetheaccuracyoffrequencyoffsetcalculation.Second,

theframeisusuallysynchronizedatthemiddleofSTS,andthefrontbeginningmaynotbe

synchronized.Experimentsshowthattakingthelast4cyclesisafeasiblesolution.

Wefirsttransformthefrequencyoffsetequations.Assumingthatthereceivedvaluesat

timesk1andk2arer(k1)andr(k2)andthetheoreticalvaluesares(k1)ands(k2),thereare

thefollowingequations:

j2πfk1/fs

j2πfk2/fs

r(k1) = s(k1)·e

r(k2) = s(k2)·e

(1)

(2)

Figure4 Frequencydomainvaluesof802.11a/gLTS

WorldWideWeb

Among them, f is the frequency offset, fs is the sampling frequency, the value of

whichis20Min802.11a/g.r(k1),r(k2),s(k1),s(k2),andfs areallknown.Wecanfind

f usingthefollowingmethod.Accordingtothecharacteristicsoftheshorttrainingword,

i.e.,its16samplingpointsrepetition,whenk2 = k1+16,s(k1) = s(k2),substitutingthe

valuesthepreviousequation,wecangetthefollowing:

Let r(k1) =A+Bj

(3)

r(k2)

fs

B

A

f = 2π·16arctan

(4)

Equation (3) is derived from the properties of complex numbers. r(k1) and r(k2) are

complexnumbers,sotheresultofdivisionisalsoacomplexnumber.Thecomplexnumber

canalwaysbewrittenintheformofA+Bj,whereAandBarerealvalues.Equation(4)

isobtainedbysubstituting(3)into(1)and(2)toobtainthefrequencyoffsetvalue.

In the implementation of TickSEC, we get A and B in the hardware, these values

are passed to the software. Then by the software calculates arctan and multiplication

to get frequency deviation. When hardware calculations A and B are needed, every 16

receivers Dividing the sample points and dividing the complex number r(k1)/r(k2) into

∗ |

|2.

r(k1)r(k2) /r(k2)

WegetasetofAandB fromthe16thsamplingpointbeforeit.Weadd64AandB

obtainedfrom64samplingpointstoaverage,reducetheerror,andfinallytheextractedPHY

layerinformationistheaverageA.B,denotestheperiodicshiftrealpartandtheperiodic

shiftimaginarypart,respectively.

4.3.3 AlignmentofthePHYlayerinformation

AfterthedesignoftheextractionofPHYlayerinformation,wefacetwopracticalproblems:

one is the frame alignment problem of the PHY layer information, and the other is the

exactreceptiontimeproblem.TheframealignmentproblemofthePHYlayerinformation

means that when the software MAC layer receives a frame, the PHY layer information

correspondingtotheframeistakenfromthePHYlayer,nottheinformationofprevious

frameornextframe.ThisproblemsarisesfromthefactthattheMACandPHYlayersin

Ticksystemworksasynchronously.SohowwecanmaketheMAClayergetthecorrect

PHYlayerinformationwithoutblockingthePHYlayerhasbecomeaproblem.Theexact

receptiontimeproblemreferstohowthesoftwareMAClayeracquirestheprecisearrival

timeoftheframewhenitreceivesaframe.JanaandKasera[14]proposestousetheframe

arrivaltimeasthebasisforcalculatingthehardwarefingerprint,andthearrivaltimemust

beaccurate,i.e.,inμs level.However,theasynchronousnatureofMAC-PHYinteraction

alsomakesthetimestampatMAClayerinaccurate.Oursolutionofthesetwoproblemsare

discussedinthefollowing.

ForthealignmentofthePHYlayerinformation,weuseathree-levelcacheillustrated

inFigure5.WhenthePHYlayerreceivesaframe,eachmodulecalculatesthePHYlayer

information throughthe preamble.Theinformation isfirst storedinside the module and

isalignedwiththeclockofthemodule.Thisiscalledintra-modulebuffering.Whenthe

SIGNALfield,whichfollowsthepreambleoftheframe,iscorrectlydecodedandtheLow

MACisreadytoreceivethecurrentframe,thePHYlayernotifiestheLowMACmodule

thatithasreceivedaframeandinitiatesaninterrupttotheembeddedprocessor.Atthis

time,TickSECwillcachethePHYlayerinformationfromvariousmodulesinanotherset

ofunifiedclockregistersthroughclockdomainconversion.Theunifiedmoduleisknown

WorldWideWeb

Figure5 Three-levelbufferingframework

asthePHYlayerinformationcollectionmodulecache.Thepurposeofthisstepistoallow

eachmoduletocontinueprocessingthenextframeandupdatethein-modulecache.

AftertheLowMACsoftwarereceivestheinterrupt,thePHYlayerinformationcachedby

thePHYlayerinformationcollectionmoduleisstoredinthethirdgroupofregistersaligned

withtheAXIbusclock,calledtheMAClayerhardwarecache,andtheLowMACsoftware

readsthedatathroughtheAXIbus.ThePHYlayerinformationcachedbytheMAClayer

hardware reads the PHY layer information of the frame that received the interrupt. The

purpose of this step is to allow the PHY layer to initiate the next frame of the interrupt

totheLowMAC.TheprocessorcanreadthePHYlayerinformationofthisframeatany

laterpositionwithinaframe.Theadvantageofadoptingthethree-levelbufferingmethodis

thatwhileensuringthatthedatasegmentofoneframeandthePHYlayerinformationkeep

synchronizing,thereceptionanddataprocessingofthefollowingframearenotblocked.

AnotherpossiblesolutionofthealignmentproblemisusingaFIFOqueuetostorePHY

layerinformation.ButwefindthissolutioninfeasiblebecausethePHYlayerwilldiscard

framesundercertainconditions,suchasunrecognizedmodulationmethod,toolongframe

length,andembeddedsoftwaremayalsoTheinterruptwillbelost.OncethePHYlayer

dropstheframeortheinterruptisnotprocessed,thebufferedPHYlayerinformationwill

notberead.Thequeueisblockedandinformationgetsdislocated.Thissituationisdepicted

inFigure6.Ifbufferingisintheregister,thePHYlayerinformationofthefollowingframe

willcoverthepreviousonewhenanerroroccurs,andwillnotcausemisalignment.

4.3.4 Designofaccuratereceptiontime

Foraccuratereceptionproblems,TickSECusesthePHYlayertimestampmethod.First,

weusea64-bitcounteratthePHYlayerandexposeittotheLowMACinterface.Ateach

clockcyclethecounterisincrementedbyone.Theclockfrequencyofthismodulehereis

100MHz,sotheprecisionofthecounteris10ns.Then,whenthePHYlayersynchronizes

toaframe,thecountervalueisreadandheld.TheLowMACsoftwarewillreadthesaved

counter value through the AXI bus when it receives an interrupt from PHY layer. This

methodusesthevalueofthecounterasatypeofPHYlayerinformationandusesathree-

levelbufferingtechniqueforrecording.Thecounterisequivalenttobufferinginthemodule.

AXI busread andwrite width is32bits. Ingeneral,the low32-bit canrecord about43

secondstimeinterval.Formorethan43seconds,thehigh32-bitshouldbeused.

WorldWideWeb

Figure6 DislocationproblemwhenusingFIFO

TheadvantageofusingthePHYlayertimestampisthattheusercanaccuratelylearn

therelativereceptiontimeofthecurrentframe.Ontheonehand,itcancalculatetheclock

offsetasaPHYlayerinformationalone[14].Ontheotherhand,itcanbecombinedwith

otherPHYlayerinformation.TherelationshipbetweenotherPHYlayerinformationover

timeandthetime-varyingPHYlayerinformationalsohaveimportantphysicalmeanings.

5 Implementation

5.1 PHYlayersoftwareinterface

PHYlayersoftwareinterfaceprovideawaytoextractPHYlayerinformationfromhardware

modulesintosoftware.TheTickSECsoftwarecodecontainsembeddedsoftwareparton

MicroblazeofLowMACandhostdriverpartonPC.Thesoftwareinterfaceshouldsupport

dataacquisitiononbothparts.

Weadoptatwo-levelprogrammingstructureofembeddedsoftwareandhostsoftware.It

firstextractsthePHYlayerinformationintotheembeddedsoftware.ThenthePHYlayer

informationistransferedtothehostviaaPCIe/USBcommunicationframework,insteadof

directlysendingPHYlayerinformationtothehostdriver.Thisstructurehasthefollowing

advantages:

–

–

–

TheLowMACcontrolflowisimplementedbyembeddedsoftware.Theusermayuse

PHYlayerinformationdirectlyintheLowMAC,forexample,todeterminewhetherto

replyanACKframeaccordingtothePHYlayerinformation.

TheembeddedsoftwareincludesaninterfacewiththehostPC.ThePHYlayerinfor-

mationisfirstextractedintotheembeddedsoftware.Theusercandecidewhetherto

continueuploadingtheinformationandmaintainthecentralizedcontrolprocess.

Theinteractionbetweenhardwarelogicandembeddedsoftwarefacilitatesextension.

Ifuserswantotherinformation,theycansimplyaddmoreAXIregisters.However,if

theyaredirectlyexportedtothedriver,thehardwarelogicoftheUSBcommunication

libraryneedstobemodifiedwhenextensionisrequires,whichwouldrequireexcessive

changestothecommunicationlibrary.

WorldWideWeb

Thespecificimplementationisdescribedasfollows.TickSEChardwareandsoftware

transfervaluesthroughAXIregisters.Eachregisteris32bitsinwidth.Table3containsthe

definitionoftheAXIregisters.Thesedataareprovidedtoboththeembeddedsoftwareon

MicroblazeforanalysisintheLowMAClayeroronthehostPC.

5.2 PHYlayerinformationanalysismodule

TickSECprovidesahardwaredataanalysismodulefordataanalysisofPHYlayerinforma-

tiontocomplementsoftwareanalysis.Thehardwaredataanalysismoduleconnectedtothe

PHYlayertoobtainPHYlayerinformationandperformdataprocessing.Theembedded

softwareprocessesdatathroughtheAXIinterface.

Thismoduleprocessconfiguresparametersandobtainsprocesseddata.Theadvantages

ofthehardwareanalysismodulearehighefficiencyandstrongreal-timeperformance.In

thehardwareanalysismodule,weprovide32setsofAXIregisters,allowinguserstointeract

withsoftwareandhardware.

5.3 PHYlayerinformationextension

TickSECalsoprovidesmethodsforuserstoexpandPHYlayerinformationinadditionto

commoninformationsuchasCSI,frequencyoffset,RSSI,andmodulationmethods.Cou-

pledwiththefullyprogrammablenatureofTick’sownPHYlayer,TickSECcanbewell

adaptedtotheincreasinglyevolvingandchangingneedsofresearchers.

The following describes an extension of PHY layer information with an example. In

additiontofrequencyoffset,[8]usesSYNCcorrelationandI/Qoriginoffsettogenerate

Table3 Registerdefinitionof

theTickSECsoftware

programminginterface

RegID

R/W

Registerdefinition

0x00

0x01

0x02

0x03

0x04

0x05

0x06

0x07

0x08

0x09

0x0A

0x0B

0x0C

0x0D

0x0E

0x0F

0x10

0x11

W

R

R

R

R

R

R

R

R

R

R

R

R

R

R

R

R

R

RequesttoreadPHYinfo

PHYinfoready

RealpartofPeriodicaloffset,high32bits

RealpartofPeriodicaloffset,low32bits

ImagpartofPeriodicaloffset,high32bits

ImagpartofPeriodicaloffset,low32bits

Numeratorofautocorrelationinsynchronization

Autocorrelationnormalizationfactor

NumeratorofcorrelationwithSTS

NumeratorofcorrelationwithLTS

Correlationnormalizationfactor

SIGNAL,containingframelengthandmodulation

CSIofsubcarrier−21

CSIofsubcarrier−7

CSIofsubcarrier+7

CSIofsubcarrier+21

High32bitsoftimestamp

Low32bitsoftimestamp

WorldWideWeb

devicefingerprints.Wewillnextusesynchronizationcorrelationasanexampletointroduce

howuserscanextendPHYlayerinformation.

We’llfirstintroducethebackgroundofsynchronizationcorrelation.WeusetheSTSfor

timesynchronization,andusetheperiodicityoftheSTSwhichrepeatsevery16sampling

points. When the correlation (autocorrelation) between the adjacent 16 sampling points

exceedsacertainthreshold,wethinkthatwehavediscoveredtheSTS.Thisprocessiscalled

framesynchronization,showninFigure7.

Tocalculatecorrelation,weusetwoadjacentslidingwindowsW1 andW2.Thesizes

ofbothtwowindowsare16samplingpoints.However,onlyframesynchronizingisnot

enough, because there are 10 repetitions of the short training words. We cannot deter-

minewhichofthetwoadjacentgroupsaresynchronized.Toaccuratelylocatethesampling

points,LTSisalsoneeded.WeuseLTScorrelationstocompare16samplingpointswith

long training words. When the correlation (cross correlation) with long training words

exceedsacertainthreshold,andtheautocorrelationislowerthanthethresholdatthesame

time,itisconsideredthatthebeginningsampleofLTSisfound.Thistimethebeginning

sampleofLTSandframedatacanbeaccuratesynchronize.Thisprocessiscalledsymbol

synchronizationandisshowninFigure8.

WhenthesamplingpointsinW1 arealllocatedintheSTS,thesamplingpointsinW2

arealllocatedintheLTS,thecross-correlationbetweenthetheoreticalvaluesofthefirst

16 points in LTS and W2 will be above a certain threshold, and the correlation between

pointsW1 andW2 willbelowerthanthethreshold.Synchronizingdependenciesinclude

autocorrelation and cross-correlation. Brik et al. [8] pointed out that synchronous cross-

correlationisrelatedtohardwareandcanbeusedtoidentifydevices.

Thefollowingusescross-correlationasanexampletointroducehowtoaddasoftware

interfacewithsynchronizingdependencies.

The first step is to list the equations of synchronous cross-correlation, where Pn is a

normalizationfactor.

L−1

Cn=

rn+k·sn∗+k

(5)

k=0

L−1

L−1

Pn=

|rn+k|2·

|sn+k|2

(6)

(7)

k=0

k=0

|Cn|2

P

Mn=

n

WeknowthatFPGAhardwareismoresuitableformultiplicationandadditionthandivi-

sion.SincedivisioninFPGArequiresmoreclockcyclesandhashigherdelay.Therefore,

wecancalculateCnandPnbyhardware.Inaddition,becauseenergyvalueofthelongtrain-

ingwords

L

−1

|s | isfixed,calledP ,andweonlyneedtocalculate

2

L−1

|rn+k|2in

k

=0

k=0

n

+k

hardware.ThecalculationofM isdonebysoftware.

In the second step, Cn and Pn are calculated in the synchronization module and are

n

derivedfromthesynchronizationmodule.Addtheportofthesynchronizationmodule,as

Figure7 Slidingwindowofframesynchronization

WorldWideWeb

Figure8 Slidingwindowofsymbolsynchronization

shownbelow.Hereistheschematiccode.Actually,inadditiontoCnandPn,wehavealso

derivedseveralsignalsforcalculatingautocorrelation.

The signal valid signal indicates that the subsequent module has successfully

decodedthesignalfield.Thisvalueis1onlyifthesignalfieldisvalid,otherwiseitis0.We

assignsync para Candsync para P1whensignalvalidis1.

The third step is clock domain conversion. This step converts sync para C and

sync para P1 in the corresponding clock domain of the synchronization module

into axi sync para C and axi sync para P1 in the AXI bus clock domain, and

assigns them into AXI registers. TickSEC provides a clock domain conversion module

reg clk domain switch.Itsusagehereislistedasfollows.

ThefourthstepistoreadCnandPn fromtheembeddedsoftwarecodeandusesoftware

tocalculatetheMnweneed.TheembeddedsoftwarecodethatreadsandcomputesMnis

listedbelow.SYNC PARA LTSistheenergyvalueofthepre-savedlongtrainingwords.

WorldWideWeb

Atthispoint,usingsynchronouscorrelationasanexample,theuserhascompletedthe

expansionofthePHYlayerinformation.

5.4 Multi-RFmode

Inordertosupporttheperfectchannel,wehaveextendedtheRFcommunicationlibrary

toprovidetwomodes,RFmodeandloopbackmode.TheRFmodeprovidesfunctionality

identicaltotheoriginalRFcommunicationlibraryandthePHYlayerisconnectedtothe

RFfrontendnormally.Inloopbackmode,ontheotherhand,theoutputofPHYtransmitter

isdirectlysentbacktothereceiver.

This approach facilitates debugging for WiFi security researchers in their early stage

of system implementation. Using the loopback mode to simulate the perfect channel,

researchersdonotneedtodealwiththecomplexitytheRFfrontend.Theycanalsoobtain

someresultwithouttheneedtocommunicatebetweenmultipledevices.Also,theswitch

betweenthetwomodesisquiteeasy,theinterfacesarecompatibleinthetwomodesand

onlyoneparameterneedstobechange.

Thefollowingdescribesthespecificimplementationoftheloopbackmode,asshown

inFigure9.ThedatainterfacebetweentheRFcommunicationlibraryandthePHYlayer

containstwoasynchronousFIFOs.Intheloopbackmode,wedirectlyconnecttheoutput

ofthesendingFIFOtotheinputofthereceivingFIFO.Whenthereisn’tdata,blanksignal

isfilledintothereceivingFIFOtosimulateblanktimewhenthereisnosignalintheair.

WhenthetransmitterofthePHYlayernotifiestheradiofrequencysupportlibrarytosend

aframe,itenterstheloopbackmodeandfetchesdatafromthesendingFIFOdirectlyinto

thereceiverFIFO.

Itisworthnotingthatinadditiontomultiplexingofdatastreams,clockandresetsignals

mustbemultiplexed.ThetransmitandreceiveFIFOsareasynchronousFIFOs.InRFmode,

theRFclockandresetsignalsarefromtheRFmodule.Inloopbackmode,theyneedtobe

changedtoPHYlayerclockingandresetsignals,asshownbelow.

Figure9 RFmodeandloopbackmode

WorldWideWeb

6 Casestudyandevaluation

6.1 Casestudysetup

Wegiveacasestudyforidentifydifferentdevicesintwoimplementationwaysusingfre-

quencyoffset.Forthesoftwareimplementationoftheplatform,weusethefirsthalfofthe

off-linedatatotrainthemachinelearningmodel,andthesecondhalfoftheoff-linerecord

asthetestset.Wechoosek-NearestNeighbor(KNN)[38],linearregressionanalysis[25],

randomforest(RF)[19],decisiontree[26],andSupportVectorMachine(SVM)[15]asthe

learningmodel.BothtrainingandtestcodeareimplementedinPython,andthemachine

learninglibraryistheopensourcePythonmachinelearningframework,scikit-learn[1].The

softwareimplementationofthismethodislimitedbyPython’slowimplementationefficiency

anditsinabilitytoexecuteonembeddedprocessors,whichcanonlybedoneoff-line.

ThehardwareimplementationutilizesthePHYAnalyzermoduletoidentifytheWiFi

deviceinrealtime.WeembedtheimplementationoftheidentificationlogicintothePHY

AnalyzermodulewiththehelpofVivadoHLS(High-LevelSynthesis)tool[30].Theiden-

tificationisdoneontheembeddedsoftwarewhichreadsdatafromPHYAnalyzerthrough

theAXIbus.

AsshowninFigure10,weuseAD9361[4]boardwithFMCinterfaceasRFfront-end

device.PHYandlowMAClayersareimplementedontheXilinxKC705[5]evaluation

board.Specifically,MicroblazeprovidedbyXilinxisadoptedtorealizethelowMAClogic,

AXIbusisusedtoconnectthehardwareIPs.WeuseCypressCYUSB3KIT-003[3]explorer

kitandanFMCinterconnectboard[2]tosupporttheimplementationofUSB3.0communi-

cationlibrary.Ubuntu14.04operatingsystemisusedonhostcomputer.Wedevelopverilog

HDLcodeandCcodeoflowMACinVivado2015.2andSDKrespectively.

6.2 PHYlayerinformationextraction

ThissectionteststhevalidityoftheTickSECreadingPHYlayerinformation,weusethereal

802.11devices,selectsthemostcommonlyused2.4GHzand5GHzfrequencyband,and

performs1–2minutemonitoringonthisfrequencybandtorecordthefrequencydeviation.

Figure10 AphotoofTickSECsystem

WorldWideWeb

Table4 Devicedistributionandfrequencyoffsetofchannel1

DeviceNo.

Last24bitsof

MACaddress

Framecount

avg.f

σ

1

2

3

4

5

6

7

8

9

10

0x003A98

0xA0C589

0xA434D9

0x66C002

0x48437C

0x08D40C

0x2ADCB6

0xDE436A

0x8AF314

0xF48B32

4247

686

556

507

409

394

364

229

195

151

−26.5586

5.0964

6.8343

6.7770

7.6319

4.3990

5.1095

3.7925

11.1968

3.3673

6.2982

7.9951

−24.5785

−0.1805

−11.0173

0.3264

−1.1527

−27.3364

−24.1565

6.2376

Table4showsthedevicesandtheirfrequencyoffsetdistributionscollectedfromreceived

framesonchannel1(2.412GHz).Itcanbeseenthatthereisarelativelylargedifference

infrequencyoffsetbetweendifferentdevices.Withtheexceptionofdevice7,thestandard

deviationoffrequencyoffsetofthesamedeviceissmall.

Table5showsthedevicesandtheirfrequencyoffsetdistributionscollectedfromreceived

frames on channel 161 (5.805GHz). Compared with 2.4 GHz, there is a relatively large

differenceinfrequencyoffsetbetweendifferentdevices.Withtheexceptionofdevice7,the

standarddeviationoffrequencyoffsetofthesamedeviceisverylarge,furtherindicating

thatthefrequencyoffsetbetweendifferentdevicesisquitedifferent.

Therearetwomainreasonsforusingthefrequencyoffset:First,thefrequencyoffset

isrelatedtothehardwarecircuitofthedevice,andthedifferencebetweendevicescannot

beignored.Forotherphysicallayerinformation,channel-relatedinformationsuchasCSI

andRSSIwillfluctuateafterthedeviceismoved,thusnotsuitabletotellbetweendevices;

andtheclockoffsetcanonlybeusedtoidentifytheAPandnotidentifytheSTA.Second,

thefrequencyoffsetisusedtoshowtheadvantagesoftheplatform,becausethefrequency

offsetisdifficulttoobtainfromthecommercialnetworkcard.

Table5 Devicedistributionandfrequencyoffsetofchannel161

DeviceNo.

Last24bitsof

MACaddress

Framecount

avg.f

σ

1

2

3

4

5

6

7

8

0xDCEF09

0x9DA868

0x67A622

0x9AE07C

0xD6FF00

0xB699D3

0x7ADC74

0x2C9FC7

Others

4953

711

672

291

189

83

−4.8232

−3.4210

−4.0277

−3.7384

−3.9803

−2.8351

−62.3400

−5.5038

−18.3011

9.7126

4.7535

7.7692

8.9364

5.4527

1.9508

24.0868

13.2189

37.5738

83

56

575

WorldWideWeb

Figure11 Adevicesubcarrieramplituderesponsecurveat2.4GHz

Besidesfrequencyoffset,otherdataarealsocollectedduringthecasestudytodemonstrate

theeffectivenessofTickSECtoreadPHYlayerinformation.CSIdataispresentedhereasan

example.Figures11and12showstheCSIoftwodevicesat2.4GHzand5GHzovertime.

Thetwodevicesarethedevicesthatreceivethemostframesintwochannels.Thenumber

ofreceivedframesis4247and4953respectively.Foraperiodofmorethan10seconds,the

amplituderesponsesofthetwosub-carriers−21and+21intheCSIareselectedfordisplay.

Thesetwosubcarrierarealsothepilotsubcarrierspecifiedinthe802.11protocol.From

Figure11,itcanbeseenthatthetrendoftheoverallmagnituderesponseisslowlychanging

exceptforthesuddendropandthesuddenincreasecausedbytheenvironmentalchange.

Wealsousemachinelearningmodelstoanalyzedataoff-line.SeenfromTable6wecan

seethat,regardlessofwhichmachinelearningmodelweuse,thecorrectrateisabove96%.

6.3 Resultanalysisofthecasestudy

Forthehardwareimplementationoftheidentificationmethod,thescenarioisasshownin

Figure13,where(A)showswhetherthepacketssentfromallsurroundingWiFidevices

Figure12 Adevicesubcarrieramplituderesponsecurveat5GHz

WorldWideWeb

Table6 Offlinecorrectrateof

identifyingdifferentWiFidevices

Models

Correctrate(%)

KNN

98.15

98.48

97.31

96.80

97.98

Linearregressionanalysis

Randomforest

Regressiontree

SVM

Cell

phone

Cell

phone

AP

AP

Cell

phone

Cell

phone

AP

AP

TickSEC

TickSEC

(a)

(b)

Figure13 Real-timehardwareidentificationofdifferentWiFidevices

Table7 Frequencyoffsetsfor

differentdevices

DeviceNo.

Framecount

avg.f

σ

Huawei

iPhone

Xiaomi

451

223

512

14.819

2.9401

2.8856

2.3449

−29.0859

9.8436

Table8 Real-timeidentification

ofthecorrectrateofdifferent

WiFidevices

Items

Identifyfromall

Identifyfrom2devices

Recvpackets

8756

6302

5899

83

Correctlyidentified

Falsepositives

Missedreports

Correctrate

7984

952

320

320

85.47%

10.87%

3.65%

93.61%

1.32%

5.08%

Falsealarmrate

Missingrate

WorldWideWeb

arefromthespecifieddevice,and(B)showsthatfromtwo“suspicious”WiFiThedevice

determineswhetheritisworththedevice.TheWiFichannelisChannel1(2.412GHz),and

allthedevicestobeidentifiedarecommercialdevicesunderrealenvironment.

Wemonitorthreedevicesandcollect1186trustableframesastrainingset.Thebrandsof

threedevicesareHuawei,iPhone,andXiaomirespectively.Thefrequencyoffsetstatistics

are as shown in Table 7. It can be seen that the frequency offset f between different

devicesisverylarge,andthestandarddeviationσ isnotasgreatasthedifferencesbetween

fs.Soitisreasonabletoidentifyingthedevicewiththeabovemethod.

ThesuccessrateoftherecognitionisshowninTable8.Itcanbeseenthatthesuccess

rateofidentifyingthedesignateddevicesfromall3devicesisabout85%,andthesuccess

rateofidentifyingthespecifieddevicesfromthetwodevicesreachesmorethan93%.

6.4 Performanceevaluation

Table9showstheresourceusageofTickSEC.Flip-Flopsandlook-uptables(LUTs)arethe

mainlogicresourcesoftheXilinx7seriesFPGAs.Flip-Flopscanbeusedasregisters.LUTs

canbeusedforlogicandstorage.CalledMemoryLUT.BRAM(BlockRAM)isthemain

storageresourceofXilinx7seriesFPGAs.MostFIFOsareimplementedusingBRAM,and

afewareimplementedusingDRAM(DistributeRAM).DRAMactuallyconsumesMemory

LUTresources.

WecanseethatTickSEChasincreasedtheuseofFlip-FlopresourcescomparedtoTick

butnotmuch.TheuseofotherresourcessuchasLUTandBRAMresourceshasactually

decreased,forthefollowingreasons:

–

TickSECusesmulti-levelregistercachingforframealignment,soitconsumesmore

Flip-Flop,butitisonlyasmallfractionoftheoriginalTickconsumption,soFlip-Flop

usageisnotmuchincreased;

–

LUThasasmalldecreasebecausetheRFandLowMACoftheoriginalTicksystem

arebothintheblockdesign.TickSECmovesthePHYlayertotheinsideoftheblock

design and encapsulated as an IP core, thus effectively reducing the LUT resources

consumedbytheconnectioninsideandoutside;

–

–

TickSECreducestheunnecessarydepthofsomeFIFOs,thusoptimizingtheusageof

BRAMandMemoryLUTs;

BUFG is used for clock division and deburring. The BUFG resource is decreased

becauseTickSECoptimizestheglobalclock.theBUFGsofthesamefrequencyclock

arecombinegenerated.

Table9 Resourceusageof

TickSECandoriginalTick

TickSEC

Used

originalTick

Used

Resource

%

%

Flip-Flop

LUT

82210

97894

4060

224

13.54

32.24

3.10

76781

98657

4551

224

12.65

32.50

3.48

MemoryLUT

I/O

32.00

25.63

10.82

43.75

32.00

30.97

10.50

53.12

BRAM

DSP48

BUFG

264

319

303

294

14

17

WorldWideWeb

Table10 LatencyoforiginalTicksystem

Framesize(bytes)

100

334

500

336

1000

382

1500

404

2000

415

3000

4000

489

Latency(μs)

449

Thenwetestthetransmissiondelay.Ifthedelayistoohigh,thetransmissionperfor-

mancewillbegreatlyaffected,andthetimeintervalreservedfortheuserwillbereduced.

Table10containstheend-to-endprocessingdelayoforiginalTicksystem[31].InTickSEC,

thedelayonlyincreasesbyabout65ns,becausethewell-designedhardwarelogicensures

thatthephysicallayerinformationisprepared.Themaintimespentisforreadingmultiple

setsofAXIregisters,thecostisnegligible.

Combinedwiththetestresults,TickSECcanextractthephysicallayerinformationeffec-

tively,andprovidesavarietyofcommonphysicallayerinformationunderthepremiseof

occupyinglessresources.

7 Conclusion

WeproposeaplatformforusingPHYlayerinformationtoverifysecurityauthentication.

TheresultsfromevaluationshowthatTickSECisefficientandeffectiveinextractingPHY

layerinformation.ItprovidesavarietyofcommonPHYlayerinformationunderthepremise

of low resource consumption and low impact on performance. The case study demon-

stratesTickSEC’svalueinpracticalsecurityauthentication.Ingeneral,TickSECcanmeet

theneedsofWiFisecurityresearchesasaverificationplatform.Weappliedthemachine

learningapproachtotheTickSEC,andweplantoaddintelligence-relatedfeaturesinthe

future.

Acknowledgements

The work is funded by National Key Research and Development Plan of China

(2017YFB0801702)andkeyresearchprojectofNationalNaturalScienceFoundation(No.61531004).

Publisher’snote SpringerNatureremainsneutralwithregardtojurisdictionalclaimsinpublishedmaps

andinstitutionalaffiliations.

References

1. Scikit-learn.(2007)

2. Cyusb3acc-005 fmc interconnect board. kits-

boards/cyusb3acc-005-fmc-interconnect-board-ez-usb-fx3-superspeed(2014)

3. Cyusb3kit-003 superspeed explorer kit. kits-

boards/cyusb3kit-003-ez-usb-fx3-superspeed-explorer-kit(2014)

4. Ad9361.

(2018)

5. Xilinx kc705 evaluation board.

(2018)

6. Bagci, I.E., Roedig, U., Martinovic, I., Schulz, M., Hollick, M.: Using channel state information for

tamper detection in the internet of things. In: Proceedings of the 31st Annual Computer Security

ApplicationsConference.ACM,pp.131–140(2015)

7. Blossom,E.:GNURadio:toolsforexploringtheradiofrequencyspectrum.Linuxjournal2004(122),4

(2004)

WorldWideWeb

8. Brik,V.,Banerjee,S.,Gruteser,M.,Oh,S.:Wirelessdeviceidentificationwithradiometricsignatures.In:

Proceedingsofthe14thACMInternationalConferenceonMobileComputingandNetworking.ACM,

pp.116–127(2008)

9. Faria,D.B.,Cheriton,D.R.:Detectingidentity-basedattacksinwirelessnetworksusingsignalprints.In:

Proceedingsofthe5thACMWorkshoponWirelessSecurity.ACM,pp.43–52(2006)

10. Fortune,S.J.,Gay,D.M.,Kernighan,B.W.,Landron,O.,Valenzuela,R.A.,Wright,M.H.:Wisedesignof

indoorwirelesssystems:practicalcomputationandoptimization.IEEEComput.Sci.Eng.2(1),58–68

(1995)

11. Fuhrmann, D.R., Antonio, G.S.: Transmit beamforming for mimo radar systems using partial signal

correlation.IEEETransaerospelectronsyst44(1),1–16(2008)

12. Han,S.H.,Lee,J.H.:Anoverviewofpeak-to-averagepowerratioreductiontechniquesformulticarrier

transmission.IEEEWirel.Commun.12(2),56–65(2005)

13. Huang,J.,Albazrqaoe,W.,Xing,G.:Blueid:aPracticalSystemforBluetoothDeviceIdentification.In:

INFOCOM,2014ProceedingsIEEE.IEEE,pp.2849–2857(2014)

14. Jana,S.,Kasera,S.K.:Onfastandaccuratedetectionofunauthorizedwirelessaccesspointsusingclock

skews.IEEETrans.Mob.Comput.9(3),449–462(2010)

15. Joachims,T.:Textcategorizationwithsupportvectormachines:learningwithmanyrelevantfeatures.

In:Europeanconferenceonmachinelearning.Springer,pp.137–142(1998)

16. Kalamandeen,A.,Scannell,A.,deLara,E.,Sheth,A.,Lamarca,A.:Ensemble:cooperativeproximity-

basedauthentication.In:Proceedingsofthe8thInternationalConferenceonMobileSystems,Applica-

tions,andServices.ACM,pp.331–344(2010)

17. Khattab,A.,Camp,J.,Hunter,C.,Murphy,P.,Sabharwal,A.,Knightly,E.W.:WARP:aflexibleplatform

for clean-slate wireless medium access protocol design. ACM SIGMOBILE Mobile Computing and

CommunicationsReview12(1),56–58(2008)

18. Li, X.: A verification platform for WiFi physical layer security research. Master’s thesis, Peking

University,Beijing(2017)

19. Liaw,A.,Wiener,M.,etal.:Classificationandregressionbyrandomforest.Rnews2(3),18–22(2002)

20. Liu,F.J.,Wang,X.,Tang,H.:Robustphysicallayerauthenticationusinginherentpropertiesofchannel

impulseresponse.In:MilitaryCommunicationsConference,2011-MILCOM2011.IEEE,pp.538–542

(2011)

21. Liu,F.J.,Wang,X.,Primak,S.L.:AtwodimensionalquantizationalgorithmforCIR-basedphysical

layer authentication. In: 2013 IEEE International Conference on Communications (ICC). IEEE, pp.

4724–4728(2013a)

22. Liu, H., Wang, Y., Yang, J., Chen, Y.: Fast and practical secret key extraction by exploiting channel

response.In:INFOCOM,2013ProceedingsIEEE.IEEE,pp.3048–3056(2013b)

23. Liu, H., Wang, Y., Liu, J., Yang, J., Chen, Y.: Practical user authentication leveraging channel state

information (CSI). In: Proceedings of the 9th ACM Symposium on Information, Computer and

CommunicationsSecurity.ACM,pp.389–400(2014)

24. Mao,Y.,Zhang,Y.,Zhong,S.:Stemmingdownlinkleakagefromtrainingsequencesinmulti-userMIMO

networks.In:Proceedingsofthe2016ACMSIGSACConferenceonComputerandCommunications

Security.ACM,pp.1580–1590(2016)

25. Olive,D.J.:Linearregressionanalysis.Technometrics45(4),362–363(2003)

26. Quinlan,J.R.:Inductionofdecisiontrees.Mach.Learn.1(1),81–106(1986)

27. Release,M.:Themathworks.Inc,Natick,Massachusetts,UnitedStates488(2013)

28. Schmogrow, R., Nebendahl, B., Winter, M., Josten, A., Hillerkuss, D., Koenig, S., Meyer, J.,

Dreschmann,M.,Huebner,M.,Koos,C.:Errorvectormagnitudeasaperformancemeasureforadvanced

modulationformats.IEEEPhoton.Technol.Lett.24(1),61–63(2011)

29. Van de Beek, J.J., Sandell, M., Borjesson, P.O.: Ml estimation of timeand frequency offset in ofdm

systems.IEEETrans.SignalProcess.45(7),1800–1805(1997)

30. Winterstein,F.,Bayliss,S.,Constantinides,G.A.:High-levelsynthesisofdynamicdatastructures:acase

studyusingvivadohls.In:InternationalConferenceonField-ProgrammableTechnology,pp.362–365

(2013)

31. Wu,H.,Wang,T.,Yuan,Z.,Peng,C.,Li,Z.,Tan,Z.,Ding,B.,Li,X.,Li,Y.,Liu,J.,etal.:Thetick

programmablelow-latencysdrsystem.In:Proceedingsofthe23rdAnnualInternationalConferenceon

MobileComputingandNetworking.ACM,pp.101–113(2017)

32. Xi,W.,Li,X.,Qian,C.,Han,J.,Tang,S.,Zhao,J.,Zhao,K.:KEEP:Fastsecretkeyextractionprotocol

forD2Dcommunication.In:2014IEEE22ndInternationalSymposiumofQualityofService(IWQoS).

IEEE,pp.350–359(2014)

33. Xiao,L.,Greenstein,L.,Mandayam,N.,Trappe,W.:Fingerprintsintheether:usingthephysicallayer

forwirelessauthentication.In:IEEEInternationalConferenceonCommunications.IEEE,pp.4646–

4651(2007)

WorldWideWeb

34. Xiao,L.,Reznik,A.,Trappe,W.,Ye,C.,Shah,Y.,Greenstein,L.,Mandayam,N.:PHY-authentication

protocol for spoofing detection in wireless networks. In: Global Telecommunications Conference

(GLOBECOM2010),2010IEEE.IEEE,pp.1–6(2010)

35. Xiong, J., Jamieson, K.: Securearray: improving wifi security with fine-grained physical-layer infor-

mation. In: Proceedings of the 19th Annual International Conference on Mobile Computing and

Networking.ACM,pp.441–452(2013)

36. Yang,J.,Chen,Y.,Trappe,W.,Cheng,J.:Detectionandlocalizationofmultiplespoofingattackersin

wirelessnetworks.IEEETrans.ParallelDistrib.Syst.24(1),44–58(2013)

37. Zeng,K.,Govindan,K.,Mohapatra,P.:Non-cryptographicauthenticationandidentificationinwireless

networks [security and privacy in emerging wireless networks]. IEEE Wirel. Commun. 17(5), 56–62

(2010)

38. Zhang, M.L., Zhou, Z.H.: Ml-knn: a lazy learning approach to multi-label learning. Pattern Recogn.

40(7),2038–2048(2007)