Secure Wireless Key Establishment Using Retrodirective Array

Secure Wireless Key Establishment Using Retrodirective Array

Yuan Ding, Junqing Zhang, Vincent Fusco
Institute of Electronics, Communications and Information Technology (ECIT), Queen's University of Belfast,
Belfast, United Kingdom, BT3 9DT
E-mail: yding03@qub.ac.uk; jzhang20@qub.ac.uk; v.fusco@ecit.qub.ac.uk

***Abstract*—In this paper a new method of establishing secret keys for wireless communications is proposed. A retrodirective array (RDA) that is configured to receive and re-transmit at different frequencies is utilized as a relay node. Specifically the analogue RDA is able to respond in 'real-time', reducing the required number of time slots for key establishment to two, compared with at least three in previous relay key generation schemes. More importantly, in the proposed architecture equivalent reciprocal wireless channels between legitimate keying nodes can be randomly updated within one channel coherence time period, leading to greatly increased key generation rates (KGRs) in slow fading environment. The secrecy performance of this RDA assisted key generation system is evaluated and it is shown that it outperforms previous relay key generation systems.**

***Index Terms*—Retrodirective array, key generation, wireless communication.**

I. Introduction

Mobile wireless communication has experienced an unprecedented growth in recent years presenting many enterprise opportunities. Along with these opportunities there are attendant risks. Wireless communications allow information flow via broadcasting, which indicates unintended receivers, namely eavesdroppers, can also receive and decode these information. Currently sensitive transmission data is encrypted at the upper protocol layers through mathematical cryptographic operations [1]. Recently the potential for the efficacy of such mathematical encryption schemes to be mitigated has been under discussion [2]. Furthermore, requirements related to trusted key management infrastructure may render conventional cryptographic method less applicable for some wireless systems, such as ad-hoc networks and low-cost wireless sensor networks [3].

Distinct from the upper layer cryptographic approaches, physical layer security techniques aim to achieve information-theoretic security. This implies that the achieved level of security will not be compromised even if an unauthorized third party has unlimited computational capability [4]. Various types of physical layer security solutions have been investigated, including keyless secure transmission [5], directional modulation [6], and key establishment from wireless channels [7]. For wireless key establishment scheme, the secret keys are generated by exploiting randomness of reciprocal propagation channels between keying nodes [7]. The information theoretical foundation of this key establishment approach was given in [8].

There are several characteristics of wireless channels that can be utilized to extract secret keys, such as received signal strength (RSS) [9], channel phase delays [10], multipath relative time delays [11], and full channel state information (CSI) [12]. These parameters are available in network interface cards or customized hardware platforms, therefore many practical key generation systems have been reported [7].

A number of approaches have been proposed to increase key generation rate (KGR) without degrading key disagreement rate (KDR). KGR describes the amount of key bits generated per time unit, and KDR denotes bit disagreement rates of the generated keys shared by legitimate nodes. In [9], [13] multiple nodes or multiple antennas at each node are exploited in order to create multiple usable common channels from which more key bits can be extracted within one channel coherence time period. Similarly, multiple independent or quasi-independent channels can be generated using frequency resources, such as channel hopping in [14], and OFDM signals in [12]. A concept ultilizing random beamforming was proposed in [14], [15]. Here the excitation weights of multi-antenna nodes are randomly updated during each key generation round, such that a controlled artificial 'fast fading' channel is created. As a consequence, more independent random secret key bits can be generated by repeated channel probing within one channel coherence time period.

In addition to the above methods, helper or relay nodes have been introduced in [16]–[18] to further enhance the key generation performance. Apart from creating more usable channels, the relay nodes can also help generate artificial noise [16], [17], which contaminates the intercepted signals received by eavesdroppers, or helps enhance the randomness of the channel characteristics [17], [18], in such a fashion to increase secret key rates.

In this paper we propose a new type of relay key generation architecture, which uses a retrodirective array (RDA) [19] as a relay node. This arrangement has the following unique characteristics that do not exist in current relay key generation systems:

a) the RDA relay node can be implemented in an analogue fashion thereby allowing low power consumption and the real-time response. The RDA node does not need to have any additional digital calculation capabilities;
b) since the RDA can operate without demodulating signals nor estimating channels, the potential for the relay node

to leak information intentionally or unintentionally is significantly reduced, i.e., it can be considered as a trusted node;

c) no system parameters including CSI, training sequences, and time-slot assignment are required by the RDA relay node;

d) multiple channel measurements can be conducted within one coherence time period, greatly increasing the achievable KGR. This is because with the help of the RDA the equivalent channel can be manipulated to be 'fast fading';

e) only two time slots are required for each key generation round, compared with at least three time slots in previous relay key generation protocols [17].

This paper is organized as follows. In Section II system models including statistical multipath channels and RDAs used throughout the paper are described. The RDA assisted key generation architecture and protocol, and eavesdropping strategies are presented in Section III. In Section IV the secret key rates of the proposed system are simulated and compared with previous relay key generation systems. Finally conclusions are drawn in Section V.

Throughout this paper, the following notations will be used: Boldface lower case and capital letters, e.g., $\boldsymbol{h}$ and $\boldsymbol{H}$, denote parameters in time and frequency domains, respectively, and they are complex numbers. Boldface capital letter with an arrow on top, e.g., $\vec{\boldsymbol{H}}$, refers to a vector, whose elements are parameters in frequency domain. Letters with superscripts RDA and r correspond to parameters in the proposed RDA and previous relay key generation systems. '$[\cdot]^*$' denotes complex conjugate operator, and '$\circ$' is the Hadamard product of two vectors. '$[x]^+$' returns zero if x is less than zero otherwise returns x.

II. System Model

A. Statistical Multipath Channel Model

In this paper a dynamic multipath-rich Rayleigh wireless propagation channel is considered. The channel impulse response (CIR) can be written as

$$\boldsymbol{h}(\tau, t) = \sum_{l=0}^{L-1} \boldsymbol{h}(\tau_l, t)\delta(\tau - \tau_l), \tag{1}$$

where $\boldsymbol{h}(\tau_l, t)$ is a complex number representing the attenuation and phase delay of the l^{th} $(l = 0, 1, ..., L-1)$ propagation path, i.e., channel taps, between communication nodes at the time instant t. τ_l refers to the time delay of the l^{th} channel tap relative to the corresponding t. $\delta(\cdot)$ is the Dirac delta function. It is assumed that, a) at each time instant the total number of channel taps, i.e., L, is identical, b) τ_l starts from zero and is uniformly spaced in time. Thus it can be expressed as $\tau_l = lT$, where T is normally determined by the sampling period of the hardware, c) the scattering multipath in the channel is sufficiently rich that the $\boldsymbol{h}(\tau_l, t)$ follows zero-mean complex Gaussian distribution, i.e., $\boldsymbol{h}(\tau_l, t) \sim CN(0, \sigma_{hl}^2)$ [20].

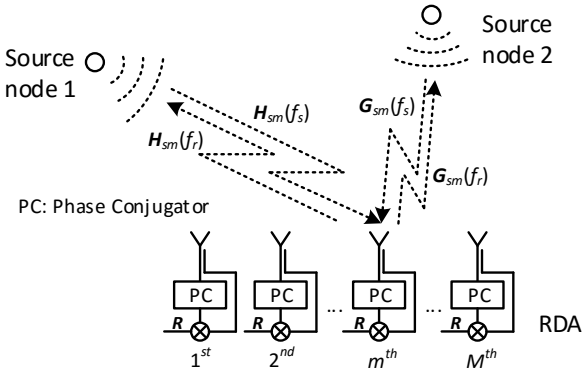

Fig. 1. RDA operating principle.

When taking Fourier transform of (1), the channel frequency response (CFR) can be obtained, and is given as

$$\boldsymbol{H}(f, t) = \sum_{l=0}^{L-1} \boldsymbol{h}(\tau_l, t)e^{-j2\pi f \tau_l}. \tag{2}$$

Unless otherwise specified, all of the simulation results presented in this paper are based on the following channel parameters for a typical wireless indoor environment [21].

- The sampling period T is set to 50 ns;
- The average power of each channel tap follows an exponential decay power delay profile with root mean square (RMS) delay spread σ_τ of 50 ns, from which the number of channel taps can be calculated to be 11;
- A bell-shaped Doppler power spectral density with Doppler spread f_d of 10 Hz is used.

B. Retrodirective Arrays (RDAs)

Before describing the RDA relay key generation system in Section III, RDA operation is briefly presented here. An RDA has the capability to re-transmit a signal back along the spatial direction(s), along which the array was illuminated by the incoming signals without the need for a-priori knowledge of their points of origin [19]. The core element of an RDA that enables the tracking functionality is the phase conjugator unit [22]. Among many forms of phase conjugator units, active analogue types are attractive due to their low power consumption, real-time response, and frequency reconfiguration flexibility [23], [24].

The basic operation upon which an RDA is predicated is illustrated by way of an example shown in Fig. 1. Two distant sources emit pilot signals $\boldsymbol{s}_1(t)$ and $\boldsymbol{s}_2(t)$, respectively at frequency f_s. The detected signal in the frequency domain at the m^{th} $(m = 1, 2, ..., M)$ RDA element can be expressed as $\boldsymbol{S}_1(f_s)\boldsymbol{H}_{sm}(f_s) + \boldsymbol{S}_2(f_s)\boldsymbol{G}_{sm}(f_s)$, where the $\boldsymbol{S}_{\{1,2\}}(f_s)$ and $\{\boldsymbol{H}, \boldsymbol{G}\}_{sm}(f_s)$ are, respectively, the Fourier representations of the pilot signal $\boldsymbol{s}_{\{1,2\}}(t)$ and the propagation channel $\{\boldsymbol{h}, \boldsymbol{g}\}_{sm}(t)$ between the sources and the m^{th} RDA antenna element. After the detected signal is processed through a phase conjugator, it becomes $[\boldsymbol{S}_1(f_s)\boldsymbol{H}_{sm}(f_s)]^* + [\boldsymbol{S}_2(f_s)\boldsymbol{G}_{sm}(f_s)]^*$. When re-transmitting $[\boldsymbol{S}_1(f_s)\boldsymbol{H}_{sm}(f_s)]^* + [\boldsymbol{S}_2(f_s)\boldsymbol{G}_{sm}(f_s)]^*$ weighted local signal $\boldsymbol{C}$ at frequency f_r by the RDA, the

received signal $\boldsymbol{Y}_1(f_r)$ at the source node 1 can be written as in (3),

$$\boldsymbol{Y}_1(f_r) = \sum_{m=1}^{M} \boldsymbol{C}\Big\{[\boldsymbol{S}_1(f_s)\boldsymbol{H}_{sm}(f_s)]^* + [\boldsymbol{S}_2(f_s)\boldsymbol{G}_{sm}(f_s)]^*\Big\}\boldsymbol{H}_{sm}(f_r). \quad (3)$$

When $f_r = f_s$, (4) can, in the absence of noise, be expressed as

$$\boldsymbol{Y}_1(f_s) = \boldsymbol{C}\boldsymbol{S}_1^*(f_s)\sum_{m=1}^{M}|\boldsymbol{H}_{sm}(f_s)|^2 + \boldsymbol{C}\boldsymbol{S}_2^*(f_s)\sum_{m=1}^{M}\boldsymbol{G}_{sm}^*(f_s)\boldsymbol{H}_{sm}(f_s). \quad (4)$$

Here the channel reciprocity is assumed. For the received signal $\boldsymbol{Y}_2(f_r)$ at the source node 2 similar expressions can be obtained, and thus is omitted here.

The first term on the right hand side in (4) represents the beamforming gain towards the source node 1, while the second term normally is quite small compared with the first term due to the fact that $\boldsymbol{G}_{sm}$ and $\boldsymbol{H}_{sm}$ are independent.

When $f_r \neq f_s$, as occurs in full-duplex RDAs, the re-transmission channel $\{\boldsymbol{H},\boldsymbol{G}\}_{sm}(f_r) \neq \{\boldsymbol{H},\boldsymbol{G}\}_{sm}(f_s)$. In free space $\{\boldsymbol{H},\boldsymbol{G}\}_{sm}(f_r)$ and $\{\boldsymbol{H},\boldsymbol{G}\}_{sm}(f_s)$ can be directly linked by compensating their frequency differences [25], thus after channel coefficient calibration (4) still holds. The scenario of RDAs in multipath environments when $f_r \neq f_s$, which is considered in this paper, normally results in reduced beamforming gains. The amount of reduction is determined by the channel parameters, the number of RDA antenna elements, and the frequency difference between receive and re-transmit. For the simulation results presented in Section IV, the following parameters are used: $\sigma_\tau = 50$ ns, $M = 9$. The frequency configuration will be presented in Section IV.

III. RDA Assisted Wireless Key Generation

In this section RDA assisted key generation system is presented and the associated adversary model is investigated.

A. RDA Assisted Key Generation

The model of the proposed RDA assisted key generation system is illustrated in Fig. 2. The nodes Alice and Bob intend to establish a shared common key with the help of an M-antenna RDA node. These three nodes are termed legitimate nodes hereafter. In this paper we assume Alice and Bob are both equipped with a single antenna. Not discussed in this paper are multiple-antenna cases which can be investigated using similar methods to those in [26] for MIMO key generation scenarios.

Each key generation round only comprises two time slots (**TS**1, 2), which are now described;

TS1) Alice and Bob locally generate random and independent signals $\boldsymbol{U}_i$ and $\boldsymbol{V}_i$, respectively, and then radiate them at an identical frequency f_1. Here the subscript 'i' refers to the i^{th} key generation round. In order to simplify notation, the subscript 'i' is omitted later in most cases. In order to facilitate signal to noise ratio (SNR) definition later, it is assumed that $E[\boldsymbol{U}] = E[\boldsymbol{V}] = 0$, and $E\left[|\boldsymbol{U}|^2\right] = E\left[|\boldsymbol{V}|^2\right] = 1$. Alice and Bob do not need to know or store the values of $\boldsymbol{U}$ and $\boldsymbol{V}$. The detected signal vector $\vec{\boldsymbol{W}}_b$ at the RDA can be expressed as

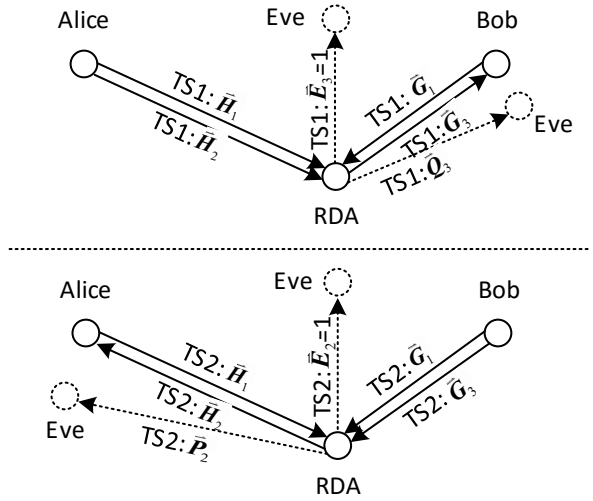

Fig. 2. Proposed RDA assisted wireless key generation system model.

$$\vec{\boldsymbol{W}}_b = q_{1b}^{1/2}(\vec{\boldsymbol{H}}_1\boldsymbol{U} + \vec{\boldsymbol{G}}_1\boldsymbol{V}) + \vec{\boldsymbol{N}}_{1b}, \quad (5)$$

where the m^{th} entry $\boldsymbol{H}_{mx}$ ($\boldsymbol{G}_{mx}$) of the vector $\vec{\boldsymbol{H}}_x$ ($\vec{\boldsymbol{G}}_x$) represents the channel coefficient between Alice (Bob) and the m^{th} RDA element at frequency f_x ($x = 1, 2, 3$), see Fig. 2. $\vec{\boldsymbol{N}}_{xy}$ ($y = a, b$) is the frequency representation of the additive Gaussian white noise (AWGN) $\vec{n}_{xy}$, whose elements follow $CN(0, \sigma_n^2)$, and all are independent. $q_{xy}^{1/2}$ is a scaling coefficient involving both the amplification factor at transmitter sides and propagation path loss, and it is used to set required SNR at receiver sides. Here the $\frac{1}{M}\sum_{m=1}^{M} E\left[\,|\boldsymbol{H}_{m1}\boldsymbol{U} + \boldsymbol{G}_{m1}\boldsymbol{V}|^2\,\right]$ is normalized to be unity. The RDA cannot separate the two signals transmitted by Alice and Bob because both signals are at the same frequency, and are occurring at the same time, and none of $\boldsymbol{H}_{m1}$, $\boldsymbol{G}_{m1}$, $\boldsymbol{U}$, and $\boldsymbol{V}$ are known.

At the same time Alice transmits a publicly known training sequence $\boldsymbol{X}$ at a different frequency f_2 ($f_2 \neq f_1$). The received signal vector at the RDA node at frequency f_2 is $q_{2b}^{1/2}\vec{\boldsymbol{H}}_2\boldsymbol{X} + \vec{\boldsymbol{N}}_{2b}$. Here $\vec{\boldsymbol{H}}_2$ is normalized such that

$$\frac{1}{M}\sum_{m=1}^{M} E\left[|\boldsymbol{H}_{m2}|^2\right] = 1, \quad (6)$$

seen in Fig. 2. Then the $\vec{\boldsymbol{W}}_b^*$ weighted $q_{2b}^{1/2}\vec{\boldsymbol{H}}_2\boldsymbol{X} + \vec{\boldsymbol{N}}_{2b}$ is radiated by the RDA at frequency f_3 ($f_3 \neq f_2, f_3 \neq f_1$).

At the Bob the detected signal $\boldsymbol{S}_b$ at frequency f_3 can be written as

$$\boldsymbol{S}_b = q_{3b}^{1/2}\vec{\boldsymbol{G}}_3 \cdot \left[\vec{\boldsymbol{W}}_b^* \circ \left(q_{2b}^{1/2}\vec{\boldsymbol{H}}_2\boldsymbol{X} + \vec{\boldsymbol{N}}_{2b}\right)\right] + \boldsymbol{N}_{3b}. \quad (7)$$

Similarly $\vec{\boldsymbol{G}}_3$ is normalized to be

$$\frac{1}{M}\sum_{m=1}^{M} E[|\boldsymbol{G}_{m3}|^2] = 1. \tag{8}$$

Since $\boldsymbol{X}$ is publicly known to every node in the system, Bob is able to obtain the waveform observation $\boldsymbol{K}_b$, which in the frequency domain for the purpose of secret key extraction is shown in (9).

$$\begin{aligned}\boldsymbol{K}_b =& q_{3b}^{1/2} q_{2b}^{1/2} \vec{\boldsymbol{G}}_3 \cdot \left(\vec{\boldsymbol{W}}_b^* \circ \vec{\boldsymbol{H}}_2\right) \\ &+ q_{3b}^{1/2} \vec{\boldsymbol{G}}_3 \cdot \left(\vec{\boldsymbol{W}}_b^* \circ \vec{\boldsymbol{N}}_{2b}\right) / \boldsymbol{X} + \boldsymbol{N}_{3b} / \boldsymbol{X}\end{aligned} \tag{9}$$

TS2) In time slot 2, $\boldsymbol{U}$ and $\boldsymbol{V}$ transmitted by Alice and Bob at frequency f_1 are still present, which generates $\vec{\boldsymbol{W}}_a$ at the RDA node, seen in (10).

$$\vec{\boldsymbol{W}}_a = q_{1a}^{1/2} \left(\vec{\boldsymbol{H}}_1 \boldsymbol{U} + \vec{\boldsymbol{G}}_1 \boldsymbol{V}\right) + \vec{\boldsymbol{N}}_{1a} \tag{10}$$

In this time slot Bob transmits the same known $\boldsymbol{X}$ at frequency f_3, which, after being weighted with $\vec{\boldsymbol{W}}_a^*$, is re-transmitted by the RDA at frequency f_2. When the known $\boldsymbol{X}$ is equalized, the waveform $\boldsymbol{K}_a$ shown in (11) can be acquired by Alice.

$$\begin{aligned}\boldsymbol{K}_a =& q_{2a}^{1/2} q_{3a}^{1/2} \vec{\boldsymbol{H}}_2 \cdot \left(\vec{\boldsymbol{W}}_a^* \circ \vec{\boldsymbol{G}}_3\right) \\ &+ q_{2a}^{1/2} \vec{\boldsymbol{H}}_2 \cdot \left(\vec{\boldsymbol{W}}_a^* \circ \vec{\boldsymbol{N}}_{3a}\right) / \boldsymbol{X} + \boldsymbol{N}_{2a} / \boldsymbol{X}\end{aligned} \tag{11}$$

From the first term of the obtained $\boldsymbol{K}_a$ in (11) at Alice node and the first term of the obtained $\boldsymbol{K}_b$ in (9) at Bob node, a common secret key can be generated and shared. It is noted that $\vec{\boldsymbol{G}}_3 \cdot \left(\vec{\boldsymbol{W}}_{\{a,b\}}^* \circ \vec{\boldsymbol{H}}_2\right)$ and $\vec{\boldsymbol{H}}_2 \cdot \left(\vec{\boldsymbol{W}}_{\{a,b\}}^* \circ \vec{\boldsymbol{G}}_3\right)$ are equivalent. The noise terms, i.e., the last two terms in both (9) and (11), reduce the correlation coefficients between $\boldsymbol{K}_a$ and $\boldsymbol{K}_b$, and hence limit the achievable secret key rates of the proposed system. These aspects are investigated in Section IV.

It is worth pointing out that even within one channel coherence time period, i.e., $\vec{\boldsymbol{H}}_1$, $\vec{\boldsymbol{G}}_1$, $\vec{\boldsymbol{H}}_2$, and $\vec{\boldsymbol{G}}_3$ remain unchanged, the equivalent common channel observation $\vec{\boldsymbol{H}}_2 \cdot \left(\vec{\boldsymbol{W}}_{\{a,b\}}^* \circ \vec{\boldsymbol{G}}_3\right)$ still varies, and for different key generation rounds they are uncorrelated. This is achieved by randomly choosing $\boldsymbol{U}_i$ and $\boldsymbol{V}_i$, which are unknown to any of the nodes in the system, in each key generation round. In other words, many key generation rounds can be performed within one channel coherence time period, leading to a greatly increased KGR.

B. Eavesdropping Strategies

In this paper it is assumed that:

- Eve knows the key generation procedures described in the previous subsection;
- Eve knows the training sequence $\boldsymbol{X}$;
- No colluding Eves are considered.

Eve can adopt a number of strategies for eavesdropping, such as directly observing one of the legitimate nodes, and placing Eve's antenna close to one of the legitimate nodes. Among these options, placing Eve's antenna close to Alice or Bob is the most effective way in terms of interception, because the eavesdropping channel between Eve and the RDA is correlated to the legitimate channel between Alice (or Bob) and the RDA. Without loss of generality, it is assumed that Eve's antenna is placed close to Alice in order to facilitate the following formulation. In this case the eavesdropping channel vector at frequency f_2, denoted as $\vec{\boldsymbol{P}}_2$, seen in Fig. 2, is correlated to $\vec{\boldsymbol{H}}_2$ through the correlation coefficient ρ_{ae}^{RDA} expressed in (12). Here only real part, i.e., $Re(\cdot)$, is considered.

$$\rho_{ae}^{RDA} = \frac{1}{M}\sum_{m=1}^{M} \frac{E\left[Re(\boldsymbol{P}_{m2}) Re(\boldsymbol{H}_{m2})\right]}{\sqrt{E\left[\left(Re(\boldsymbol{P}_{m2})\right)^2\right] E\left[\left(Re(\boldsymbol{H}_{m2})\right)^2\right]}} \tag{12}$$

Eve cannot estimate $\vec{\boldsymbol{P}}_2$, and hence $\vec{\boldsymbol{H}}_2$, since $q_{2a}^{1/2} q_{3a}^{1/2} \left(\vec{\boldsymbol{W}}_a^* \circ \vec{\boldsymbol{G}}_3\right) \boldsymbol{X} + q_{2a}^{1/2} \left(\vec{\boldsymbol{W}}_a^* \circ \vec{\boldsymbol{N}}_{3a}\right)$ radiated by the RDA is unknown to any nodes in the system. Fortunately, from Eve's point of view, she does not need to know $\vec{\boldsymbol{H}}_2$. It is better for her to estimate $\boldsymbol{K}_a$ as a whole directly. The obtained waveform, $\boldsymbol{K}_e$, used for estimation can be written as

$$\begin{aligned}\boldsymbol{K}_e =& q_{2a}^{1/2} q_{3a}^{1/2} \vec{\boldsymbol{P}}_2 \cdot \left(\vec{\boldsymbol{W}}_a^* \circ \vec{\boldsymbol{G}}_3\right) \\ &+ q_{2a}^{1/2} \vec{\boldsymbol{P}}_2 \cdot \left(\vec{\boldsymbol{W}}_a^* \circ \vec{\boldsymbol{N}}_{3a}\right) / \boldsymbol{X} + \boldsymbol{N}_{2e} / \boldsymbol{X},\end{aligned} \tag{13}$$

where channel noise $\boldsymbol{N}_{2e}$ at the Eve node is assumed to have the same distribution as $\boldsymbol{N}_{2a}$.

IV. Secrecy Performance Evaluation

In this section the secrecy performance, i.e., secret key rates expressed in (14), [8], of the proposed RDA assisted key generation system is evaluated, and compared with those in previous relay systems. The previous relay key generation systems used for comparison are schemes described in [17]. For system simulation results presented in this section, the *knn* distance method [27] is adopted for mutual information estimation.

$$\begin{aligned}R_s^{RDA} = &\Big[I\Big(Re\left(\boldsymbol{K}_a\right); Re\left(\boldsymbol{K}_b\right)\Big) - \\ &\min\Big(I\Big(Re\left(\boldsymbol{K}_a\right); Re\left(\boldsymbol{K}_e\right)\Big), I\Big(Re\left(\boldsymbol{K}_b\right); Re\left(\boldsymbol{K}_e\right)\Big)\Big)\Big]^+\end{aligned} \tag{14}$$

The calculated secret key rates R_s^{RDA} in the proposed RDA assisted key generation systems are shown in Fig. 3. In the simulation it is assumed that the RDA is equipped with 9 antenna elements, and the $\Delta f = f_3 - f_2 = f_2 - f_1$ is chosen as 2 MHz. The magnitudes of $\boldsymbol{U}$ and $\boldsymbol{V}$ are set to be unity with their phase uniformly distributed within the range of 0 to 2π. The SNRs in all transmission links in the key generation process are assumed to be identical, i.e.,

$$SNR^{RDA} = q_{1a}/\sigma_n^2 = q_{3a}/\sigma_n^2 = q_{1a} q_{2a} q_{3a}/\sigma_n^2. \tag{15}$$

In [17] four relay key generation schemes were presented, which are classified by the authors as amplify-and-forward (AF), signal-combining amplify-and-forward (SC-AF), multiple-access amplify-and-forward (MA-AF), and amplify-and-forward with artificial noise (AF-AN). The AF scheme, as the authors pointed out, is not secure when the

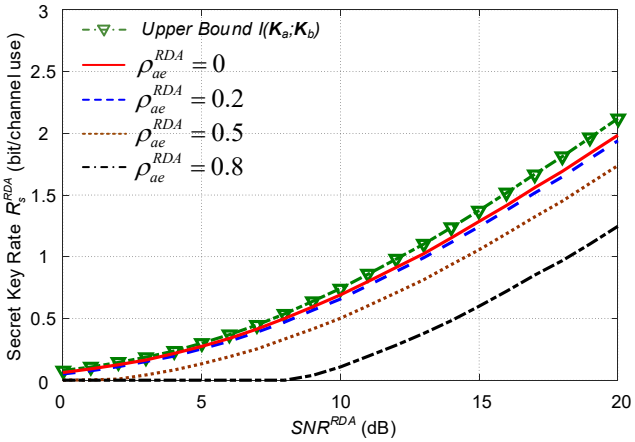

Fig. 3. Calculated secret key rates R_s^{RDA} in 9-element RDA assisted key generation systems as functions of SNR^{RDA} when Eve's antenna is placed close to Alice. (σ_τ = 50 ns and Δf = 2 MHz)

relay is monitored by Eve. The AF-AN scheme relies on the design of the artificial noise that is projected by the relay node towards Eve, but not Alice and Bob. For the architecture proposed in this paper, the generation of artificial noise using RDA for the benefit of wireless key generations will be presented separately in the future. Compared with the SC-AF, the MA-AF reduces the number of required time slots for a single key generation round from four to three at the cost of requirement for synchronization between Alice and Bob. The secret key rates in the SC-AF and MA-AF systems are almost identical when the unit 'bit/channel use' is adopted. They are both denoted as R_s^r in this paper.

In order to facilitate discussion in this paper, the waveforms acquired at Alice and Bob used for key generation purpose in the SC-AF scheme are presented in (16) and (17).

$$\begin{aligned}\boldsymbol{K}_a^r =& \frac{1}{\sqrt{2}}\left[q_{r1}^{1/2}(\vec{\boldsymbol{H}}^r + \vec{\boldsymbol{G}}^r) + \vec{\boldsymbol{N}}_{a2}^r + \vec{\boldsymbol{N}}_{b2}^r\right]\cdot\vec{\boldsymbol{H}}^r + \boldsymbol{N}_{a3}^r \\ &- \left(q_{r1}^{1/4}\vec{\boldsymbol{H}}^r + \frac{\vec{\boldsymbol{N}}_{a1}^r}{q_{r1}^{1/4}}\right)\cdot\left(q_{r1}^{1/4}\vec{\boldsymbol{H}}^r + \frac{\vec{\boldsymbol{N}}_{a1}^r}{q_{r1}^{1/4}}\right) \end{aligned} \tag{16}$$

$$\begin{aligned}\boldsymbol{K}_b^r =& \frac{1}{\sqrt{2}}\left[q_{r1}^{1/2}(\vec{\boldsymbol{H}}^r + \vec{\boldsymbol{G}}^r) + \vec{\boldsymbol{N}}_{a2}^r + \vec{\boldsymbol{N}}_{b2}^r\right]\cdot\vec{\boldsymbol{G}}^r + \boldsymbol{N}_{b3}^r \\ &- \left(q_{r1}^{1/4}\vec{\boldsymbol{G}}^r + \frac{\vec{\boldsymbol{N}}_{b1}^r}{q_{r1}^{1/4}}\right)\cdot\left(q_{r1}^{1/4}\vec{\boldsymbol{G}}^r + \frac{\vec{\boldsymbol{N}}_{b1}^r}{q_{r1}^{1/4}}\right) \end{aligned} \tag{17}$$

$\vec{\boldsymbol{H}}^r$ ($\vec{\boldsymbol{G}}^r$) refers to the Rayleigh wireless channel between Alice (Bob) and the relay. They are independent, and are normalized to be

$$\frac{1}{M}\sum_{m=1}^{M} E[\,|\boldsymbol{H}_m^r|^2\,] = \frac{1}{M}\sum_{m=1}^{M} E[\,|\boldsymbol{G}_m^r|^2\,] = 1. \tag{18}$$

It is assumed that all of the noise terms are independent and follow $CN(0,\sigma_r^2)$. The SNRs of signal transmissions in each step in the SC-AF key generation process are set to be identical, denoted as

$$SNR^r = q_{r1}/\sigma_r^2. \tag{19}$$

The secret key rates R_s^r in the SC-AF and MA-AF schemes are defined the same as R_s^{RDA} in (14) with $\boldsymbol{K}_{\{a,b,e\}}$ being replaced with their counterparts $\boldsymbol{K}_{\{a,b,e\}}^r$. Here $\boldsymbol{K}_e^r$, used for R_s^r calculation in Fig. 4, is the detected waveform by Eve which is placed close to Alice. In this case, a pair of legitimate and eavesdropping channels with correlation coefficient ρ_{ae}^r is created. Clearly, it can be concluded that more noise involved in the SC-AF (MA-AF) key generation systems, seen in (16) and (17), reduces the achieved secret key rates R_s^r significantly, when the channel SNRs are identical.

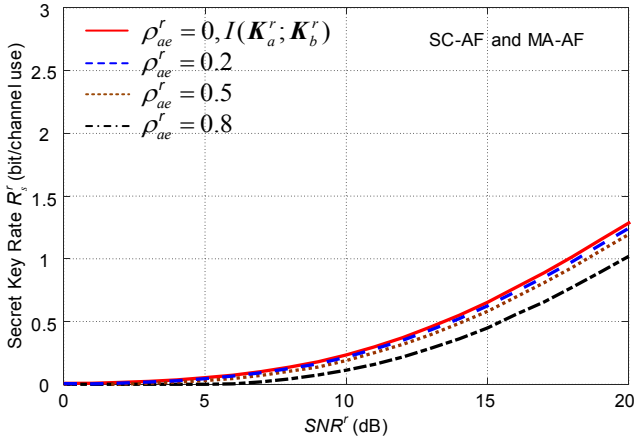

Fig. 4. Calculated secret key rates R_s^r in SC-AF and MA-AF key generation systems as a function of SNR^r when Eve's antenna is placed close to Alice.

From Figs. 3 and 4 it can be concluded that the proposed RDA assisted key generation system outperforms, with regard to secrecy performance, both the previous SC-AF and MA-AF relay key generation systems in [17].

Table I summarizes the characteristics of the SC-AF, the MA-AF, and the proposed RDA assisted wireless key generation systems. Another advantage of using RDA as a relay node, which is not discussed before in this paper, is the high flexibility of adjusting transmission gains from the relay to Alice (Bob). This can be readily achieved by altering the ratio between $|\boldsymbol{U}|^2$ and $|\boldsymbol{V}|^2$ at Alice and Bob nodes, which is proportional to the ratio between power gains towards Alice and Bob [28].

V. Conclusion

A new type of wireless key generation system architecture, using an RDA as a relay node, was proposed and analyzed in this paper. By configuring analogue RDAs receive and retransmit at different frequencies, the number of time slots required for each key generation process was reduced to two. Furthermore, the equivalent reciprocal wireless channels between legitimate keying nodes can be controlled, by Alice and Bob, to be 'fast fading', which is able to increase KGRs significantly. Also distinct from the previous relay based key

TABLE I
SUMMARY OF CHARACTERISTICS OF SC-AF, MA-AF, AND PROPOSED RDA ASSISTED KEY GENERATION SYSTEMS.

	SC-AF	MA-AF	RDA
Number of required time slots	4	3	2
Nodes requiring knowledge for time slots	Alice, Bob, and relay	Alice, Bob, and relay	Alice and Bob
Strict time synchronization	No	Yes	No
Requirement for calculation capability in the relay node	Yes	Yes	No
R_s when Eve's antenna is placed close to Alice or Bob	Low (Fig. 4)	Low (Fig. 4)	High (Fig. 3)
Multiple key generation rounds within one channel coherence time period	No	No	Yes

generation systems, the RDAs employed do not need to have additional digital computational capability, and do not need to acquire knowledge about system parameters, such as time slots assignment and training sequences, which makes this architecture more flexible in terms of adding more legitimate keying nodes and/or more RDA relay nodes. Through simulations it was shown that the proposed RDA assisted key generation systems have better secrecy performance than that in the previous relay key generation systems.

REFERENCES

[1] A. Kahate, *Cryptography and Network Security*, 3rd ed. New Delhi: Tata McGraw-Hill Education, 2013.

[2] A. JA. (2015, Sept.) Will quantum computers threaten modern cryptography? [Online]. Available: http://www.tripwire.com/state-of-security/featured/will-quantum-computers-threaten-modern-cryptography

[3] A.-S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges," in *Proc. 8th Int. Conf. Adv. Commun. Technol., (ICACT)*, vol. 2, Phoenix Park, Feb. 2006, pp. 1043–1048.

[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[6] Y. Ding and V. Fusco, "A review of directional modulation technology," *International Journal of Microwave and Wireless Technologies*, pp. 1–13, Jul. 2015.

[7] J. Zhang, T. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, Mar. 2016.

[8] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[9] S. N. Premnath, J. Croft, N. Patwari, and S. K. Kasera, "Efficient high-rate secret key extraction in wireless sensor networks using collaboration," *ACM Trans. Networking*, vol. 11, no. 1, p. 2, 2014.

[10] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Select. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.

[11] J. Huang and T. Jiang, "Secret key generation exploiting ultra-wideband indoor wireless channel characteristics," *Security and Commun. Networks*, vol. 8, no. 13, pp. 2329–2337, Sept. 2015.

[12] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, Jun. 2016.

[13] K. Zeng, D. Wu, A. J. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE INFOCOM,*, San Diego, CA, Mar. 2010, pp. 1–9.

[14] G. Revadigar, C. Javali, H. J. Asghar, K. B. Rasmussen, and S. Jha, "Mobility independent secret key generation for wearable health-care devices," in *Proc. BodyNets*, Sydney, Australia, Sept. 2015, pp. 1–7.

[15] M. G. Madiseh, S. W. Neville, and M. L. McGuire, "Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation," *IEEE Trans. Inform. Forensics Security*, vol. 7, no. 4, pp. 1278–1287, Aug. 2012.

[16] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "Smokegrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Inform. Forensics Security*, vol. 8, no. 11, pp. 1731–1745, Nov. 2013.

[17] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," *IEEE Trans. Inform. Forensics Security*, vol. 6, no. 3, pp. 650–660, Sept. 2011.

[18] C. Thai, J. Lee, and T. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1517–1530, Feb. 2016.

[19] V. Fusco and N. Buchanan, "Developments in retrodirective array technology," *IET Microw., Antennas Propag.*, vol. 7, no. 2, pp. 131–140, May 2013.

[20] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inform. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.

[21] V. Erceg, L. Schumacher, P. Kyristsi, A. Molish, and D. Baum, et al, "TGn channel models," IEEE TGn 802.11, Tech. Rep. 03/940r4, May 2004.

[22] L. Chen, Y. C. Guo, X. W. Shi, and T. L. Zhang, "Overview on the phase conjugation techniques of the retrodirective array," *Int. J. Antennas Propag.*, vol. 2010, 2010.

[23] V. Fusco, C. B. Soo, and N. Buchanan, "Analysis and characterization of pll-based retrodirective array," *IEEE Trans. Microw. Theory Tech.*, vol. 53, no. 2, pp. 730–738, Feb. 2005.

[24] N. Buchanan, V. Fusco, M. Van Der Vorst, N. Williams, and C. Winter, "New retrodirective antenna techniques for mobile terminal applications," in *Proc. 32nd Antenna Workshop, ESA/ESTEC*, Noordwijk, The Netherlands, Oct. 2010, pp. 5–8.

[25] N. Buchanan, V. Fusco, and M. Van Der Vorst, "Phase conjugating circuit with frequency offset beam pointing error correction facility for precision retrodirective antenna applications," in *Proc. 41st Eur. Microw. Conf. (EuMC)*, Manchester, UK, Oct. 2011, pp. 1281–1283.

[26] K. Chen and B. Natarajan, "MIMO-based secret key generation strategies: rate analysis," *Int. J. Mobile Comput. and Multimedia Commun.*, vol. 6, no. 3, pp. 22–55, 2014.

[27] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Physical Review E*, vol. 69, no. 6, p. 066138, 2004.

[28] Y. Ding and V. Fusco, "Improved physical layer secure wireless communications using a directional modulation enhanced retrodirective array," in *XXXIth URSI General Assembly and Scientific Symp. (URSI GASS)*, Beijing, China, Aug. 2014, pp. 1–4.