Realizing Physical Layer Authentication Using Constellation Perturbation on a Software-defined Radio Testbed

Ashwin Amanna*, Anu Saji*, James Bohl* and Arun Subramanian†
*ANDRO Advanced Applied Technology, ANDRO Computational Solutions, LLC, Rome NY,
{aamanna, asaji, jbohl}@androcs.com
†GE Global Research, San Ramon, CA,
arun.subramanian1@ge.com

***Abstract*—Ensuring secure command and control in a tactical military environment is vital as the combat forces face many potentially sophisticated adversaries who seek out the vulnerabilities in the communications infrastructure. Although authentication schemes has been substantially explored, the ability of new techniques to coexist with existing system (i.e., *legacy* systems) is often overlooked. The objective of this work is to establish feasibility of a physical (PHY) layer authentication technique that can be implemented easily to coexist with legacy systems. In this paper, we discuss the implementation of a PHY layer authentication scheme that can seamlessly integrate within systems containing legacy receivers, which do not have the ability to decode PHY layer authentication tags. To this end, we design and evaluate a quadrature phase shift keying (QPSK) and $\pi/4$ Differential quadrature phase shift keying (DQPSK) based authentication schemes and demonstrate their operation with legacy as well as non-legacy receivers. The addressed authentication scheme follows constellation perturbation by a pre-determined angle which performs the tag embedding without incurring additional network bandwidth. The implementation and evaluation platform consists of a software defined radio (SDR) testbed by using the open source radio framework, GNU Radio, and Universal Software Radio Peripherals (USRP-N210s). For moderate to high signal-to-noise ratios, the QPSK tagging scheme achieves low ($< 10^{-4}$) bit error rates (BER) and tag error rates (TER); this is due to a novel phase locked loop (PLL) design. The use of forward error correction (FEC) on the tag is also considered, and an improved TER and power saving is demonstrated. Results from our wireless SDR experiments validate the mechanism and demonstrate the practicality of the approach.**

I. Introduction and Background

Mission critical applications such as a military application in a hostile environment are more susceptible to network attacks than commercial or personal ad-hoc networks. Tactical communication networks are constrained by low bandwidth, high error rates and mobility. Public key infrastructure (PKI) supports the distribution and identification of public encryption keys, allowing secure exchange of data over networks by authenticating the identitiy of other party. As tactical network cybersecurity is becoming inevitable, PKI is gaining widespread acceptance across the Department of Defense (DoD). Incorporating secure communication amounts to requiring additional bandwidth to facilitate authentication. The five main security services for ad-hoc networks are: authentication, confidentiality, integrity, non-repudiation, availability [2]; *authentication* being the most daunting task since it is the bootstrap of the whole security system. Authentication refers to the process of determining whether a received message originated from a genuine or *authentic* source. Most of the work in authentication schemes have focused primarily above the PHY layer.

[6] and [8] addresses multiplexed authentication mechanism whereby a series of messages are devoted to authentication. This results in the authentication bits to be received with the same quality as the data but at the cost of data throughput. [9] addresses a PHY layer authentication aimed at minimizing the packet overhead but still has a light overhead tailored to their scheme. Digital watermarking technique follows embedded authentication mechanism by modifying the data in a controlled manner to provide additional information to the receiver. Unlike multiplexed authentication approach, the embedded authentication scheme degrades the data quality but offers the added advantage of requiring no additional bandwidth [1].

Secure communication in public infrastructure has gained significant interest in the recent years. One such example is in passenger and freight railroad systems, *Positive train control (PTC)*. Secure railroad communications and signaling is a vital component for ensuring a robust and resilient infrastructure; naïve cybersecurity features and designs leave the network vulnerable to external attacks. Conventional authentication schemes transmit both the payload and authentication code similar to current PTC systems [4], which employs a 32 bit truncated HMAC-SHA1 authentication code. HMAC-SHA1 operates in the application layer of the PTC system. The HMAC-SHA1 is a cryptographic hash function which generates the tag bits based on the payload and a secret key that is shared between the transmitter and receiver. This tag is

[1] The research presented in this investigation was supported by the FRA, Office of Research and Development, FRA Grant No. DTR-FR-5315C00015. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the view of the FRA and/or U.S. DOT.

978-1-5090-3781-0/16/$31.00 ©2016 IEEE

appended to the payload and are transmitted at the same power as the payload. The major disadvantage of this approach is the addtional tag overhead imposed on the system. This motivates the need to develop authentication schemes with no additional bandwidth requirement.

We implement the embedded authentication mechanism for QPSK scheme as introduced in [7] and extend it to $\pi/4$ DQPSK scheme. The technique is to *locally perturb* the phase encoding at the transmitter such that each QPSK symbol, $s_k,\ k \in \{1,2,3,4\}$, is transmitted as $s_k \pm \Delta_s$, where $\pm\Delta_s$ is a predetermined complex perturbation value on the IQ-plane. The sign or "direction" of perturbation corresponding to either $+\Delta_s$ or $-\Delta_s$ can be uniquely mapped to an *authentication tag bit*: either a '1' or a '0', which is determined *a priori* using some key generation/management method. The receiver has to decode both s_k as well as the the perturbation direction, i.e., the authentication tag. The system design with respect to both approaches are presented in depth in the upcoming sections. We demonstrate a thorough evaluation of both approaches on a SDR testbed and present the detailed analysis in sections III-A3 and III-B3.

At its core, our approach is an embedded authentication approach; we tag the modulated symbols assuming there exists a key-generation system operating under-the-hood. We have validated our proposed approach on a GNU Radio and USRP platform; this proof-of-concept hardware-software realization constitutes the primary contribution of this paper. In order to minimize the phase errors due to tagging, we have modified the design of the PLL. To the best of our knowledge, this PLL design is novel and it is instrumental in achieving low bit error rates (BER). We are able to extend the baseline QPSK design to $\pi/4$ DQPSK, and can demonstrate comparable bit error performance at the modified receivers.

The tag embedding approach discussed in this paper allows sender to add authentication to the system in a stealthy way so that users unaware of the authentication ,for example, *legacy receivers*, can still continue to communicate without requiring any modifications to the hardware or protocol. This becomes essential, when authentication is piggybacked onto an existing system. The tag embedding authentication via constellation perturbation can be used alongside the pre-existing upper layer security protocols to augment the security of the system. The primary contribution of this work is the inter-operable SDR based PHY authentication realization and a detailed evaluation of the system performance with legacy and non-legacy receivers. In our work, we represent the legacy receivers as the one that uses a standard conventional PLL and non-legacy receivers as the one with modified PLL.

The rest of this paper is organized as follows: In Section II, we discuss the principle behind authentication using perturbed symbols; we describe and evaluate the system in detail, in Section III; and we conclude by outlining directions for further research in Section IV.

II. Authentication by PHY Layer Tag Embedding

At the PHY layer, the abstraction at the higher layers is lost and all communication is designed and analyzed at the bit and symbol level. Denote the modulated QPSK symbol as $s_i \in \mathbb{C}$ where $i \in \{1,2,3,4\}$ indicates the quadrants on the complex plane. Typically, Gray coding is used to map bit pairs $b_{1i}b_{0i} \mapsto s_i$ such that,

$$b_{0i} = \begin{cases} 0 & \text{for } i = 3,4 \\ 1 & \text{for } i = 1,2 \end{cases} \quad \text{and} \quad b_{1i} = \begin{cases} 0 & \text{for } i = 2,3 \\ 1 & \text{for } i = 1,4 \end{cases} \tag{1}$$

$$s_i = \left[(-1)^{1-b_{1i}} + j^{3-2b_{0i}}\right]/\sqrt{2}, \tag{2}$$

for each quadrant i, with $j = \sqrt{-1}$. Note that the in-phase (I) and quadrature (Q) components of s_i are each of equal magnitude $(1/\sqrt{2})$ so that $|s_i| = 1$. The argument of s_i,

$$\theta_i = \arg\{s_i\} = (2i-1)\frac{\pi}{4},$$

so that, equivalently, $s_i = e^{j\theta_i}$. PHY layer tagging for authenticating a message concatenates the symbol bit sequence $b_{1i}b_{0i}$ to a *tag* bit t_i. This tag bit, in the context of baseband modulation, maps to a predetermined perturbation angle ε. Denote the perturbed angle by φ_i so that $t_ib_{1i}b_{0i} \mapsto s_i' = e^{j\varphi_i}$.

$$\varphi_i = \begin{cases} \theta_i + \varepsilon(-1)^{1-t_i} & \text{for odd } i \\ \theta_i + \varepsilon(-1)^{t_i} & \text{for even } i \end{cases} \tag{3}$$

Recall that bit pairs are mapped to their respective quadrants on the IQ plane using Gray coding, such that 11, 01, 00, and 10 are mapped to quadrants 1, 2, 3, and 4 respectively. This, in effect, means that for symbols s_1 and s_3, corresponding to 11 and 00, θ is perturbed by $+\varepsilon$ when the tag bit is 1 and $-\varepsilon$ when the tag bit is 0. On the other hand, the tag bit 1/0 represents a perturbation of $\mp\varepsilon$ for symbols s_2 and s_4 (for bit pairs $b_{1i}b_{0i} = 01, 10$). This retains the Gray coding structure for the bit triplet $t_ib_{1i}b_{0i}$. Note that the transmitted symbol s_i' does not impose any additional overhead at the PHY layer: the extra bit is encoded as an angle perturbation and complex baseband symbol s_i' encapsulates the authentication information within the complex argument.

In a way, the QPSK tagging approach looks similar to 8-PSK modulation scheme but there are a few key differences. While the performance of the tagging scheme at 22.5^o can be similar to that of an 8-PSK modulation scheme, where every 1 bit out of the 3 bit symbol can be interpreted as a tag, the QPSK tagging approach lets the user to control the perturbation angle. The degree of perturbation will let us prioritize the payload and/or the tag depending on the scenario. This will be demonstrated in Fig. 4, at lower perturbation angles the TER is higher whereas BER is 0 while both BER and TER are 0 when the perturbation angles are chosen in the range of 7^o to 30^o. The QPSK tagging approach is inter-operable with legacy QPSK receivers; transmitting an 8-PSK modulated symbol considering 1 bit out of the 3 bit symbol is a tag would conflict with the PLL as it will not lock on to the 8-PSK modulated synchronizing pattern.

III. System Design

In designing the transceiver, we have assumed that there exists a functioning key generation and key management scheme in place. The task of the key generator is to determine the tag bit based on the data bits, and hence we assume that this tag bit (t_i) is available, as the output of some tag-generator “black-box”. Figures 1 and 2 shows the transceiver components of a tagged QPSK system, which will be described in greater detail in the following subsection.

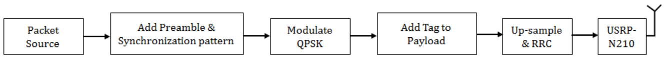

Fig. 1: Schematic of a Tagged QPSK transmitter.

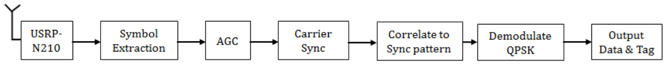

Fig. 2: Schematic of a Tagged QPSK receiver.

A. ***Tagged QPSK system***

1) Transmitter: While the PHY layer operates at the bit level, a software defined radio, typically, implements algorithms at the byte level. For a packet of length L_b bits, we need a tag sequence of length $L_b/2$ bits since every tag perturbs a symbol, which is encoded by two bits. In terms of bytes, a register of length L_b bits corresponds to $L_B = \lceil L_b/8 \rceil$ bytes. In our prototype transmitter, a packet *payload* consists of a randomly generated string, 250 bytes long and *tag* sequence of length 125 bytes. At the interface of packetization and the PHY layer, preamble and sync pattern bits are concatenated to the beginning of the payload. These bits are baseband modulated using conventional QPSK modulation (see equation(2)), as these bits cannot be perturbed in phase because they are used by the receiver for phase synchronization so that the latter bits, i.e. tagged payload, may be correctly sampled and detected. This part of baseband modulation is an important component of a working system. Baseband modulation is often followed by filtering and pulse shaping, after which the USRP upconverts the symbols to carrier frequency.

2) Receiver and Phase Lock Loop: The receiver consists of four main parts, symbol timing synchronization, phase/frequency synchronization, packet synchronization, and decoding tag and data symbols into bits. For symbol timing synchronization, the optimal symbol timing is estimated during a packet preamble. This timing estimate is then used to extract the packet symbols from the incoming sample stream. After extracting all of the packet symbols, phase/frequency synchronization is performed to remove any frequency and phase offset from the symbol stream. There will still be a 90^o,180^o or 270^o phase ambiguity in the symbols which gets resolved after the packet synchronization.

The phase/frequency synchronization is performed using a PLL that removes the phase and frequency offset from the symbol stream. This PLL first finds the phase error between the current symbol and the closest constellation point. It then adjusts a numerically controlled oscillator (NCO) such that when the NCO output is multiplied by the incoming symbols it will reduce the phase error. The phase error function for a standard QPSK constellation is the phase difference between the received symbol and the nearest of the four QPSK constellation points. This phase error will also work with tagging up to a point as the phase errors caused by the tag will average to zero over time. Above some perturbation angle, the PLL will not be able to stay locked to the correct phase. It will in effect still stay locked, but the constellation diagram will be rotated 45^o and will not be decoded successfully. To prevent this, the PLL can be modified simply by taking the phase error to be the phase difference between the received symbol and the nearest symbol in the tagged QPSK constellation. The phase error will then be zero for all received constellation points and the PLL will remain locked.

After the phase correction, the packet synchronization finds the exact start of the packet. This is done by correlating to a known synchronization pattern at the beginning of the packet. The first data symbol is directly after this pattern. Since there may be a phase ambiguity in the symbol stream as mentioned above, this phase will be reflected in the phase of the correlation value. The data symbols after the synchronization are multiplied by the conjugate of the correlation value to remove the phase ambiguity from the data. Once the start of the data is found, each data symbol is decoded into two data bits based on which quadrant of the constellation the received symbol is in. Then the received symbol is multiplied by the conjugate of the ideal version of the received symbol. This has the effect of removing the data part of the symbol leaving only the tag perturbation angle. The tag is decoded depending on the data bits and whether the perturbation angle is greater than or less than 0.

3) System Characterization: While characterizing a PHY layer authentication system, we must evaluate two metrics in the design: BER and TER. Since authentication at the PHY layer uses tags to perturb the phase information, it is important to understand how BER and TER relate to each other. TER also serves as a measure of authentication efficacy.

We conducted experiments to measure these metrics for the transceiver with the modified PLL as a function of the perturbation angle, ε. Recall that the payload is 250 bytes long, i.e., $250 \times 8 = 2000$ bits. We exercised this setup over 10 iterations and, therefore, we have 20,000 bits over which BER and TER calculations are reported. Transmitter and receiver USRPs were separated by 4 ft. The receiver gain was fixed at 5 dB and the transmitter gain was varied from 5 dB to 30 dB in steps of 5 dB.

Based on the data from the experiments described above, we evaluated BER and TER values. These are plotted in Fig. 3. The angle ε is varied over the interval $[0, \pi/4]$ rad, i.e., from $0°$ to $45°$. We observe that $\min_{\varepsilon} \mathrm{BER} \leq 10^{-4}$ and that this lower bound is maintained over $0 \leq \varepsilon \leq \pi/8$ for all transmit gains. Beyond a critical angle $\varepsilon' \geq \pi/8$ rad, the BER begins to increase sharply. For low transmit gains (corresponding to low SNR values), $\varepsilon' \approx \pi/8$, and may reach a little over $\pi/6$ rad for higher transmit gains.

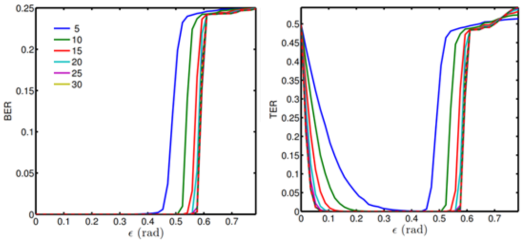

Fig. 3: **Over-the-air:** QPSK Error rates vs Perturbation Angle for varying transmit gains.

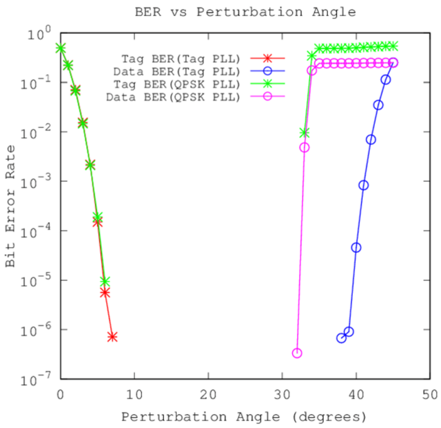

Fig. 4: **Over-the-air:** Legacy vs Non-legacy receivers.

The TER shows similar characteristics as the BER curves for $\varepsilon > \pi/8$. However, since the tags are encoded as angle perturbations, TERs are also sensitive to small perturbation angles, which may be interpreted as a low tag-signal-to-noise ratio. For the interval $(0, \pi/8)$, the tag error rate is a monotonically non-increasing function of ε. The slope of TER(ε) is observed to vary with the transmit gain; the results corroborate intuition in that for a given ε, lower transmit gains correspond to poorer tag error performance. These curves may be contrasted to the case when a modified PLL is used. For a transmit and receive gains of 20 dB, Fig. 4 shows the bit and tag error rates obtained when using an unmodified PLL (referred to as QPSK PLL in the figure). The modified PLL evidently is more resilient to phase perturbation.

Next, we consider the effect of noise within the system. This testbed architecture consisted of a cabled environment with a resistive combiner connected to a third SDR acting as a noise source. The power of the noise source was measured in relation to the power of the transmitted signal to identify *signal to noise ratio* (SNR). The experiments were conducted for a payload size of 1500 bytes and tag length of 750 bytes and transmitting 100 packets for each transmission. HMAC strength is directly related to the length of the authentication code. Specifically, National Institute of Standards and Technology (NIST) [3] qualifies HMAC security in terms of three properties: 1) collision resistance, 2) preimage resistance, and 3) second preimage resistance. Specifically, collision resistance strength is 1/2 of the HMAC length. Similarly, preimage and second preimage strength is equal to the HMAC length. Additionally, HMAC strength is also dependent on key generation and management techniques. This paper does not address key generation or management techniques. Figure 5 shows QPSK BER (solid lines) and TER (dashed lines) under varying perturbation angles using a traditional unmodified PLL. Each line represents a different SNR with a step size of 2dB starting at 12dB and ending at 26dB. Similarly, we repeat the test to show QPSK performance under varied SNR using the modified PLL in Fig. 6. It can be seen that for higher SNR curves (22 to 26 dB), the BER increases before the perturbation angle is 30^o whereas modified PLL increases the angle at which BER occurs. In other words, the modified PLL increases the tolerance limit (in terms of perturbation angle) of the system. Thus, with these tests we have shown that the system performance improves with the modified PLL.

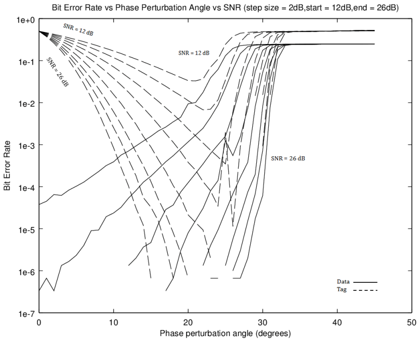

Fig. 5: **Cabled environment:** QPSK Error rates vs Perturbation Angle using a standard PLL (legacy receiver).

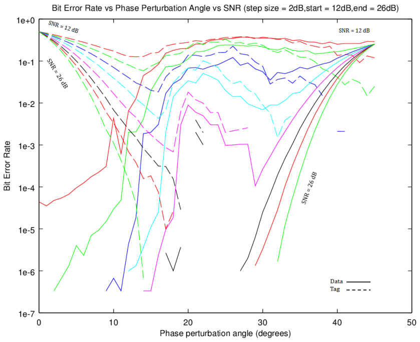

Fig. 6: **Cabled environment:** QPSK Error rates vs Perturbation Angle using a modified PLL (non-legacy receiver).

B. *Tagged* $\pi/4$ *DQPSK system*

$\pi/4$ DQPSK is similar to QPSK modulation scheme where one QPSK constellation is used to modulate odd symbols and another offset by $\pi/4$ radians modulate even symbols. The symbols hence mapped are differentially encoded prior to transmission. This is desired to simplify the hardware design of the radio with regards to amplifiers, such that non-linear, more power efficient, amplifiers can be used. The use of differential modulation is a common design choice due to the simplified receiver design. Differential modulation make use of a received symbol and the most recent previous symbol to identify the transmitted data. This approach minimizes the need to implement phase correction.

1) Transmitter: The packet structure is the same as with the tagged QPSK system comprising of preamble, synchronization pattern and payload. At the transmitter, after QPSK modulating the symbols, every other symbol is rotated by $\pi/4$ radians. Then the symbols are differentially encoded using the following:

$$Y_{n+1} = Y_n X_n, \tag{4}$$

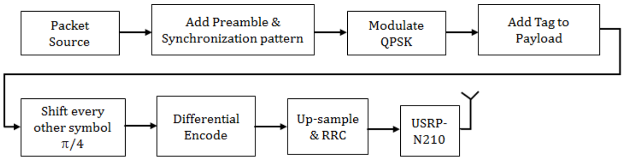

Fig. 7: $\pi/4$ DQPSK Transmitter chain.

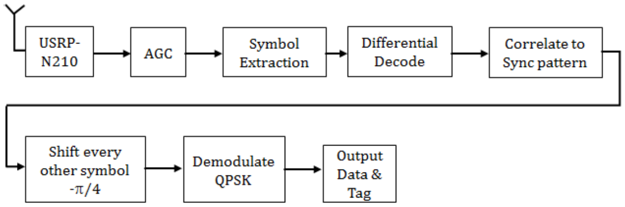

Fig. 8: $\pi/4$ DQPSK Receiver chain.

2) Receiver: At the receiver, after extracting symbols, the symbols are differentially decoded as follows:

$$Y_n = X_n X_{n-1}^*, \tag{5}$$

This reverses the differential encoding that was performed at the transmitter. The output of the differential decoder is mostly invariant to received signal frequency offset. A phase offset will be incurred due to the received frequency offset, but since the frequency offset is small the phase offset will be negligible.

Figure 8 outlines the steps at the receiver to retrieve the payload and tag. The automatic gain control (AGC) normalizes the amplitude of the received signal. This is required to prevent the variation of carrier synchronization and symbol synchronization response time with the received signal level. The AGC operates on blocks of 4096 samples. First, the root mean squared (RMS) amplitude of the samples is calculated. Then each sample is divided by the RMS amplitude. Root Raise Cosine (RRC) filtering is used in the transmitter and receiver to perform up-sampling and down-sampling. The input signal is up-sampled by a factor of 32 using RRC taps. Similarly, the received samples are down-sampled by 32 samples per symbol which is implemented using a 32 bit time register. The 5 most significant bits are used to select the sample to output. After differential decoding, packet synchronization is performed as before by correlating with the sync pattern to find the start of the data. Once the start of packet is located, the $\pi/4$ offsets applied to every other symbols is removed to obtain the original QPSK constellation. The resulting QPSK constellation can now be demodulated to obtain the payload and tag.

3) System Characterization: As with QPSK tagging in III-A3, here we characterize the system on the basis of BER and TER. The experimental testbed consisted of two USRPs serving as the transmitter and receiver in a colocated and cabled environment. The number of packets sent, payload and tag sizes were set to match the QPSK experiments (Fig. 5 and 6). Figure 9 shows BER and TER under *"no injected noise"*. We see that performance follows the same trends as QPSK. The higher the transmit gains the lesser the errors experienced. Figure 10 repeats the same SNR test as mentioned in subsection III-A3 for the $\pi/4$ DQPSK system. It was expected that decoding performance of both tagging and original payload will degrade under low SNR conditions. [5] indicated that 10^{-4} BER was considered the minimum acceptable performance. PTC radios specify a maximum usable sensitivity with BER $< 10^{-4}$ as $-108dBm$ for $32kbps$ $\pi/4$ DQPSK. The thermal noise floor in this bandwidth ($25kHz$) at a temperature of $300K$ is $-123.83dBm$. The minimum SNR

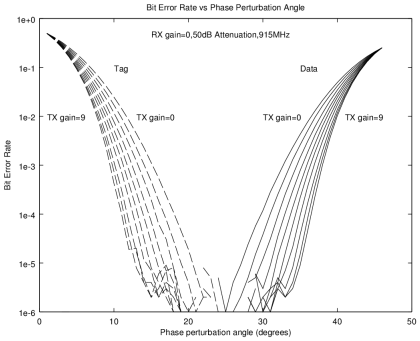

Fig. 9: **Cabled environment:** $\pi/4$ DQPSK Error rates vs Perturbation Angle under varied Transmit gain.

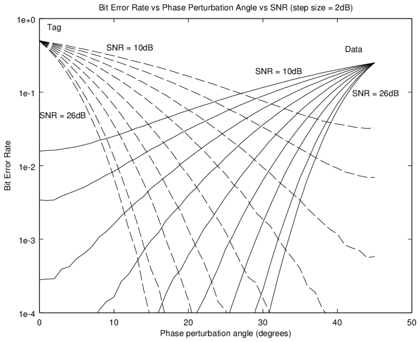

Fig. 10: **Cabled environment:** $\pi/4$ DQPSK Error Rates vs Perturbation Angle under Varied SNR.

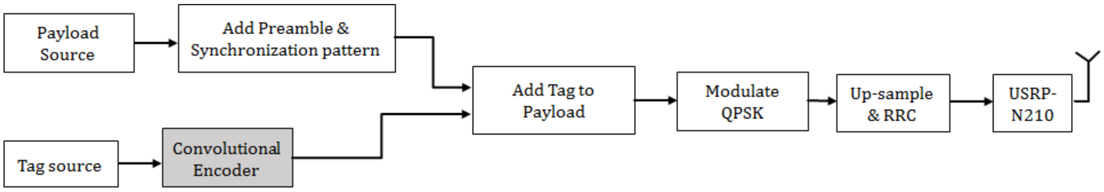

Fig. 11: Tagged QPSK transmit chain with FEC.

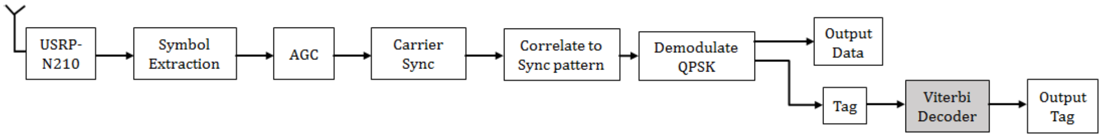

Fig. 12: Tagged QPSK receive chain with FEC.

is therefore $-108dBm-(-123.83dBm)=15.83dB$. As shown in Fig. 10, in the absence of tagging (i.e.,0^o perturbation), the BER meets the BER $< 10^{-4}$ requirement at an SNR of $15.83dB$. With tagging the SNR required for tag and data to meet the BER $< 10^{-4}$ specification is around $21dB$. This is an increase of approximately $5dB$ reducing the receiver sensitivity to $-103dBm$. The TER and BER can be improved by adding FEC to the PHY layer at a lower SNR for both modulation schemes. To experimentally prove the validity of this argument, we incorporated convolution encoding/viterbi decoding in the tag branch of QPSK transmission system as shown in Figures 11 and 12. The convolution encoder accepts N bytes of tag and outputs $2(N+1)$ encoded tag bytes. The constraint length of the encoder is 5. Likewise, the Viterbi decoder converts a $2(N+1)$ bytes to N bytes.The USRP transmit gain was varied from 4 to $22dB$ for a perturbation angle of 7^o, tag length of 374 bytes and payload size of 1500 bytes. A total of 250 packets were sent during 1 transmission. As can be seen in Fig.13, the BER for this experimental setting was 0 irrespective of the presence of FEC whereas comparing the TER curves of the system with and without FEC shows a transmit gain save of $8dB$ to achieve an error rate of 10^{-4}.

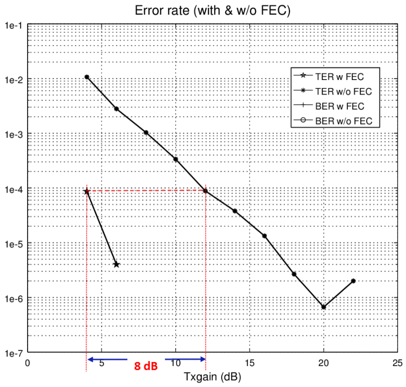

Fig. 13: **Over-the-air:** QPSK Error Rates vs transmit gain.

IV. Conclusion and Future work

We have empirically characterized the performance of a PHY layer authentication system which encodes the authentication information as symbol perturbations. We proposed and verified the operation of a modified PLL while also demonstrating the improvement in system performance with the inclusion of FEC. A theoretical characterization of these curves, in terms of convexity and variation as a function of transmit gain and/or SNR would be insightful and would also have predictive value for systems which may operate outside the range of parameters we have controlled in our experiments. Further ideas such as tag symbol, in contrast to tag bits also need to be explored. The radios in our experiments were static; characterization of the system under dynamic conditions is an important extension of this work.

References

[1] I. J. Cox, M. L. Miller, and A. L. McKellips, “Watermarking as communications with side information,” *in Proc. of the IEEE*, vol. 87, no. 7, pp. 1127–1141, July 1999.

[2] S. W. D. Han and L. Zhang, “Authentication Service for Tactical Ad-Hoc Networks with UAV,” in *Proc. of Computing and Intelligent Systems: International Conference (ICCIC)*, Wuhan, China, September 2011.

[3] Q. H. Dang, “SP 800-107. Recommendation for Applications Using Approved Hash Algorithms,” National Institute of Standards & Technology, Gaithersburg, MD, United States, Tech. Rep., 2009.

[4] R. Goel, D. Wijesekera, and A. B. Bondi, “Identity Management for Interoperable PTC Systems in Bandwidth-Limited Environments: The Final Report, Part 3 (of three parts) The Proposed Solution,” Federal Railroad Administration, Gaithersburg, MD, United States, Tech. Rep., July 2014.

[5] T. K. Himsoon and W. P. Siriwongpairat, “Design and Analysis of 220 MHz RF Communications for Interoperable Positive Train Control System,” in *Proc. of ASME from 2011 Joint Rail Conference*, Pueblo, Colorado, USA, March 2011.

[6] G. J. Simmons, “A survey of information authentication,” *in Proc. of the IEEE*, vol. 76, no. 5, pp. 603–620, May 1988.

[7] X. Tan, K. Borle, W. Du, and B. Chen, “Cryptographic link signatures for spectrum usage authentication in cognitive radio,” in *Proc. of the ACM Conference on Wireless Network Security (WiSec)*, New York, NY, USA, June 2011.

[8] X. Wang, Y. Wu, and B. Caron, “Transmitter identification using embedded pseudo random sequences,” *IEEE Transactions on Broadcasting*, vol. 50, no. 3, pp. 244–252, Sept 2004.

[9] H. Wen, P. H. Ho, C. Qi, and G. Gong, “Physical layer assisted authentication for distributed AdHoc wireless sensor networks,” *IET Information Security*, vol. 4, no. 4, pp. 390–396, December 2010.