Dimensional Reduction Analysis for Physical Layer Device Fingerprints with Application to ZigBee and Z-Wave Devices

Authors:

Trevor J. Bihl

Michael A. Temple

Kenneth W. Bauer

Benjamin Ramsey

US Air Force Institute of Technology

Wright-Patterson AFB OH

26-28 Oct 2015

Overview

- **Problem Statement**
- **Background/Setup**
  - **ZigBee and Z-Wave Devices**
- **Methodology**
  - **RF-DNA Fingerprinting Feature Generation**
  - **GRLVQI Device Discrimination**
  - **Dimensional Reduction Analysis (DRA)**
  - **p-value vs Test Statistic DRA**
- **Results**
  - **Classification and Verification Results**
- **Future Work**
  - **Extend to Additional Classifiers**
  - **Develop Additional DRA Methods for RF Fingerprinting**

Problem Statement

The AFIT of Today is the Air Force of Tomorrow.

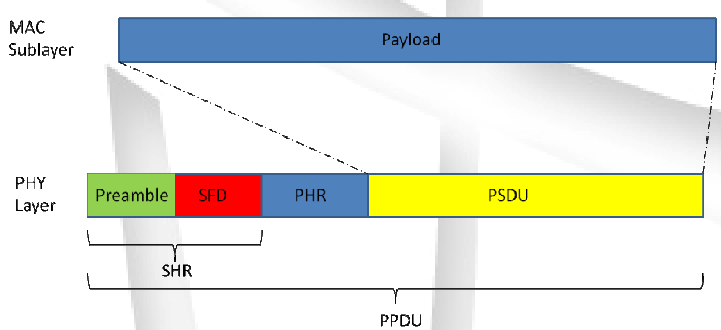
Investigate Suitability of p-Values and Test Statistic Based Dimensional Reduction Analysis (DRA) Methods for Device Fingerprinting Using Radio Frequency Distinct Native Attribute (RF-DNA) Features.

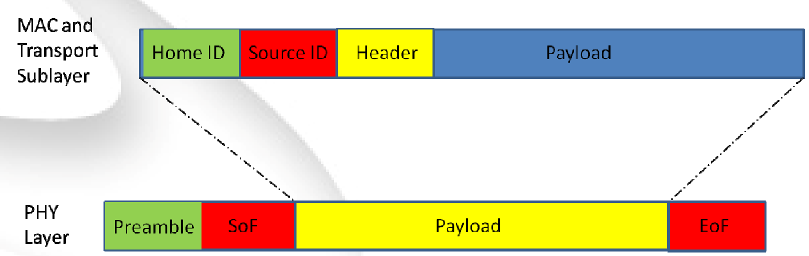
Background

ZigBee & Z-Wave Devices

The AFIT of Today is the Air Force of Tomorrow.

	ZigBee	Z-Wave
Standard	IEEE	Proprietary
Frequency	2.4 GHz	906 MHz
Bit Rate	250 Kbits/s	40 Kbits/s
Security	IEEE 802.15.4 Standard	None: 200 and 300 Series AES 128: 400 Series
Latency	50 to 100 mSec	~1000 mSec
Range	10 to 100 m	30 to 100 m
Message Size (Bytes)	127 (max)	64 (max)



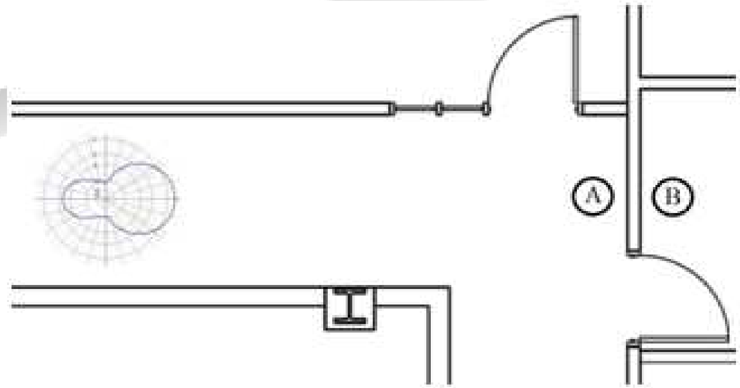


Methodology

ZigBee Emission Processing [2, 13, 14]

The AFIT of Today is the Air Force of Tomorrow.

- **Experimentally Collected ZigBee Emissions**
  - **10 Like-Model Devices**
- **Collection Environments**
  - **CAGE – Anechoic Chamber**
  - **LOS – Hallway Line-of-Sight (LOS)**
  - **WALL – Through Wall Propagation**
- **Authorized Devices**
  - **Emissions Collected in CAGE, LOS, & WALL for 4 of 10 Devs (Dev 1 – Dev 4)**
  - **N_C = 4 Like-Model Auth Devs, Different Ser #s**
- **Rogue Devices**
  - **N_{Rog} = 9 Like-Model Rogue Devs, Different Ser #s (Dev 5 – Dev 10)**
  - **Emissions Collected in Selected Environments (See Table)**



ZigBee Experimental Collection Setup for LOS (A) & WALL (B) Environment Emissions [19,54]

ZigBee ID	CAGE	LOS	WALL
Dev5		X	X
Dev6		X	X
Dev7		X	X
Dev8	X		
Dev9	X		
Dev10	X		

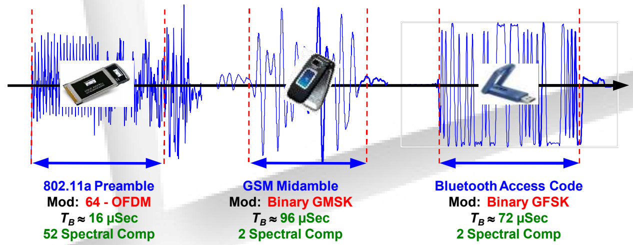
ZigBee Rogue Device ID and Collection Environments [19,54]

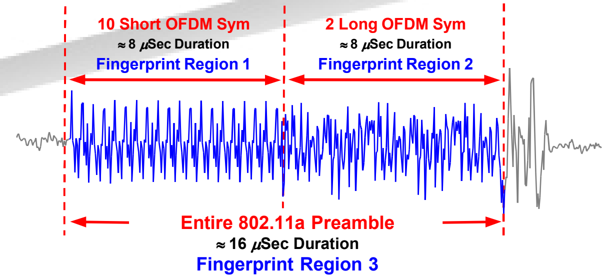
Methodology

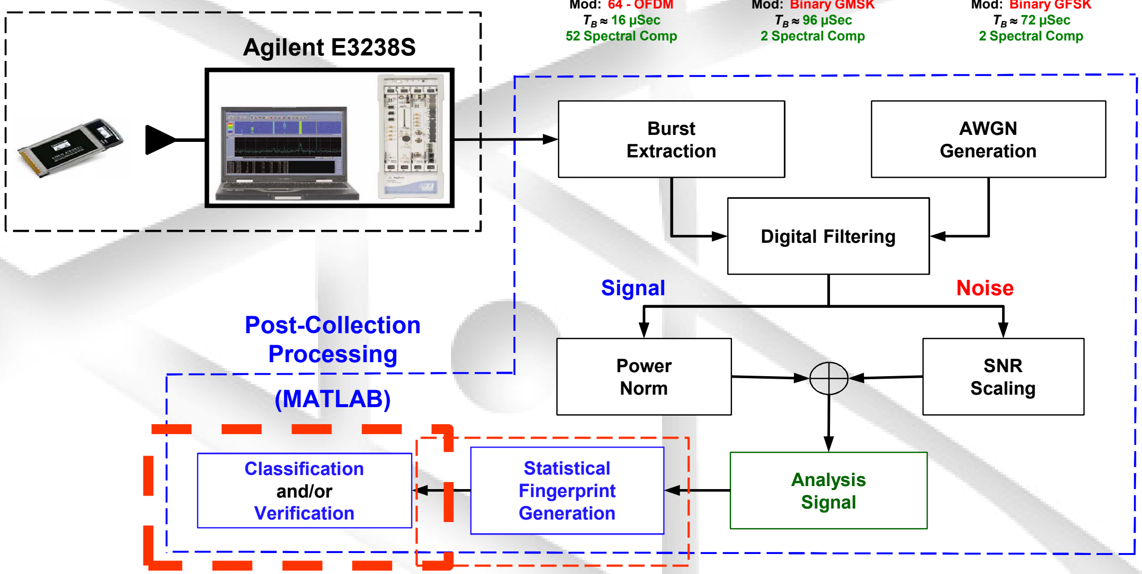
AFIT's RF-DNA Fingerprinting Process [7]

The AFIT of Today is the Air Force of Tomorrow.

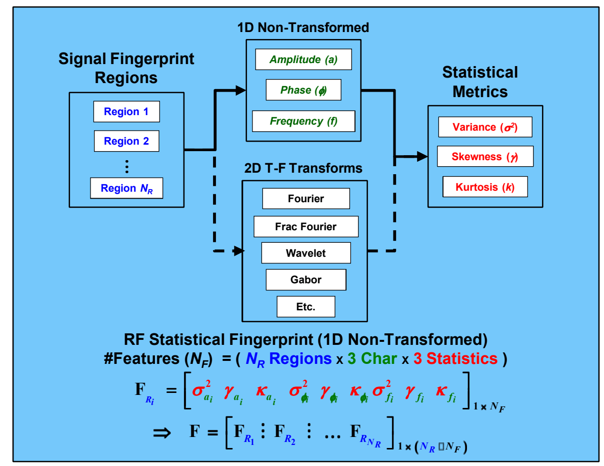
(A) Agilent E3238S (RFSICS)
(A) Nat'l Instruments (NI)
(B) Riscure Inspector



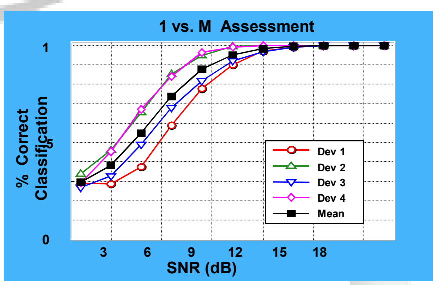




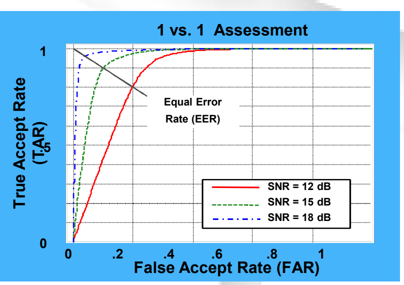
RF Statistical Fingerprint Generation



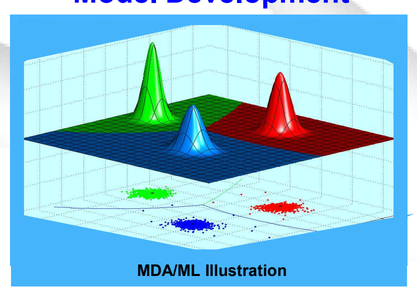
Device Classification



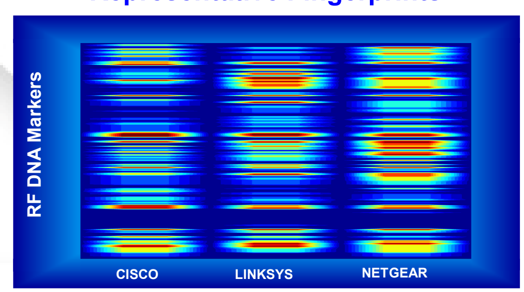
ROC Verification



Model Development



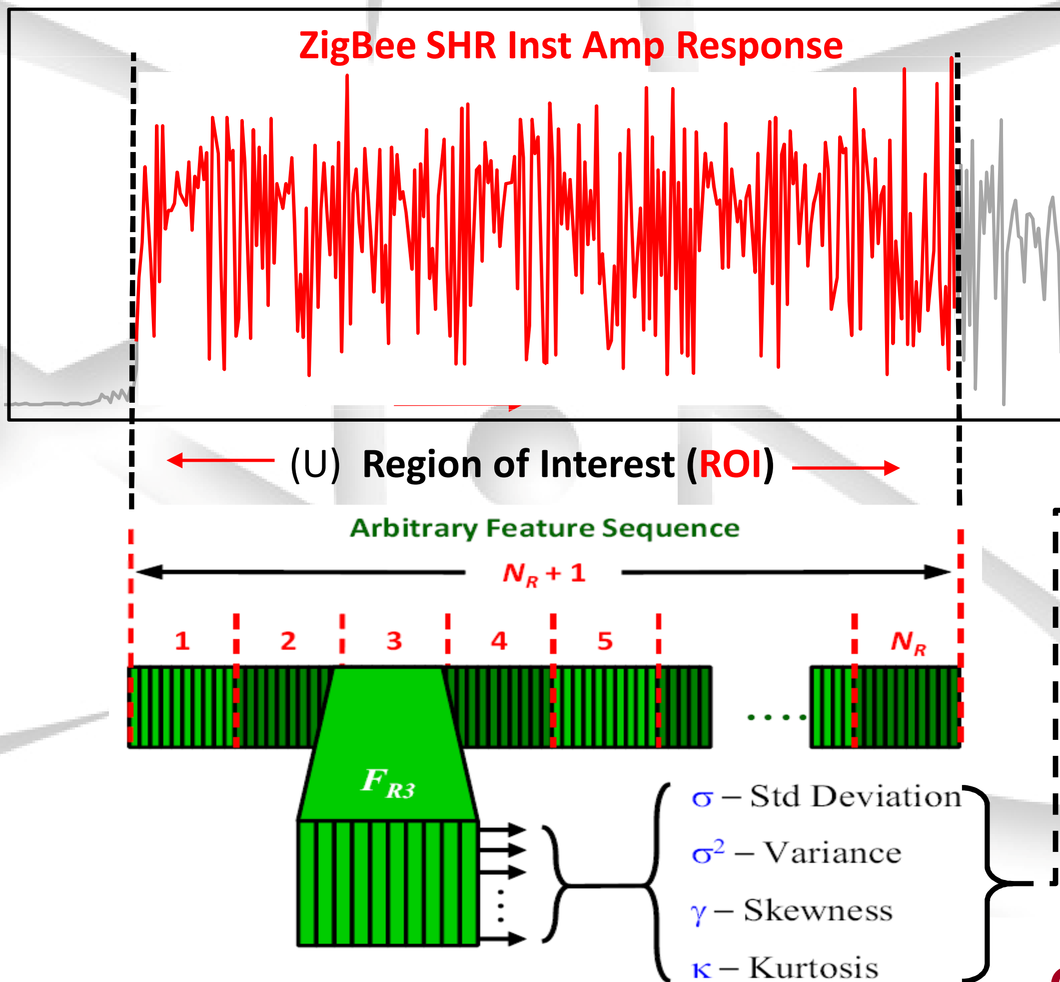
Representative Fingerprints



Methodology

ZigBee Emission Processing [2, 13, 14]

Time Domain (TD) RF-DNA Fingerprint Generation



Non-Transformed Instantaneous:

(a) Amplitude

(b) Phase

(c) Frequency

$$\mathbf{F}_{R_i} = \begin{bmatrix} \sigma_i & \sigma_i^2 & \gamma_i & \kappa_i \end{bmatrix}_{1\times 4}^{i^{\text{th}}\,\text{Region}}$$

Composite Fingerprint

$$\begin{bmatrix} \mathbf{F}_{R_1} \vdots \mathbf{F}_{R_2} \vdots \cdots \vdots \mathbf{F}_{R_{N_R}} \end{bmatrix}_{1\times 4\times N_R}$$

Fingerprints Input to

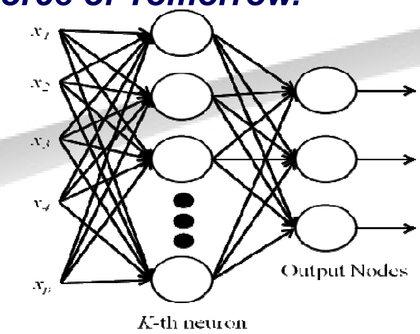
Classifier Model Development

Methodology

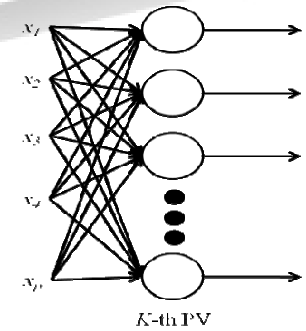
Device Classification: GRLVQI

The AFIT of Today is the Air Force of Tomorrow.

- **LVQ-Based Classifiers**
  - Gradient Descent & Prototype Vector (PV) Approach for Classification
  - Gradient = 1st Derivative of Cost Function
  - Iteratively Examines PV-to-Data Distances
    - Correctly Classified PVs … Move Toward data
    - Incorrectly Classified PVs … Move Away From Data
- **GRLVQI … LVQ Extension [2, 9, 14]**
  - G = *Generalized* … Sigmoidal Cost Function
  - R = *Relevance* … Gradient Descent Feature Relevance Ranking
  - I = *Improved* … Improved Logic, PV Freq, Add'l Learn Rate, Etc.
- **No Explicit *Assumption* / *Knowledge* Required for Data Distribution (PDF)**
  - Appropriate PV Initialization Required
  - Normal PVs ⇒ Standardized Data

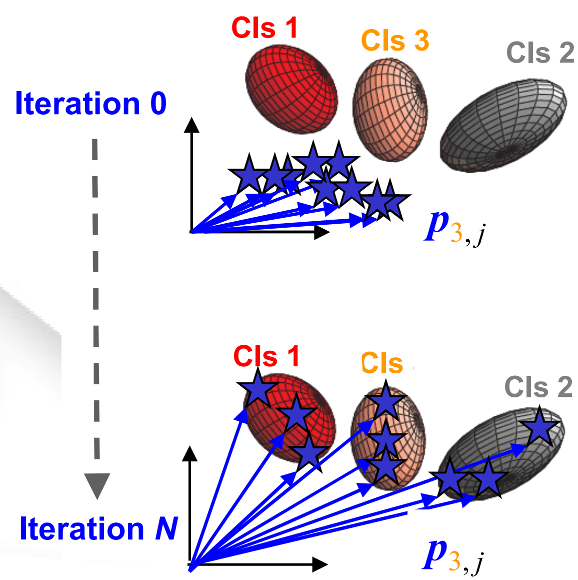


Artificial Neural Net (ANN)



Learning Vector Quant. (LVQ)

LVQ Update



Methodology

Dimensional Reduction Analysis (DRA)

The AFIT of Today is the Air Force of Tomorrow.

- **Method #1:** ***(Distribution Based)*: Two Sample Kolmogorov–Smirnov (KS) [13,14, 17]**

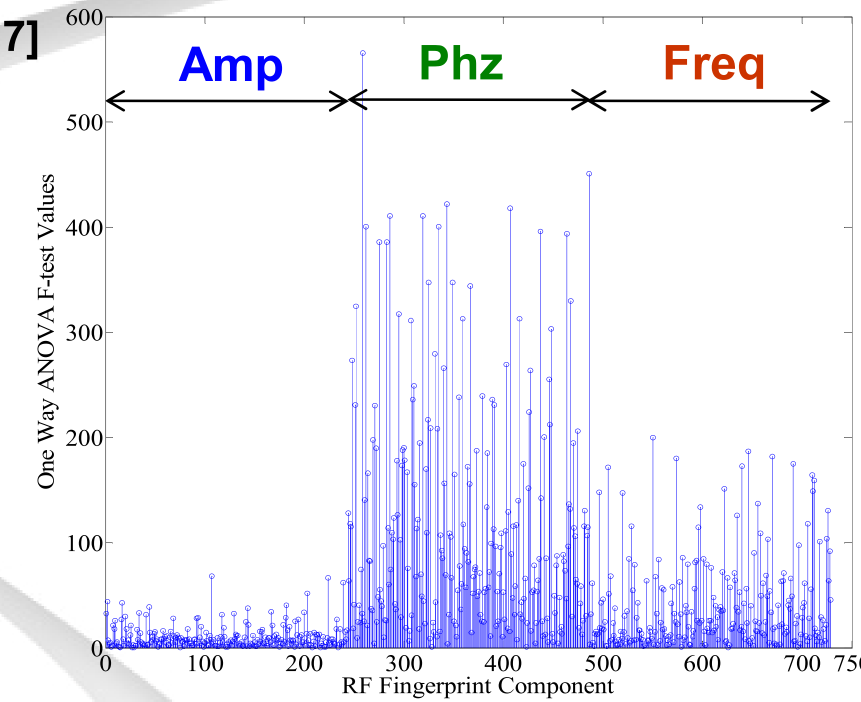
$$KS = \max\left(\left|F_1(x) - F_2(x)\right|\right)$$

- **Method #2:** ***(Distribution Based)*: ANOVA F-Statistics** [18]

$$F_{0(i)} = \frac{MS_{Feature(i)}}{MSE_{Model(i)}}$$

- **Method #3:** ***(Classifier Based) GRLVQI Relevance*** [9]

- **Method #4:** ***Dimensionality Assessment*** [18, 21]



Amplitude (*a*) : ZigBee Feats #1 - #243
Phase (ϕ) : ZigBee Feats #244 - #486
Frequency (*f*) : ZigBee Feats #487 - #729

Methodology

DRA: Dimensionality Assessment

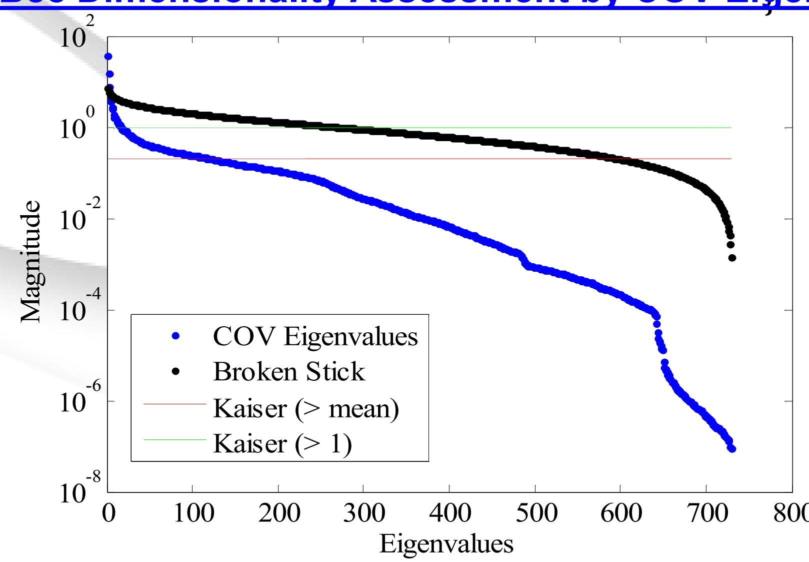
The AFIT of Today is the Air Force of Tomorrow.

- **Selecting quantity of features in subsets non-trivial**
- ***Qualitative* DRA**
  - ***Previously Considered [13,14]***
  - $N_{DRA,\ ZigBee}$ **= [25, 50, 243]**
- ***Quantitative* DRA**
  - **Introduced Here**
  - **Removes Subjectively**
  - **Intrinsic Data Dimensionality**
- **P-value and Data Eigenvalue methods considered**
  - **P-values Overestimate Required** N_{DRA}
  - **Data Eigenvalue Methods Yield** N_{DRA} **Consistent with Prior Work**
  - $N_{DRA,\ ZigBee}$ **= [17, 123]**
  - $N_{DRA,\ Z\text{-}wave}$ **= [7, 34]**

ZigBee Dimensionality Assessment by Significance Level

SNR (dB)	Method	Significance Level 0.1%	1%	5%	10%
0	F-TEST	196	264	350	402
	KS-TEST (ΣP-VALUES)	37	74	130	160
10	F-TEST	589	639	674	688
	KS-TEST (ΣP-VALUES)	337	414	512	557
18	F-TEST	706	713	720	722
	KS-TEST (ΣP-VALUES)	666	692	711	716
30	F-TEST	718	725	727	728
	KS-TEST (ΣP-VALUES)	727	729	729	729

ZigBee Dimensionality Assessment by COV Eigenvalues



Methodology

DRA: Test Statistics vs p-Values

The AFIT of Today is the Air Force of Tomorrow.

- **Recent RF-DNA DRA Research Focused on p-values for feature relevance ranking** [1, 2, 13-14, 28-29]
  - **Test Statistic to p-Value Conversion Req'd**
- **Computing Test Statistic Values**
  - **Ratio between quantities or a simple relationship**
- **Test Statistics vs. P-Values**
  - **p-Values Represent Area Under a Probability Curve**
- **Computing p-Values Requires** [26]

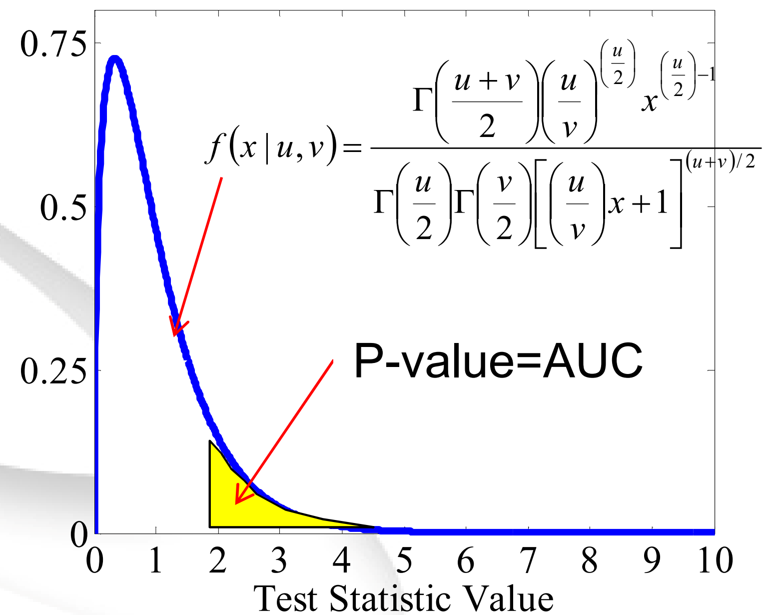
1. Stated Hypothesis Test
2. Test Statistic Value
3. Degrees of Freedom
4. Distributional Assumption
5. Reference Distribution

(Not all are always considered / stated in DRA, e.g. [1, 2, 13, 14])

- **The mapping between test statistic and *p*-value is typically nonlinear**
- **Simple F-Test Stat.** [18]

$$F_{0(i)} = \frac{MS_{Feature(i)}}{MSE_{Model(i)}}$$

- **Complicated F-Test p-value** [18]



- **The KS-test involves a similar nonlinear mapping** [17]

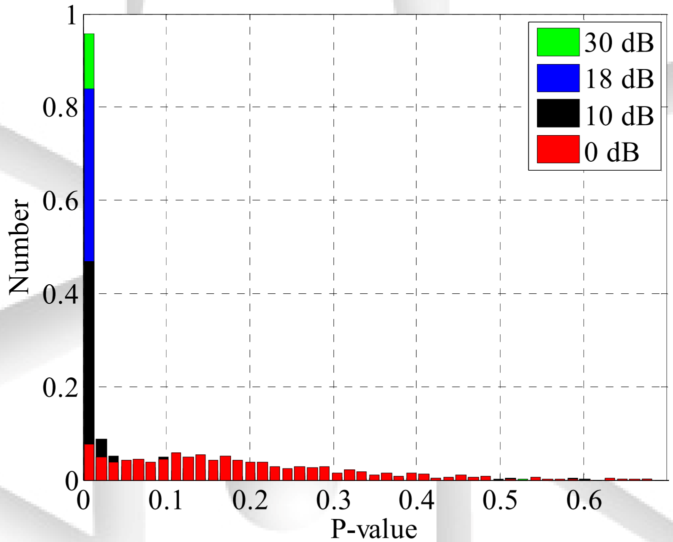
Methodology

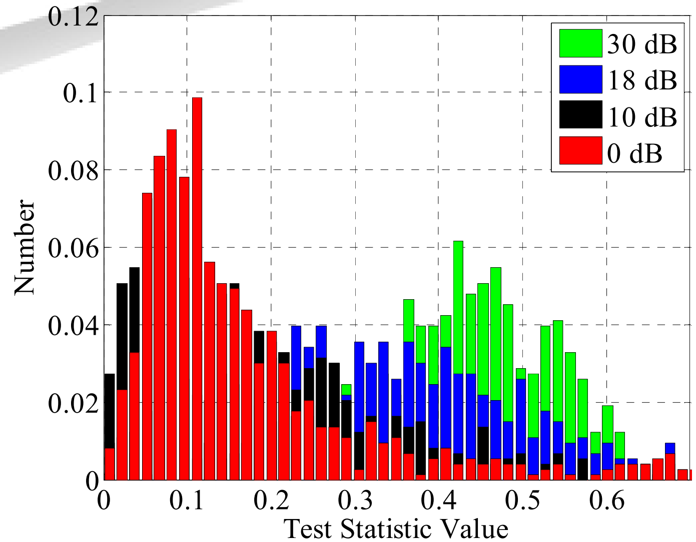
ZigBee DRA: Test Statistics vs P-Values

The AFIT of Today is the Air Force of Tomorrow.

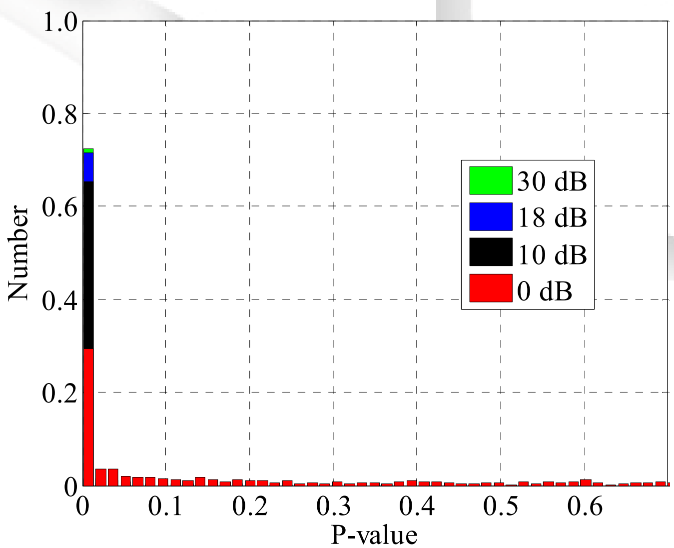
p-values | **Test Statistic Values**

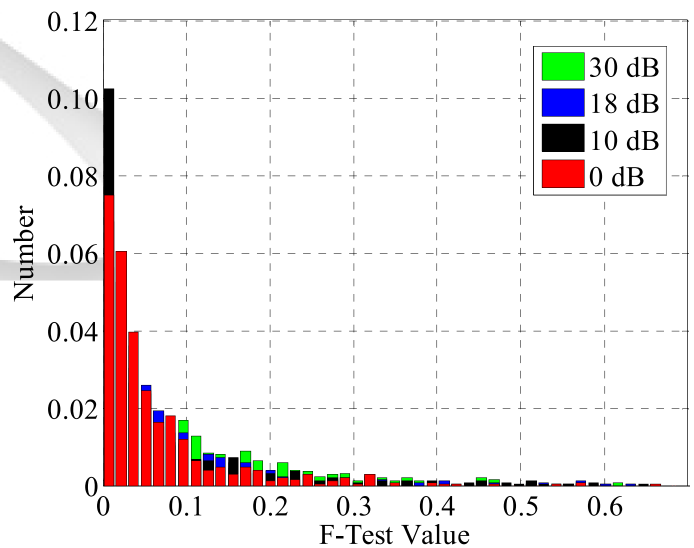
KS-test





F-test





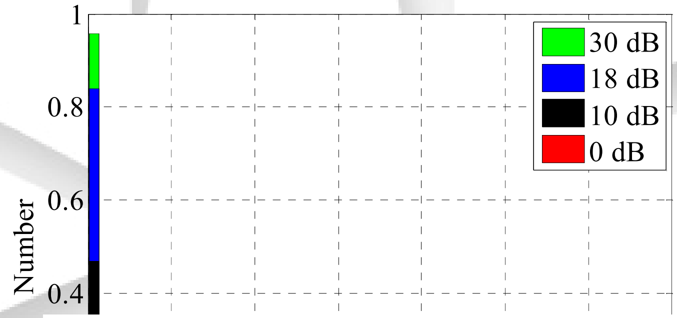
Methodology

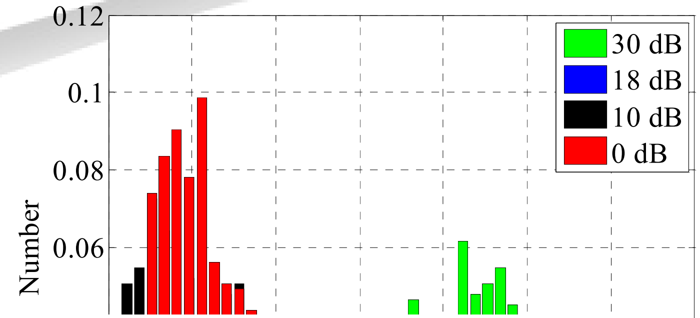
ZigBee DRA: Test Statistics vs P-Values

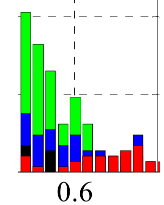
The AFIT of Today is the Air Force of Tomorrow.

p-values | **Test Statistic Values**

KS-test

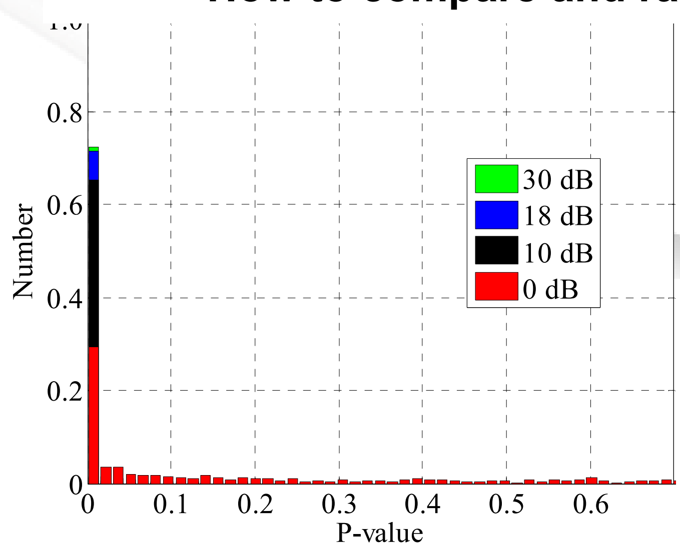


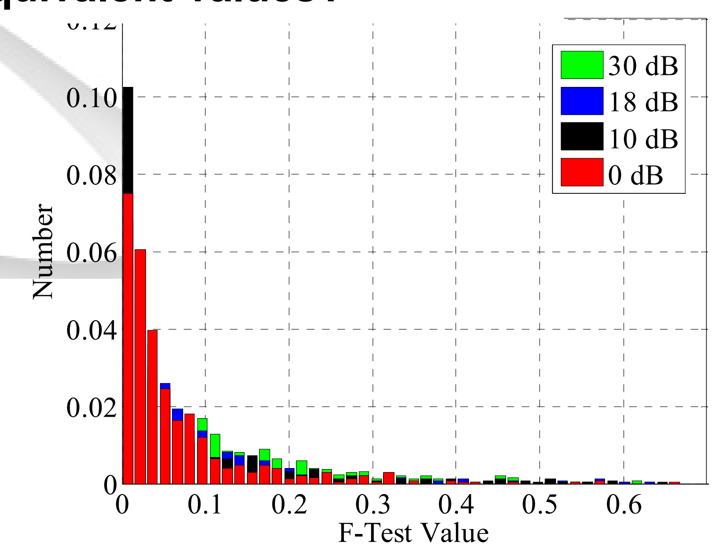




- **With large datasets, p-values tend towards zero**
  - **Hence resolution is lost when converting to p-values**
- **Interpretation/procedural issues also remain**
  - **How to compare and rank equivalent values?**

F-test



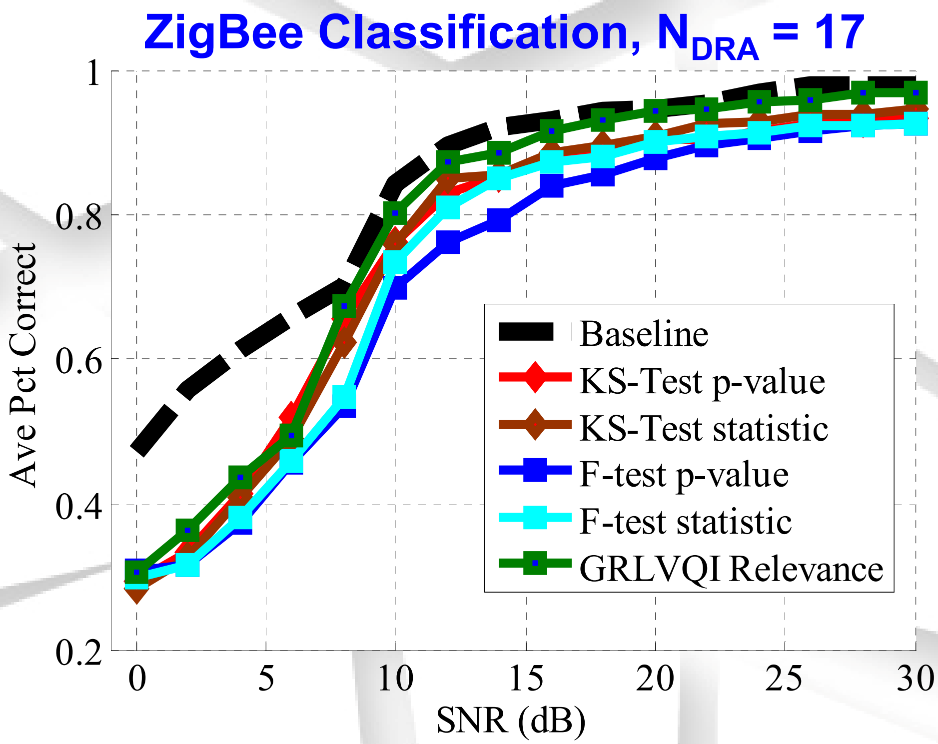


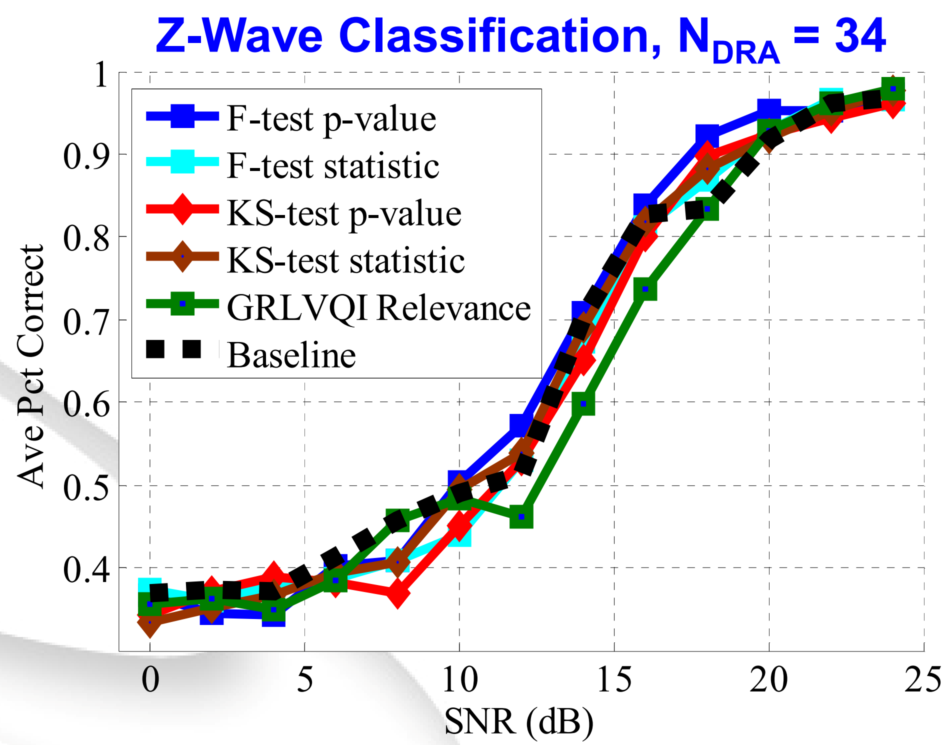
Results

Device Classification: ZigBee & Z-Wave

The AFIT of Today is the Air Force of Tomorrow.

- Test statistic methods offer comparable or better performance to *p*-value based methods





Results

Device ID Verification: ZigBee

- Based on "one vs one" claimed identity scenarios
- Presented as:
  - *%TVR = True Verification Rate*
  - *% RRR = Rogue Rejection Rate*
  - Bold Entry - Best or Statistically Equivalent Performance

DRA Method	KS test Statistic			KS ΣP-value		
N_F	***17***	***50***	***123***	***17***	***50***	***123***
TVR	0%	0%	0%	0%	0%	0%
RRR	8.33%	8.33%	0%	**52.8%**	2.78%	0%
DRA Method	F Test Statistic			F Test P-value		
N_F	***17***	***50***	***123***	***17***	***50***	***123***
TVR	0%	0%	0%	**25%**	0%	0%
RRR	8.33%	5.56%	0%	38.9%	19.4%	0%
DRA Method	GRLVQI					
N_F	***17***	***50***	***123***			
TVR	**25%**	**50%**	**50%**			
RRR	**52.8%**	**66.7%**	**72.2%**			

Results

Device ID Verification: ZigBee

The AFIT of Today is the Air Force of Tomorrow.

- Based on “one vs one” claimed identity scenarios
- Presented as:
  - *%TVR = True Verification Rate*
  - *% RRR = Rogue Rejection Rate*
  - Bold Entry - Best or Statistically Equivalent Performance

DRA METHOD	KS TEST STATISTIC			KS ΣP-VALUE		
N_F	***17***	***50***	***123***	***17***	***50***	***123***

- **Distribution-based DRA offers poor verification performance with non-linear GRLVQI classifier**

DRA METHOD	F TEST STATISTIC			F TEST P-VALUE		
N_F	***17***	***50***	***123***	***17***	***50***	***123***
TVR	0%	0%	0%	**25%**	0%	0%
RRR	8.33%	5.56%	0%	38.9%	19.4%	0%

DRA METHOD	GRLVQI		
N_F	***17***	***50***	***123***
TVR	**25%**	**50%**	**50%**
RRR	**52.8%**	**66.7%**	**72.2%**

Conclusions & Future Work

Conclusions

- **Introduction of F-test for DRA in RF Fingerprinting**
- **Test Statistic Methods vs *P*-values**
  - ***P*-values Susceptible to Converge on 0** [26]
  - **Test Statistic DRA Offers Robustness**
- **Introduction Quantitative Dimensionality Assessment**
  - **N_{DRA} = 123 (quantitative) better than N_{DRA} = 243 (qualitative) of [14]**
- **Comparison of 5 DRA Methods for RF Fingerprinting**
- **First Look RF-DNA Fingerprinting Using Z-Wave Devices**

Future Work

- **Expand Z-Wave Assessments to Include Rogue Devices**
- **Reevaluate with an MDA-based classifier**

References

The AFIT of Today is the Air Force of Tomorrow.

[1] B. W. Ramsey, B. E. Mullins, R. Speers and K. A. Batterton, "Watching for weakness in wild WPANs," *Military Comm. Conf. (MILCOM),* pp. 1404-1409, 2013.

[2] B. W. Ramsey, M. A. Temple and B. E. Mullins, "PHY foundation for multi-factor ZigBee node authentication," *IEEE Global Comm. Conf. (GLOBECOM),* pp. 795-800, 2012.

[3] Y. Zatout, "Using wireless technologies for healthcare monitoring at home: A survey," *Int. Conf. e-Health Networking, Applicat. and Services (Healthcom),* pp. 383-386, 2012.

[4] J. Wright, "KillerBee: Practical ZigBee exploitation framework," in *11th ToorCon Conf.*, San Diego, 2009.

[5] Y. Sheng, K. Tan, G. Chen, D. Kotz and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," *27th Conf. on Comput. Comm.,* 2008.

[6] B. Danev, D. Zanetti and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys,* vol. 45, no. 1, 2012.

[7] W. E. Cobb, E. W. Garcia, M. A. Temple, R. O. Baldwin and Y. C. Kim, "Physical layer identification of embedded devices using RF-DNA fingerprinting," *Military Comm. Conf. (MILCOM),* pp. 2168-2173, 2010.

[8] M. D. Williams, M. A. Temple and D. R. Reising, "Augmenting bit-level network security using physical layer RF-DNA fingerprinting," *IEEE Global Comm. Conf. (GLOBECOM),* pp. 1-6, 2010.

[9] P. K. Harmer, D. R. Reising and M. A. Temple, "Classifier selection for physical layer security augmentation in Cognitive Radio networks," *IEEE Int. Conf. on Comm.(ICC),* pp. 2846-2851, 2013.

[10] T. Wu, J. Duchateau, J.-P. Martens and D. van Compernolle, "Feature subset selection for improved native accent identification," *Speech Comm.,* vol. 52, no. 2, pp. 83-98, 2010.

References

The AFIT of Today is the Air Force of Tomorrow.

[11] A.-C. Haury, P. Gestraud and J.-P. Vert, "The Influence of Feature Selection Methods on Accuracy, Stability and Interpretability of Molecular Signatures," *PLoS ONE,* vol. 6, no. 12, 2011.

[12] T. Kind, V. Tolstikov, O. Fiehn and R. H. Weiss, "A comprehensive urinary metabolomic approach for identifying kidney cancer," *Analytical Biochemistry,* vol. 363, 2007.

[13] C. K. Dubendorfer, B. W. Ramsey and M. A. Temple, "An RF-DNA verification process for ZigBee networks," *Military Comm. Conf. (MILCOM),* pp. 1-6, 2012.

[14] C. K. Dubendorfer, B. W. Ramsey and M. A. Temple, "ZigBee device verification for securing industrial control and building automation systems," *Int. Conf. on Critical Infrastructure Protection (IFIP13),* vol. 417, pp. 47-62, 2013.

[15] S. Prabhakar, S. Pankanti and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security and Privacy,* pp. 33-42, March/April 2003.

[16] A. K. Jain, R. P. Duin and J. Mao, "Statistical Pattern Recognition: a Review," *IEEE Trans. on Pattern Anal. Mach. Intell.,* vol. 22, no. 1, pp. 4-37, Jan. 2000.

[17] W. J. Conover, *Practical Nonparametric Statistics*, 2nd ed., New York: John Wiley & Sons, pp. 344-385, 1980.

[18] W. R. Dillon and M. Goldstein, *Multivariate Analysis Methods and Applications*, New York: John Wiley & Sons, 1984.

[19] J. D. Habbema and J. Hermans, "Selection of variables in discriminant analysis by F-statistic and error rate," *Technometrics,* vol. 19, no. 4, pp. 487-493, 1977.

[20] M. Cowles and C. Davis, "On the Origins of the .05 Level of Statistical Significance," *Amer. Psychologist,* vol. 37, no. 5, pp. 553-558, 1982.

References

[21] R. J. Johnson, J. P. Williams and K. W. Bauer, "AutoGAD: An improved ICA-based hyperspectral anomaly detection algorithm," *IEEE Trans. Geosci. Remote Sens.,* vol. 51, no. 6, pp. 3492-3503, 2013.

[22] C. J. Huberty and J. M. Wisenbaker, "Variable importance in multivariate group comparisons," *J. of Education Stat.,* vol. 17, no. 1, pp. 75-91, 1992.

[23] A. Cord, C. Ambroise and J.-P. Cocquerez, "Feature selection in robust clustering based on Laplace mixture," *Pattern Recognition Lett.,* vol. 27, no. 6, pp. 627-635, 2006.

[24] P. Radivojac, Z. Obradovic, A. K. Dunker and S. Vucetic, "Feature selection filters based on the permutation test," *Mach. Learning: ECML 2004,* pp. 334-346, 2004.

[25] K. Schmidt, T. Behrens and T. Scholten, "Instance selection and classification tree analysis for large spatial datasets in digital soil mapping," *Geoderma,* vol. 146, no. 1-2, pp. 138-146, 2008.

[26] L. G. Halsey, D. Curran-Everett, S. L. Vowler and G. B. Drummond, "The fickle P value generates irreproducible results," *Nature Methods,* vol. 12, no. 3, pp. 179-185, 2015.