Abstract—We address the problem of efficiently establishing a shared secret key over an open wireless channel in the presence of an active (jamming) adversary. A commonly employed technique in practice for key sharing is the cryptographic elliptic-curve Diffie-Hellman (DH) protocol; however, its communication cost in a jammed environment is very high. Hence, we employ novel physical-layer techniques to enhance the performance of the DH protocol in a wireless setting. Specifically, we propose a protocol that exploits the randomness inherent to the wireless environment by testing rapidly for time-frequency bands where success can be obtained, essentially probing for those bands that are favorable to the communicating parties and unfavorable to the adversary. The proposed protocol is significantly more energy and time efficient than the standard DH approach, and addresses a number of deficiencies of previous protocols that also attempt to break the circular dependency that arises when bootstrapping secure wireless communications.

I. INTRODUCTION

Efficient secure wireless communication between two nodes typically requires them to share a secret key for bootstrapping the channel and enabling higher-layer security mechanisms. For example, spread-spectrum techniques are widely employed for establishing a secure wireless channel, but they require a shared secret spreading code between the legitimate wireless nodes [1], [2]. Establishing pairwise shared keys between the nodes in a network can be achieved by either pre-distribution using trusted offline mechanisms or by on-demand exchange in the field. While the former approach is simple, it is inefficient and incurs a high security management overhead, and is non-scalable for large networks. Thus, for large dynamic wireless networks with changing memberships and a significant overhead of centralized shared key distribution, on-demand key exchange is necessary and a shared secret key needs to be established by the two nodes over the open wireless medium.

Secret key exchange is a fundamental problem in security and has been studied in the information-theoretic [3], [4], [5] and the cryptographic literature [6], [7]. The main challenge in the wireless case is the broadcast nature of open wireless transmission, which provides ample opportunity for eavesdropping and signal jamming to the adversary. We maintain that the consideration of an active adversary (e.g., hostile jammer), rather than a passive eavesdropper as in [8], [9], is critical to the problem. Secret key exchange takes place between two nodes who do not share any prior secrets. Therefore, a secure anti-jamming channel has not yet been established because forming this channel itself requires a secret key [2]. Hence, the legitimate nodes have to use the publicly available open wireless channel for the secret key exchange protocol which makes it highly vulnerable to communication disruption. As a result, exchange of message bits necessary for establishing a secret key may incur a high communication cost per bit to overcome jamming attacks. Here, we propose a secret key exchange method which aims to minimize the number of bits that pay such a cost. In particular, we consider first exchanging a short secret code across the channel at a (potentially) high communication cost, which is then in turn used as a spreading/hopping code to reduce the cost per bit for the longer messages that follow to establish a secure key.

We refer to our proposed method as the Physical-Layer-Enhanced Key Exchange (PEK) Method. The PEK Method is summarized in Fig. 1. Alice and Bob are two nodes with no prior secrets and want to establish a symmetric key in the presence of a potentially jamming adversary Eve by exchanging public messages using a cryptographic method (e.g. Elliptic-curve Diffie-Hellman). Therefore, two long public messages \(DH_A\) and \(DH_B\) have to be exchanged by Alice and Bob, which will have a high communication cost under a jamming adversary without a pre-established efficient channel. In PEK, Alice generates a random spreading code and transmits a short message containing this (ephemeral) spreading code in plain (Step 1 in Fig. 1). After receiving the spreading code, Bob transmits his public message \(DH_B\) using this code and thus temporarily guards his communication against possible jamming, and Alice does the same for her public message, \(DH_A\). But it is possible that Eve also receives the spreading code, and can jam the spread spectrum system Bob is employing in Step 2. Therefore, the first stage of PEK has to be such that Alice communicates the short ephemeral code to Bob that Eve is not able to decipher, and this is achieved using the inherent wireless channel randomness. Thus, our method can be viewed as information-theoretic key exchange (the short ephemeral spreading code) assisting computational-security based key exchange through which we establish the long code necessary for enabling a long-term spread spectrum channel.

To accomplish the first step in Fig. 1, we take advantage of a key aspect of wireless communications: the time- and frequency-dependent channel quality caused by multipath fading, which makes both the legitimate nodes’ and adversary’s actions subject to randomness to be exploited. Whenever Alice
Fig. 1. Summary of the Physical-Layer-Enhanced Key Exchange Method (PEK) to do secret key establishment over wireless channels under a possibly jamming adversary. Alice and Bob are nodes with no prior symmetric secrets and they want to establish a secret key by exchanging public messages, $DH_A, DH_B$, according to Diffie-Hellman key exchange. In Step 1 Alice sends a short message containing a randomly generated spreading code. In Steps 2 and 3, public messages are exchanged using spread spectrum based on this code. Spread spectrum guards the message transmission against jamming as long as the spreading code is known by Alice and Bob only. This method relies on the fact that wireless channels are random and packet losses are common, so it is possible to deliver a short secret code even under a jamming and eavesdropping adversary. Thus, a typical scenario is where Step 1 is repeated until Alice finally receives a valid message from Bob.

In PEK, when Alice sends the message containing the spreading code in Step 1, she waits for an answer on the corresponding spread spectrum band. She may fail to receive a reply either because Bob was not able to decode her message or Bob’s reply is jammed by Eve because Eve also received the code. Therefore, Step 1 is repeated until Alice can deliver a message to Bob which Eve fails to decode. We employ a (publicly known) slow frequency-hopped scheme in Step 1 of PEK. Packets will get through when the random fading of the selected frequency band allows signal-to-noise-plus-jamming at the receiver to be high enough, so the transmitter hops until such happens. One way to think about this approach is as probing the frequency spectrum for that band for which the Alice-Bob channel is good, and the Eve-Bob and Alice-Eve channels are poor. The cost of these repeated trials is reasonable because of the short length of the ephemeral spreading code in Step 1, and, we argue that, the return in terms of improved efficiency for Steps 2 and 3 in Fig. 1 will exceed the extra cost brought by Step 1.

The circular dependency between forming an anti-jamming channel and availability of a secret key was noted and addressed in [2], [11] by a method called Uncordinated Frequency Hopping (UFH), where the transmitter and receiver hop randomly on different frequency bands and exchange messages when they share a common hop which is not shared by the adversary. The shared cryptographic messages are then utilized to generate a secret key. Stated differently, [2], [11] introduce artificial randomness to arrive at a channel that has a low-probability occurrence of a “good” channel between Alice and Bob in the face of jamming. In contrast, [12] introduces a scheme where the transmitter employs a successively weaker key over time and the receiver records the output of the channel. At the end of the transmission, the receiver deciphers the weaker keys and then works back to de-spread the longer signal from its recorded signal. The scheme in [2], [11] suffers from a high communication cost and a sophisticated follower-jammer concern, while [12] has concerns of recording wideband signals and jamming of progressively weaker keys which would prevent backward de-spreading. Also, the front-end filter receiving the wideband signal can be easily saturated by an attacker by jamming with full power on a specific frequency band. In contrast to the approaches of UFH and [12], which could also be employed on a wideband wired channel, PEK makes use of the unique properties of the wireless channel.

In summary, we address the secret key exchange problem by proposing the Physical-Layer-Enhanced Key Exchange Method which has the following properties: 1) Secret key exchange messages are transmitted over an ephemeral spread spectrum channel, thus reducing the number of bits transmitted over an open channel. 2) It uses the natural randomness present in wireless channels thus avoiding the communication cost present in UFH [2], [11] to create randomness. 3) It uses physical layer tools like cooperative jamming in order to combat easy eavesdropping advantage brought by the wireless channel. 4) Its communication cost is flexible to jamming intensity enabling a lower cost under less severe jamming or no-jammer case.

II. Communication Model

We consider a frequency-hopped communication system where the allocated frequency range is divided into smaller frequency bands. The fading experienced by a signal depends on which frequency band or bands the signal occupies. Here, a slowly fading frequency-selective fading channel [13] is assumed, where bands with sufficient frequency separation experience independent fading. In the wideband systems being assumed for future secure communication systems [14], there will be many such independently fading bands. The frequency response of the channel is assumed to be static over a packet, but to vary from one packet to another, which is the standard quasi-static fading model [1]. Note that, it is also possible for a node to generate intentional channel variation if needed [18].

Now, consider a signal sent with a slow frequency hopped (SFH) system. In an SFH system, the transmitter dwells in
a given frequency band for the transmission of a number of bits before hopping to a different band. Given the quasi-static model, the signal is multiplied by a single fading factor during the time the system dwells in a given frequency band. A signal carrying a message consists of a number of physical-layer symbols. Let \( x_{A,i} \) be the \( i \)th (complex) symbol of an \( M \)-symbol message sent by Alice on a given hop of an SFH system. The received symbols at Bob and Eve, \( y_{B,i} \) and \( y_{E,i} \), respectively, are:

\[
y_{B,i} = h_{AB} \sqrt{\frac{E_s}{d_{AB}^{\alpha}}} x_{A,i} + n_{B,i},
\]
\[
y_{E,i} = h_{AE} \sqrt{\frac{E_s}{d_{AE}^{\alpha}}} x_{A,i} + n_{E,i},
\]

where \( E_s \) is the symbol energy, \( \alpha \) is the path-loss exponent, \( d_{XY} \) is the distance between nodes \( X \) and \( Y \). \( n_{X,i} \) is the \( i \)th complex zero-mean Gaussian noise symbol at node \( X \) with \( E[n_{X,i}^2] = N_0 \), \( i = 1, 2, \ldots, M \). \( h_{XY} \) is the (complex) fading coefficient between nodes \( X \) and \( Y \) for that hop. We assume Rayleigh fading with \( E[h_{XY}^2] = 1 \), which implies \( h_{XY} \) is a complex Gaussian random variable with zero mean and independent components; hence, \( h_{XY}^2 \) is exponentially distributed with mean \( 1 \). The fading of channels between different sender-receiver pairs is assumed independent.

A packet is lost if the received signal-to-noise-and-interference ratio (SINR) is below a certain threshold, \( \gamma \). This assumption is reasonable for modern codes that demonstrate a threshold effect [15, pg. 882]. The SINR threshold for successful communication, \( \gamma \), is determined by the rate at which the symbols are sent. The frequency band allocated and pulse shaping dictate the number of symbols that can be aired per second. Therefore, the rate at which bits are transmitted (bits per second) is proportional to the rate \( R \) bits/symbol. Information theoretical results show that the relation between this rate and the corresponding SINR threshold is given by

\[
R = \log_2(1 + \gamma). \tag{2}
\]

Hence, a lower rate allows signals to be more easily decoded at the expense of longer message delays and greater energy costs.

Here, we perform some basic analyses on the above model to support succeeding sections. The probability of a correct packet reception at \( B \) and \( E \), respectively, is given by:

\[
P^{(A-B)}_{\text{rcv}} = P \left( \frac{|h_{AB}|^2 E_s}{d_{AB}^{\alpha}} > \gamma \right)
= \exp \left( -\gamma \frac{N_0 d_{AB}^{\alpha}}{E_s} \right), \tag{3}
\]

and

\[
P^{(A-E)}_{\text{rcv}} = \exp \left( -\gamma \frac{N_0 d_{AE}^{\alpha}}{E_s} \right). \tag{4}
\]

With other parameters fixed, the success of decoding depends on the degree of fading of a given sender-receiver channel.

Fast frequency hopping (FFH) [16], where the system hops multiple times during the transmission of a single symbol, is also considered. The symbol is split across \( K \) bands, \( k = 1, 2, \ldots, K \), each with different fading coefficients, \( h^{(k)}_{AB} \); hence the received signal energy at Bob will be

\[
P^{(A-B)}_{\text{rcv}} = P \left( \frac{1}{K} \sum_{k=1}^{K} |h^{(k)}_{AB}|^2 \frac{E_s}{d_{AB}^{\alpha}} > \gamma \right). \tag{5}
\]

The probability of successful reception with FFH is then

\[
P^{(A-B)}_{\text{rcv}} = P \left( \frac{1}{K} \sum_{k=1}^{K} |h^{(k)}_{AB}|^2 \frac{E_s}{d_{AB}^{\alpha}} > \gamma \right). \tag{6}
\]

For large \( K \), \( \frac{1}{K} \sum_{k=1}^{K} |h^{(k)}_{AB}|^2 \) approaches its expected value. In fact, the probability of success with \( K \)-fold diversity converges rapidly to its limiting value [1]. In other words, for an FFH system, it is reasonable to assume that

\[
P^{(A-B)}_{\text{rcv}} = \begin{cases} 1, & \text{if } \frac{E_s d_{AB}^{\alpha}}{N_0} \geq \gamma; \\ 0, & \text{if } \frac{E_s d_{AB}^{\alpha}}{N_0} < \gamma. \end{cases} \tag{7}
\]

### III. FORMING SECRECY BY PACKET LOSS

PEK makes use of packet losses an eavesdropper suffers (Fig. 1) to share the information about a secret anti-jamming channel between Alice and Bob. In this section, we analyze the performance of secret generation by packet loss, using the physical layer basics presented in the previous section. We show that creating a secret by making use of packet losses can perform poorly when the adversary has a relative advantage over the intended receiver and propose solutions to overcome it using cooperative techniques. Consider Alice sending a packet to Bob in the presence of Eve, like in Step 1 of PEK. The performance measure we evaluate is the probability of the event, \( S \), that “the message sent by Alice is received only by Bob”, i.e., it qualifies as a secret message. In other words,

\[
P(S) = P^{A-B}_{\text{rcv}} (1 - P^{A-E}_{\text{rcv}}). \tag{8}
\]

#### A. Passive Adversary and Cooperative Jamming

Assume a scenario where Alice and Bob are a fixed distance apart and the location of the passive eavesdropper, Eve, is varied on the line between Alice and Bob. For each location Eve may occupy, we calculate the probability of delivering a message to Bob only, \( P(S) \). Replacing (3) and (4) in (8),

\[
P(S) = \exp \left( -\gamma \frac{N_0 d_{AB}^{\alpha}}{E_s} \right) \left( 1 - \exp \left( -\gamma \frac{N_0 d_{AE}^{\alpha}}{E_s} \right) \right). \tag{9}
\]

The plot is given in Fig. 2 (a) (dashed curve). The immediate observation is that delivering a secret packet is most difficult when Eve is close to Alice, because Eve has a large average SINR advantage over Bob due to path-loss. Hence, creating secrecy by packet loss is inefficient in terms of energy and delay when the attacker is close to the sender while the intended receiver is located further away. We refer to this case as the near-far problem. Moreover, the attacker’s location is typically unknown and performance is dictated by the worst-case scenario.

The solution we propose to the near-far problem is cooperative jamming, where a second antenna on the sender side (or...
a closely located helper node) helps by transmitting noise into the air. In a near-far case, Eve receives a strong signal but also suffers strong noise. On the other hand, Bob is not as affected by this artificial noise as Eve because he is far away, thus leveling the difference between Bob and Eve’s SINR values.

In particular, the packet receive probability at Bob becomes:

\[ P_{\text{rcv}}^{(A \rightarrow B)} = \exp\left( -\frac{N_0}{E_A} d_{AE}^\alpha \right) \frac{1}{K_C}, \]

where

\[ K_C \triangleq \left( \frac{E_C}{E_A} + 1 \right). \]  

Similarly,

\[ P_{\text{rcv}}^{(A \rightarrow E)} = \exp\left( -\frac{N_0}{E_A} d_{AE}^\alpha \right) \frac{1}{K_C}. \]  

Here \( E_C \) and \( E_A \) are the transmit energy of the helper node (or the second antenna) denoted by \( C \), and Alice, respectively. These values are set such that \( E_s = E_C + E_A \). Because \( C \) and \( A \) are very closely located, we assume \( d_{AE} = d_{CE} \) and \( d_{AB} = d_{CB} \).

In Fig. 2 (a) (solid curve), we plot the probability that Alice’s message is secret when cooperative jamming is employed. Notice that, compared to the plot with no cooperative jamming, the near-far (worst-case) performance is significantly improved.

B. Jamming Adversary and Role-Switching

The situation above is changed when the adversary is capable of not only eavesdropping but also disrupting the message transfer at the same time, i.e., when a jamming adversary is present. Note that jamming and listening at the same time, i.e., having full duplex communication is in general hard to achieve because it requires the isolation of the transmit signal from the receiver antenna. In this case, \( P_{\text{rcv}}^{(A \rightarrow E)} \) is the same while \( P_{\text{rcv}}^{(A \rightarrow B)} \) will be reduced due to jamming:

\[ P_{\text{rcv}}^{(A \rightarrow B)} = \exp\left( -\frac{N_0}{E_A} d_{AB}^\alpha \right) \frac{1}{K_E}, \]

where

\[ K_E \triangleq \frac{\beta}{E_A/d_{AB}^\alpha} + 1. \]

Here \( \beta \) is the attacker’s transmit (jamming) power, and \( K_C \) is as given in (11).

In Fig. 2 (b), we plot the probability of a message being secret under a jamming adversary. There is an additional weak performance point, namely when the adversary is close to the receiver side and inundates the receiver with noise. A solution to improve performance in the jamming adversary case is to utilize the asymmetry in secret message transfer. Namely, instead of one node always being the receiver, the nodes can switch sender-receiver roles after a certain number of trials. The effect of role-switching will roughly be to choose the advantaged side as the sender.

For the jamming adversary case, Fig. 2 (c) shows the expected number of trials until a secret message is transmitted.
When nodes employ neither cooperative jamming nor role-switching, performance becomes worst when Eve is close to either side. Cooperative jamming improves the performance in the near-Eve case but the far-Eve case is still a problem. The best performance is achieved when nodes switch roles after a certain number of trials in addition to using cooperative jamming.

IV. PHYSICAL-LAYER-ENHANCED KEY EXCHANGE

Background and Motivation

We consider secret key exchange utilizing the Elliptic Curve Cryptography based Diffie-Hellman (DH) protocol [6] and adapt it to the wireless context. The Diffie-Hellman protocol for key exchange requires two message transfers: one from A to B, and the other from B to A, which are denoted as $DH_A$ and $DH_B$, respectively. Each message consists of a number of components such as the node’s public key, signature, etc. [17]. For a 128-bit security level, these messages would typically be 1024 bits each. In terms of pre-established security infrastructure, we assume that each node has a public-private key and that a certification authority (CA) provides certificates to bind node identities to their respective keys. Also, we assume that no other (secure) channels exist between A and B, including non-wireless, for them to exchange a shared secret during key exchange.

Using computational security assumptions, the DH protocol enables exchange of a secret key even in the presence of an adversary; however, as we show next, under a jamming adversary a direct DH protocol suffers from significant inefficiency and communication cost.

Consider the communication cost of establishing a secret key using the DH method in the presence of a jamming adversary. We know that Alice and Bob will have to exchange public messages $DH_A$ and $DH_B$, respectively. Suppose that each message is of length $B$ bits and is sent at a rate of $R$ bits/symbol; so, each message requires the transmission of $B/R$ physical-layer symbols. Let us assume that the adversary forces signal jamming with power $\beta$ which results in a certain success probability for message transmission. Under the basic protocol, Alice keeps sending her public message $DH_A$ until it is successfully received by Bob, at which point Bob repeats the process and transmits his public message $DH_B$. Assume these messages are sent with a slow frequency hopped (SFH) system using a publicly-known hopping pattern.

The total number of symbols that needs to be transmitted is a random variable, $N$, with expected value:

$$E(N) = E(N_1) + E(N_2),$$

where

$$E(N_1) = \sum_{m=0}^{\infty} \frac{(B/R)(m+1)(1-p_B)^mp_B}{},$$

$$E(N_2) = \sum_{n=0}^{\infty} \frac{(B/R)(n+1)(1-p_A)^np_A}{}. \quad (14)$$

Here, $m, n$ denote the number of failed attempts in delivering $DH_A, DH_B$, respectively. $N_1, N_2$ are the number of symbols transmitted by Alice and Bob, respectively, and $p_B = P_{rcv}(A\rightarrow B)$ and $p_A = P_{rcv}(B\rightarrow A)$ are as given in (13) with $K_C = 1$.

We calculate the value of $E(N)$ for an illustrative scenario where Alice and Bob are a fixed distance apart (taken as 10 units) and Eve is located on the line between them; clearly, jamming is most severe when the attacker is close to Alice or Bob. To establish a 128-bit secret key, Alice and Bob need to exchange $B = 1024$ bits in each direction. For a rate $R = 0.2$ bits/symbol, which is chosen to minimize the communication cost, this requires $B/R \approx 5k$ symbols for each transmission of a public message. Fig. 3 shows how poorly key exchange performs under severe jamming by dramatically increasing the expected number of symbols transmitted, hence wasting energy and time. In the worst case, the secret key exchange requires more than 100k symbol transmissions on average. Finally, since an attacker location is generally unknown, the worst-case performance is the primary concern.

Physical-Layer-Enhanced Key Exchange (PEK) Method

In the direct DH protocol, Alice and Bob lack an efficient channel to guard their communication against jamming. From Section III, we see that channel fading in conjunction with cooperative jamming provides a mechanism for generating an information-theoretic secret key, but an important realization is that the packet loss technique of Section III is efficient only for short key exchanges (i.e., short packet transmissions where the process can be repeated to exploit the frequency-time fading characteristics). This brings us to the main idea behind our proposed Physical-Layer-Enhanced Key Exchange Method (PEK) – namely, first establish an ephemeral channel using a short key exchange based on a physical layer technique, and then exchange the long DH messages over the ephemeral channel to finally establish the long secret key.

The PEK method is summarized in Fig. 1, where, in Step 1, Alice randomly generates a spreading code for use in Steps 2 and 3 and sends this code over a frequency hopped
system with a publicly known hopping pattern. Upon decoding Alice’s message from Step 1, Bob extracts the ephemeral spreading code from it and sends his public message $DH_B$ on a frequency hopped pattern based on this code, and finally Alice does the same for her public message $DH_A$; thus the DH messages are carried on an efficient anti-jamming channel.

Fig. 4 summarizes how PEK works in terms of Alice’s actions. After sending a randomly generated short spreading code in Step 1, Alice starts listening on the corresponding band. If Bob was not able to decode the message containing the spreading code, he is not able to reply and Alice sends another spreading code. This repeats until Bob is able to decode Alice’s message to obtain the spreading code and replies with his DH-message, $DH_B$. If Alice can decode $DH_B$, she replies with her DH-message, $DH_A$. On the other hand, if Eve also receives the spreading code in Step 1, she is forced to jam the band to prevent Alice from decoding Bob’s possible reply, in which case the steps repeat again. The trade-off then is in the exchange of a large number of short messages (short code) and fewer long $DH$ messages.

The rates Alice and Bob choose for sending their messages determine the number of physical-layer symbols required per message and the probability that these messages are successfully decoded. In Step 1, Alice picks rate $R_1$ bits/symbol. Therefore, the message sent by Alice in Step 1 requires transmitting $k/R_1$ symbols. Alice sends this message with an SFH system and, hence, the probability that a node can receive this message is as given in (3) and (4). In Step 2, (and in the case where he decodes Alice’s message) Bob picks rate $R_2$ bits/symbol. Sending a $B$-bit $DH_B$ message, therefore, takes $B/R_2$ symbols. Since these symbols are sent on an FFH system, Bob picks $R_2$ such that the received SINR at Alice is enough to decode his message as long as the FFH transmission is not jammed (see (7)). Step 3 is very similar to Step 2 where Alice picks the rate $R_3$ for her FFH transmission of $DH_A$. Usually the SINR assumptions are symmetric for Bob and Alice and thus $R_3 = R_2$.

The relative benefit of the PEK method depends on how easy it is to send a short secret message from Alice to Bob that enables the formation of an ephemeral secret FFH channel. PEK will improve key exchange efficiency if the cost of establishing this channel is small compared to the cost of $DH$ messages exchanged without such an efficient channel, like the case plotted in Fig. 3. In the following, we analyze the performance of PEK under different scenarios moving from a simple to a more sophisticated attacker model.

### A. Passive Adversary Case

When the adversary is known to be passive (i.e., an eavesdropper), the scenario is identical to the classical wired eavesdropping case for which the standard Diffie-Hellman protocol suffices. The PEK method in this case incurs an additional cost in Step 1, which may not be required; however, an important point to note is that this additional exchange of bits is very small because delivering the spreading code in Step 1 will take a small number of trials under a passive adversary.

Another important case is where there is potentially a jamming adversary, but there is no active jamming during a certain key exchange session. In a real network scenario, an attacker may not always be actively jamming or may not even be present at a given time; thus, security protocols will need to be cognizant of this. In PEK, the probing of bands in Step 1 also serves as a check on whether there is intense jamming or not. If there are no jammers around, Steps 1 and 2 will be completed rather easily, hence enabling a lower cost in a low-threat environment. Thus, while PEK is designed for active adversarial cases, its performance is minimally affected in the passive adversary case. In comparison, methods proposed in [2], [12] suffer comparable cost in passive and active adversary cases.

### B. Jamming Adversary Case

We assume that there is a single jamming adversary who can both listen and jam at the same time (i.e., full-duplex). A larger number of adversaries will naturally degrade performance, since it is much less likely to simultaneously have a poor channel to each of many adversaries than to a single adversary. We leave the consideration of an increased number of adversaries to a future work.

We evaluate PEK in terms of how much transmit energy is spent by the legitimate nodes. We assume cooperative jamming is employed during the transmission of the message in Step 1 (see Section III-A) where energy is equally divided for transmission of Alice’s message and cooperative jamming. Note that an attacker may also employ a second antenna; however, the additional gain in PEK would be limited. In Step 1 of PEK, Eve can use multi-antenna for additional advantage in receiving the spreading code from Alice and to project away from cooperative jammer’s noise, i.e., separate the signal from artificial noise. However, as Alice probes different bands for a good channel, she is essentially also changing the projection of her message onto Eve’s antennas, hence making it difficult for Eve to continuously suppress the noise she suffers.

As can be seen in Fig. 4, when Alice sends the $k$-bit message (where $k$ is small, chosen as 32 bits) containing the short code and starts listening, one of four events can happen:

1) $B \cap E$: Failure (low-cost): Both Bob and Eve are not able to decode Alice’s message in Step 1 and hence both
miss the spreading code. Alice hears nothing in Step 2 on the FFH system based on the spreading code. The cost is \( k/R_1 \) symbols transmitted by Alice.

2) \( B \cap E : \text{Failure (low-cost)} \): Only Eve is able to decode Alice’s message. In Step 2, Alice hears potential noise on the FFH system due to Eve’s jamming. The cost is \( k/R_1 \) symbols transmitted by Alice.

3) \( B \cap E : \text{Failure (high-cost)} \): Both Bob and Eve decode Alice’s message. In Step 2, Bob replies with \( B \)-bit DH message, \( DH_B \). In worst case, Alice cannot decode this message due to jamming. The cost is \( (k/R_1 + B/R_2) \) symbols sent by Alice and Bob.

4) \( S = B \cap \bar{E} : \text{Success} \): Only Bob decodes Alice’s message. Bob replies with \( B \)-bit DH message. Alice decodes this message. The cost is \( (k/R_1 + B/R_2) \) symbols sent by Alice and Bob. Alice proceeds to Step 3.

Each of these four events has a probability obtained in a manner similar to (13); e.g., \( P(B \cap E) = (1 - P_{rv}(A \rightarrow B))P_{rv}(A \rightarrow E) \).

Alice repeats the above steps until the event \( B \cap \bar{E} \) occurs. Whenever Bob misses the spreading code, this results in a failure but with a low cost since \( k \) is a small number. However, when both Bob and Eve receive the code, this results in a failure with a high cost. In a typical scenario, Alice receives Bob’s DH-message after a series of failed attempts to either deliver the spreading code to Bob (\( B \cap E \) or \( B \cap \bar{E} \)) or to hear Bob’s response in jamming (\( E \cap B \)). Fig. 5 shows how this process works on the time-frequency plane. Let \( N_1 \) be the random variable denoting the number of symbols transmitted starting with Alice’s first transmission until she successfully decodes Bob’s DH-message. Then,

\[
E(N_1) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \left( m+1 \right) \left( \frac{k}{R_1} + \frac{B}{R_2} + n \frac{k}{R_1} \right) \left( m+n \right) \left( \frac{m}{m+n} \right) p_{B \cap E} p_{B \cap E} \rho_{PS},
\]

where \( m \) denotes the number of high-cost failures (i.e., \( B \cap E \)) and \( n \) denotes the number of low-cost failures (i.e., \( B = (B \cap E) \cup (B \cap \bar{E}) \)). \( p_X \) denotes the probability of event \( X \).

The last step to complete secret key exchange is Step 3, where upon receiving Bob’s DH-message, Alice replies with her \( B \)-bit \( DH_A \) message with rate \( R_3 \) on the same FFH pattern that Bob employed to transmit \( DH_B \) to her. As noted above, due to similar SINR assumptions, \( R_3 \) will typically be the same as \( R_2 \). Per (7), \( DH_A \) will be received as long as this assumption is valid, i.e., \( DH_A \) will be delivered in one attempt and will require \( N_2 = B/R_3 = B/R_2 \) symbols. Therefore, the expected number of total symbols sent during key establishment by PEK is given by

\[
E(N) = E(N_1) + B/R_2. \tag{15}
\]

In Fig. 6, we plot the expected number of symbol transmissions by the legitimate nodes to establish a secret key. Again, we assume Alice and Bob are a fixed distance \( d_{AB} \) apart and Eve is located on the line between Alice and Bob in a given range. Worst-case assumption on jamming intensity depends on how large this range is. Note that Alice and Bob optimize their communication rates depending on this assumption. Plots show that for all the considered ranges Eve might span, PEK requires almost half the transmit energy compared to a direct DH key exchange, so employing PEK enhances the efficiency of secret key exchange. This means the extra energy spent in PEK to form a secret ephemeral channel is justified by the reduced cost in exchanging DH-messages in latter steps.

C. Message Insertion by Attacker

We consider an attacker which is capable, in addition to eavesdropping and jamming with random noise, of inserting her own messages into the medium. These fake messages can be in the form of a fake FFH code in Step 1 of PEK or
messages by two nodes who share no prior symmetric secrets, and hence, lack a secure channel to guard their communication against disruption. Therefore, message transfers have to be done over a public wireless channel. An active adversary can exploit this and cause significant cost to key exchange by jamming. We describe a physical layer communication model and analyze the communication cost of secret key exchange in the presence of a jamming adversary. Then, we propose a method where a short spreading code is first transmitted to form an ephemeral channel to carry the long messages required for key exchange. In order for the spreading code to be secret between nodes, we exploit the time- and frequency-dependent randomness in wireless channels which causes inevitable packet losses to a possible attacker. We analytically show that establishing a temporary channel to do key exchange results in increased overall efficiency compared to the case where message exchanges are done without an efficient channel.

V. SUMMARY AND CONCLUSIONS

We address the problem of secret key exchange over a wireless channel. Secret key exchange requires exchanging long messages by two nodes who share no prior symmetric secrets, a fake DH-message. Note that we assume an authenticated DH protocol for key exchange, which means any fake DH-message will fail authentication. However, the time wasted receiving an attacker’s message and/or energy spent replying an attacker can cause inefficiency to the PEK Method. The case of message insertion is discussed in detail in [17] and omitted here due to space constraints.

REFERENCES