Social-Aware Secret Key Generation for Secure Device-to-Device Communication via Trusted and Non- Trusted Relays

Muhammad Waqas, Manzoor Ahmed, Yong Li, Senior Member, IEEE, Depeng Jin, Member, IEEE, Sheng Chen, Fellow, IEEE

Abstract—Physical layer security (PLS) is a promising technology in device-to-device (D2D) communications by exploiting reciprocity and randomness of wireless channels, which attracts considerable research attention in the D2D communications community. In this paper, we investigated PLS for secure key generation rate (SKGR) in D2D communications based on cooperative trusted and non-trusted relays. By leveraging social ties, we exploit three social phenomena for secure communications, i.e., trusted scenario (social trust), non-trusted scenario (social reciprocity) and partially trusted scenario (mixed social trust and social reciprocity). The coalition game theory is further utilized to select the optimal relay pairs for improving SKGR. On the basis of social ties, we develop an algorithm for SKGR that protects the keys secret from both eavesdropper and non-trusted selected relays. We incorporate secure relays selection and system wide security for D2D communications. The stability and convergence of the proposed algorithm are also proved in our work. Both numerically and analytically results verify effectiveness and consistency of our proposed scheme, which ensures better SKGR performance in D2D communications.

Index Terms—Device-to-device communication, physical layer security, key generation rate, social ties, social trust, social reciprocity.

I. INTRODUCTION

With the dramatic increase of smart mobile devices and the proliferation of wireless communication applications, mobile traffic has continuously increased at an exponential rate. According to Cisco, global mobile data traffic grew 63 percent in 2016 and reached to 7.2 exabytes per month at the end of 2016, up from 4.4 exabytes per month at the end of 2015 [1]. Cisco also forecasts that global mobile data traffic will increase sevenfold between 2016 and 2021, reaching 49 exabytes per month by 2021 [1]. To meet this ever-increasing demand, device-to-device (D2D) communication has been actively considered as a promising technical component for the next-generation cellular network [2]. It enables mobile devices in proximity to communicate directly at high data rate, low power consumption, and low latency, without involving the cellular infrastructure. Therefore, D2D communication is an enabling technology to assist overburdened cellular networks by improving spectrum efficiency, throughput, network coverage and delay [3]. Most of the studies have focused on various technical problems in D2D communication, including mode selection [4], resource allocation [5], [6] and interference management [7]. However, D2D security under the PLS technique in term of key generation, and by leveraging social ties that can unify security solutions is not yet matured [8].

Owing to the openness of wireless links, any receiver located within the communication range of the transmitter can receive the transmitted signal naturally. In addition, adversaries can initiate various passive and active attacks during the communication period [8]. Thus, security is a paramount concern in wireless communication [9]–[12]. Given the inherent vulnerability of wireless links, any D2D transmission can be easily obtained by unauthorized users deployed within its range. In this regard, classical encryption schemes based on secret key sharing are typically used for securing information between communicating nodes. However, this approach is less attractive for D2D communication because unlike the cellular tier that is supported by a strong centralized infrastructure, the D2D tier relies on a loosely distributed infrastructure, and a mobile device has limited computational capability. In addition, generating secret keys depends on every node possessing a public key certificate in classical encryption schemes. It is questionable that whether each mobile device in D2D communication can bear a public key certificate. Last not the least, in classical encryption schemes, the public key infrastructure also needs to be secured [13]. By contrast, a physical layer security (PLS) technique secures the communication between the two D2D devices by applying the physical characteristics of the wireless channel between the two D2D users. Since an eavesdropper does not have the knowledge of the channel variations between the two communicating D2D devices, it can be prevented from reading the transmitted messages between the D2D users. Consequently, by exploiting dynamic channel variations, PLS techniques [8] can overcome diverse security threats to data transmission and user privacy.

According to [14], authentication can also be achieved through secret keys by utilizing PLS techniques. The problem of impersonation attack for example can be tackled by adding the authentication signal to the message signal in such a way that the authentication signal appears as noise to the message signal based on PLS techniques. Unlike conventional cryptography which works by ensuring that all the involved entities load and execute the proper and authenticated cryptographic information, PLS takes the advantages of channel randomness nature of transmission media to achieve commu-
communication confidentiality and authentication [15]. The essence of PLS techniques is to recognize the identity information that relies on the uniqueness of the channel state information (CSI) of the transmit-receive channel medium linking the source and destination. The CSI is essentially invariant within the channel coherent time, which gives the transmitter and receiver the opportunities to emulate or acquire the correlation characteristics of their unique link [16].

Hence, information theoretic security (ITS) under the umbrella of PLS has emerged as an effective technique to achieve information confidentiality. ITS exploits randomness and reciprocity of wireless channels for secret key generation (SKG) [17]–[19]. In ITS, SKG is achieved directly from wireless channels, and therefore this approach is more promising for securing D2D communications. The randomness of a wireless channel is shared between two communicating devices according to the channel reciprocity, which is inaccessible to and thus indeterminable to the unauthorized users [20]. Hence, the randomness induced by unpredictable wireless channels can be used as the random source for generating secret keys. Mobile devices engaging in D2D communication can extract a secret key from the common channel randomness. The secret key can be generated on demand and modified continuously. However, the rate at which secret keys are generated from the wireless channel depends to a great extent on how fast the channel changes. In a static wireless environment, the channel remains the same and its randomness is very low. Thus, how to induce more channel randomness to enhance key generation rate becomes the principal problem. An effective solution for this problem is to explore some relay nodes in the vicinity of the target nodes. These relay nodes provide the additional randomness in the channel to ensure SKG between the target D2D nodes.

The exponential growth in global mobile data traffic to a large extent can be traced to the following phenomenon that people are increasingly involving in online social interactions. Various social networks, like Facebook, Twitter, WeChat and etc., have grown phenomenally. Cooperative D2D communication is a proficient technique in the social networking [21]. By leveraging the social features, social-aware D2D communication can significantly enhancing achievable performance [22]. In particular, social ties, which characterize the strengths of relationships among mobile users, define two basic social interacting environments, called social trust and social reciprocity [23]. Social trust is established among mobile users having strong social-ties such as kinship, colleagueship and friendship, etc. In a social-trust environment, mobile devices are likely to cooperate fully, and a user can ask other trustworthy users to serve as relays in order to improve its SKG rate (SKGR). In the absence of social trust, a group of individuals can exchange mutually beneficial activities. This is called social reciprocity, which is another widely observed social phenomenon. In a social-reciprocity environment, cooperation among users has to be based on mutual benefits, e.g., mobile devices can provide relay assistance to each other in order to improve their SKGRs. It can be seen that social ties play a vital role in representing social trust or non-trust D2D communication scenarios [24]. In the real world, a social community typically involves users with mixed social interactions, i.e., with strong and weak social ties, which represents a partially social trust environment. Therefore, we can enhance secure D2D communications by exploiting diverse properties of social ties.

A. Related Work

Recently, social-aware D2D communication approach has gained much attention [21], [22], [25]–[34]. Most of the researches focus on how to utilize the social features of D2D users to improve the overall D2D transmission rate and resource utilization. For example, Chen et al. [21] presented a relay selection scheme based on social trust and social reciprocity to improve the system throughput in D2D communication. Specifically, they proposed a coalition game theoretical approach to determine the effective D2D cooperation strategy and devised a network assisted relay selection technique. Li et al. [22] summarized the influence of social features on D2D communications, and quantitatively analyzed the achievable gains in a social-aware D2D communication system. The work [25] studied a reward-based Markov decision process to enable secondary users to cooperatively access the primary users’ spectrum resource in cognitive radio networks. The study [26] described an imitation-based spectrum access mechanism for implementing efficient spectrum access. Cao et al. [27] proposed a cooperative video multi-cast scheme, called SoCast, to stimulate cooperation among mobile users by leveraging their social ties. Zheng et al. [28] proposed a social-aware algorithm for efficient multi-file dissemination in multi-hop D2D communication networks. In particular, the authors discussed the utilization of social network properties to serve ad-hoc peer discovery. Sun et al. [29] used a Bayesian approach to model the social ties for D2D mobile users and to accomplish effective data transmission among D2D users.

Furthermore, the work [35] described a PLS based SKG scheme by exploiting the reciprocity of signal envelopes. Chen et al. [30] proposed an allocation mechanism to improve the SKGR for two-relays based cooperative MIMO architectures. Gopinath et al. [31] analyzed various pre-processing techniques for PLS based key generation. The results of [31] showed that utilizing reciprocal properties of physical channel enhances the probability of agreement between the generated keys while de-correlation can mitigate key redundancy. Sadeghi et al. [32] investigated the impact of in-band full-duplex wireless communications on SKG. The authors proposed a scheme to improve the SKGR over multi-path fading channels. However, these schemes do not explicitly exploit the social features for secure D2D communications. Thai et al. [33] presented a PLS based SKG scheme for multi-antenna authorized nodes with the help of non-trusted relays. Sun et al. [34] proposed a cooperative PLS based key generation method to establish the shared secret keys between D2D users. The D2D users choose some close neighbors as relays nodes to extract the secret key directly from the wireless channels among them. However, the authors did not consider trusted or non-trusted behaviors in selecting relays, and considered only the social reciprocity phenomenon [34].
It can be seen that most of the existing works did not consider how to utilize social properties to enhance secure D2D communications, and only a very few studies exploited the social reciprocity property for PLS based SKG. No work to date has explicitly considered all the three scenarios of social ties (social trust, social reciprocity and partial trust) for cooperative relaying based secure D2D communication.

B. Our Contributions

Against the above background, in this paper, we formulate the social-aware D2D secure communication system in both physical and social domains to improve the SKGR. The SKGR is utilized to secure the system from non-trusted relay and eavesdropper. Specifically, we explicitly employ social ties' properties to formulate our cooperative two-relay selection problem for all the three scenarios of social ties. Our main contributions are summarized as follows.

- We frame the cooperative relays based scheme that plays significant role in helping SKG for D2D network. On the basis of ITS, we show that the proposed scheme is optimal for D2D communications with two relays scheme.
- We leverage social ties to encourage efficient cooperation among devices for secure cooperative D2D communication. We depict all three social scenarios of social trust, social reciprocity and partially trusted. The trusted behavior among D2D nodes not only secures the communication from eavesdropper but also from non-trusted relay nodes. Hence, in this paper we consider trusted and non-trusted as well as partially trusted behaviors of relay nodes.
- We formulate the problem of relay pairs selection based on social ties as a coalition game theory. Moreover, we design an algorithm by utilizing the coalition game theory to select an optimal relay pairs based on social ties, and prove the stability and convergence of the algorithm.
- We evaluate the influence of different social environments on the optimal relay pairs selection. We show that the SKGR based on social ties achieves the optimal result by enhancing the average user key generation rate approximately from 10% to 70%, as compared to direct key generation rate. We also confirm that different social phenomena have different optimal average user key generation rates.

The rest of the paper is organized as follows. In Section II, after presenting the system overview and the model formulation, we formulate our relay nodes selection problem in both physical and social domains. Section III is devoted to the coalition game formulation to our relay pair selection problem, and presents the algorithm for finding the optimal solution. Stability and convergence properties of our coalition formation algorithm are analyzed in Section IV. Section V presents the performance evaluation of our proposed scheme. The paper is concluded in Section VI.
reliability, because of strong social ties. Social reciprocity based scenario characterizes as a social environment where none of
the available nodes are trusted by D2D pairs to be selected as
relay nodes based on social tier information along. A partially
trusted environment on the other hand comprises of social trust
and social non-trusted (i.e., social reciprocity) nodes.

B. System Model and Problem Formulation

As shown in Fig. 1 (a), we consider the D2D pair consisting
of \(d_i, i = 1, 2\), i.e., D2D nodes \(D_1\) and \(D_2\), and the relay pair
containing \(r_j, j = 1, 2\), i.e., relay nodes \(R_1\) and \(R_2\). The SKG
process between D2D pair and relay pair consists of three
steps, channel estimation, keys generation and key agreement.
In the channel estimation phase, \(d_i, i = 1, 2\), estimates the
channels with the help of the selected relay pair \(r_j, j = 1, 2\).
Specifically, in the first time slot, D2D node \(d_i\) transmits a
training signal \(s_{d_i}\) over the wireless channels, and the signals
received at D2D node \(d_i\) and relay nodes \(r_j, j = 1, 2\), are
given respectively as

\[
y_{d_i} = g_{d_i,r_j}s_{d_i} + n_{d_i}.
\]

\[
y_{r_j} = g_{d_i,r_j}s_{d_i} + n_{r_j},
\]

where \(g_{d_i,r_j}\) and \(g_{d_i,r_j}\) are the channel gains for the links
from \(d_i\) to \(r_j\) and the links from \(d_i\) to \(r_j\), respectively,
while \(n_{d_i}\) and \(n_{r_j}\) are the corresponding links' additive white
Gaussian noises (AWGNs), all having variance \(\sigma_n^2\). In the
second time slot, relay nodes \(r_j\) transmit the training signals
\(s_{r_j}\), and the signals received by \(d_i\) are given by

\[
y_{d_i} = g_{r_j,d_i}s_{r_j} + n_{d_i},
\]

where \(g_{r_j,d_i}\) are the channel gains for the links from \(r_j\) to
\(d_i\), and \(n_{d_i}\) are the links' AWGNs with variance \(\sigma_n^2\). Note that
for the notational simplification, we have omitted the time slot
index in (1) to (3). We further assume that the wireless net-
work adopts the time division duplexing (TDD) protocol, and
therefore, the channel reciprocal property holds. Consequently,
we have \(g_{d_i,r_j} = g_{d_i,r_j} = g_{d_i}\) and \(g_{d_i,r_j} = g_{r_j,d_i} = g_{r_j,j}\).
Both \(g_{d_i}\) and \(g_{r_j}\) follow the normal distributions
with zero mean and variances \(\sigma_d^2\) and \(\sigma_r^2\), respectively, that is,
\(g_{d_i} \sim \mathcal{N}(0, \sigma_d^2)\) and \(g_{r_j} \sim \mathcal{N}(0, \sigma_r^2)\).

In this physical layer based key generation process, an
eavesdropper is passive [31], [32], [35], [36], specifically, it is
not a legitimate participant of the channel estimation process.
True, an eavesdropper may be able to receive the transmitted
signals \(s_{d_i}\) and \(s_{r_j}\). However, if the eavesdropper is more
than one-half wavelength away from the targeted nodes that
are trying to establish a secret key, the channels between the
D2D nodes as well as the channels between the D2D nodes
and the relay nodes are uncorrelated with the channels between
the eavesdropper and these targeted nodes [34]. For example,
in the case of wireless transmissions in the 2.4 GHz band,
we only require the eavesdropper to be more than 6.25 cm
away from the target nodes for these different channels to
be uncorrelated. Thus, even if the eavesdropper were able
to estimate the channel gains between itself and the target nodes,
it could not predict the channel gains between the targeted
nodes. In other words, the channel responses between the
targeted devices are unavailable and also unpredictable to any
eavesdropper more than one-half wavelength away from the
targeted nodes. Moreover, the eavesdropper may not be able
to estimate the channels between itself and the legitimate nodes at
all, since it is not synchronized with the D2D and relay nodes,
and thus its received signals are noise like.

Based on their received training signals, the D2D and relay
nodes \(d_i\) and \(r_j\) can estimate the channel gains \(g_d\) and \(g_{r,j}\),
respectively. More specifically, at the first time slot, let the
training symbol transmitted by D2D node \(d_i\) be denoted as
\(X_{d_i}^*\). The estimated channel gain at D2D node \(d_i\), \(i \neq i\),
can be expressed as

\[
h_{1,d_i} = g_{d_i} + \frac{X_{d_i}^*}{\|X_{d_i}^*\|^2}n_{d_i} \sim \mathcal{N}\left(0, \sigma_d^2 + \frac{\sigma_n^2}{\|X_{d_i}^*\|^2}\right),
\]

where \(X_{d_i}^*\) is the conjugate of \(X_{d_i}\). Similarly, the estimated
channel gains at relay nodes \(r_j\) are given by

\[
h_{1,r_j} = g_{r_j} + \frac{X_{r_j}^*}{\|X_{r_j}^*\|^2}n_{r_j} \sim \mathcal{N}\left(0, \sigma_r^2 + \frac{\sigma_n^2}{\|X_{r_j}^*\|^2}\right).
\]

At the second time slot, let the training symbol transmitted by
relay node \(r_j\) be denoted as \(X_{r_j}\). The estimated channel gains

![Fig. 1. Key generation scenarios with and without relay node. (a) Social trust scenario, (b) Social reciprocity, and (c) Mixed Scenario.](image-url)
at D2D nodes $d_i$ can be expressed as

$$h_{2,r_j,d_i} = y_{j,i} + \frac{X_t}{\|X_r\|^2}n_{d_i} \sim \mathcal{N}\left(0, \sigma_r^2 + \frac{\sigma_n^2}{\|X_r\|^2}\right). \quad (6)$$

According to [37], the optimal key generation rate between D2D pair without the involvement of relay nodes is defined as the mutual information (MI) $I(h_{1,d_i}; h_{1,d_2})$ scaled by the channel coherence time $T_c$

$$\mathbb{R}^{\text{direct}}_{KG} = \frac{1}{T_c}I(h_{1,d_i}; h_{1,d_2}). \quad (7)$$

Let the transmitted signal power be denoted as $p$. Since the channel coherence time is $T_c$, the optimal training session for D2D node $D_i$ is $\frac{T_c}{2}$, where $i = 1, 2$. With this optimal training session length $\frac{T_c}{2}$, the training symbol energy is $\|X_d\|^2 = p\frac{T_c}{2}$. As detailed in Appendix A, $\mathbb{R}^{\text{direct}}_{KG}$ can be expressed as

$$\mathbb{R}^{\text{direct}}_{KG} = \frac{1}{T_c}\log_2 \left(1 + \frac{\sigma_r^4 p^2 T_c^2}{4(\sigma_n^4 + \sigma_r^2 \sigma_n^2 p T_c)} \right). \quad (8)$$

Observe from (8) that $\mathbb{R}^{\text{direct}}_{KG}$ is approximately proportional to $\frac{1}{T_c}$. Therefore, if the channel coherente time $T_c$ is large, i.e., the channel variations are low, the achievable SKGR is low. Observe also from (8) that the achievable SKGR increases with $\sigma_r^4 p^2 T_c^2$ and $\sigma_n^4 + \sigma_r^2 \sigma_n^2 p T_c$. Therefore, if the channel coherent time $T_c$ is large, i.e., the channel variations are low, the achievable SKGR is low. 

For given $i$, where $i = 1, 2$, the optimal training session for D2D node $D_i$ should last $\frac{T_c}{2}$, while the corresponding optimal training session for $R_j$, $j = 1, 2$, should also last $\frac{T_c}{2}$. Further assume that the powers of all the training signals are $p$. Therefore, similar to the derivation of (8), $\mathbb{R}^{\text{relay}}_{KG}$ can be expressed as

$$\mathbb{R}^{\text{relay}}_{KG} = \frac{1}{T_c} \log_2 \left(1 + \frac{\sigma_r^4 p^2 T_c^2}{8(\sigma_n^4 + \sigma_r^2 \sigma_n^2 p T_c)} \right) \times \prod_{i=1}^2 \prod_{j=1}^2 \left(1 + \frac{\sigma_r^4 p^2 T_c^2}{8(\sigma_n^4 + \sigma_r^2 \sigma_n^2 p T_c)} \right). \quad (10)$$

C. Key Agreement Based on Social Ties

After the generation of keys among D2D pair and relay pair, the nodes involved need to make a key agreement. As mentioned previously, we consider the key agreement between D2D pair and relay pair in the three different scenarios.

1) Key agreement based on social trust: In this environment, all the nodes involved socially trust each other. Hence, the D2D users will keep the keys secret only from eavesdropper. It is obvious that in this social trust environment, not only the selection of relay nodes for SKG becomes effective for securing the communication system but also there is less chance of collusion among the selected relay nodes with the eavesdropper and others. The key generation in the social trust phenomenon is illustrated in Fig. 1(a). Afterwards, D2D pair $D_1$ and $D_2$ agree on a key $K_1$ between their corresponding correlated observations. Similarly, $D_1$ and relay $R_1$ agree on a key $K_2$, while $D_2$ and $R_1$ agree on a key $K_3$. Likewise, $D_1$ and $R_2$ agree a key $K_4$, while $D_2$ and $R_2$ agreed on a key $K_5$, form their respective correlated observations as shown in Fig. 1. Then, relay pair $R_1$ and $R_2$ broadcast $K_2 \oplus K_3$ and $K_4 \oplus K_5$, respectively. Subsequently, D2D pair $D_1$ and $D_2$ have the following secret keys by concatenating $(K_1, K_2, K_3, K_4, K_5)$. However, these are not the final keys as $K_2$ & $K_3$ and $K_4$ & $K_5$ cannot simultaneously serve in the final set of keys. This is because the eavesdropper can learn $K_2$ & $K_3$ and $K_4$ & $K_5$ when they are broadcasted over the public channel. Therefore, D2D pair considers the following set of keys: either the set of $\{K_1, K_2, K_4\}$, if the size of $K_2$ and $K_4$ are smaller than the size of $K_3$ and $K_5$; otherwise the set of $\{K_1, K_3, K_5\}$ is adopted. With either set of the keys, $\lambda_1$ or $\lambda_2$, any eavesdropper can at best get insufficient information of these keys. This is because an eavesdropper experiences an independent wireless channel from that of the authorized D2D pair [37, 39]. Consequently, the key set is secure from any eavesdropper.

2) Key agreement based on social reciprocity: In this environment, D2D users do not trust the selected relay nodes socially. Hence, although the non-trusted relay nodes help the D2D pair to generate the more random keys, the D2D users are not sure these relay nodes will not collude with eavesdropper or others. Therefore, the D2D pair must keep the secret keys secure from both the eavesdropper and the selected relay nodes. In order to keep the keys secret even from both eavesdropper and the selected relay nodes, the D2D pair $D_1$ and $D_2$ implement the XOR operation on the following key sets, $(K_2, K_4)$ and $(K_3, K_5)$, and they agree on the secret key set, $\lambda_3 = (K_1, K_2 \oplus K_4)$ or $\lambda_4 = (K_1, K_3 \oplus K_5)$, by concatenating. It is readily seen that the key set agreed by the D2D pair, $\lambda_3$ or $\lambda_4$, satisfies the requirement of secrecy conditions given in [37, 39]. Consequently, each relay node and eavesdropper can only achieve insufficient information about the key set agreed by the D2D pair. In other words, this key set is secured from the both relay nodes$^1$. In fact, the proof is straightforward. Assume that $\lambda_3$ is agreed by the D2D pair. Note that relay $R_1$ has $K_2$ and it can also acquire $K_4 \oplus K_5$ when it was broadcasted. However, as proved in Appendix B,

$$I((K_2, K_4 \oplus K_5); K_2 \oplus K_4) = 0. \quad (11)$$

Therefore, relay $R_1$ is unable to generate $K_2 \oplus K_4$ from $K_2$ and $K_4 \oplus K_5$, that is, $(K_1, K_2 \oplus K_4)$ is secured from relay

$^1$The secure key set, $\lambda_3$ or $\lambda_4$, agreed by the D2D pair is referred to as the private key and is shown to be secure from the relay nodes in [39].
Therefore, the set of feasible relay pairs for D2D pair $d_{1, i_2}$ is specified by $R_p(d_{1, i_2}) = \{ \forall r_{j_1, j_2} \in V_p: \alpha^P_{d_{1, i_2}, r_{j_1, j_2}} = 1 \}$. Clearly, if $R_p(d_{1, i_2})$ is empty, the D2D pair $d_{1, i_2}$ have to generate keys directly without the assistance of any relay pair, and its achievable SKGR is given in (8). By contrast, if $R_p(d_{1, i_2})$ is not empty, $d_{1, i_2}$ will be able to select a relay pair from $R_p(d_{1, i_2})$ to assist the key generation, and its achievable SKGR in this case is given in (10). Thus, with the physical constraints, the achievable SKGR for D2D pair $d_{1, i_2}$ is summarized as follows:

$$R_{KG}(d_{1, i_2}) = \begin{cases} R_{KG}(d_{1, i_2}|\text{no relay}) = \mathcal{R}_{KG}^{\text{direct}} & (8), \\ R_p(d_{1, i_2}) = \emptyset & (10), \\ R_{KG}(d_{1, i_2}|r_{1, 2}) = \mathcal{R}_{KG}^{\text{relay}}, \quad r_{1, 2} \in R_p(d_{1, i_2}) & (12). \end{cases}$$

2) Social domain: We introduce the social link graph $G_s = (V_s, E_s)$ to model the social relationships among the D2D pairs and the potential relay node pairs. In this social graph, the vertex set $V_s$ contains all the D2D pairs and the potential relay node pairs, similar to $V_p$, while the edge set $E_s$ represents the social links or connections between the D2D pairs and the potential relay node pairs, according to a specific social relationship metric.

2.1) Social trust: In this scenario, the social trust is chosen to be the social relationship metric. The entries of $E_s$ are denoted by $\beta^{\text{d}_{1, i_2}}_{r_{1, 2}}, \forall d_{1, i_2}, r_{1, 2} \in V_s$, where $\beta^{\text{d}_{1, i_2}}_{r_{1, 2}} = 1$ indicates that there exist the social-trust connections between the two D2D nodes of $d_{1, i_2}$ and the two potential relay nodes of $r_{1, 2}$, while $\beta^{\text{d}_{1, i_2}}_{r_{1, 2}} = 0$ indicates that no such social-trust connection exists.

2.2) Social reciprocity: In this scenario, none of the potential relay pairs is socially trusted by the D2D pairs. Cooperation among users has to be based on mutual benefits, and hence the social reciprocity is chosen to be the social relationship metric. In this case, we denote the entries of $E_s$ by $\gamma^{\text{d}_{1, i_2}}_{r_{1, 2}}, \forall d_{1, i_2}, r_{1, 2} \in V_s$, where $\gamma^{\text{d}_{1, i_2}}_{r_{1, 2}} = 1$ indicates that there exist the social-reciprocity connections between the two D2D nodes of $d_{1, i_2}$ and the two potential relay nodes of $r_{1, 2}$, while $\gamma^{\text{d}_{1, i_2}}_{r_{1, 2}} = 0$ means that no such social-reciprocity connection exists.

2.3) Mixed social trust and social reciprocity: In this scenario, we denote the entries of $E_s$ by $\theta^{\text{d}_{1, i_2}}_{r_{1, 2}}, \forall d_{1, i_2}, r_{1, 2} \in V_s$, where $\theta^{\text{d}_{1, i_2}}_{r_{1, 2}} = 1$ indicates that one node of $r_{1, 2}$ has the social-trust connections with the two D2D nodes of $d_{1, i_2}$ as well as the other node of $r_{1, 2}$ has the social-reciprocity connections with the two D2D nodes of $d_{1, i_2}$, while $\theta^{\text{d}_{1, i_2}}_{r_{1, 2}} = 0$ means that no such social connection exists.

3) Relay pair selection: In relay pair selection, the physical constraints, namely, the physical graph, must be taken into consideration. Moreover, we can incorporate the social ‘constraints’, namely, the social graph, to achieve better relay pair selection. To this end, we can define the combined graph of $G_{p|s} = (V_{p|s}, E_{p|s}) = (V_p \cap V_s, E_p \cap E_s)$. The set of feasible relay pairs for D2D pair $d_{1, i_2} \in V_{p|s}$ can then be specified by (13) at the top of the next page.

The optimal social-aware relay pair selection for the D2D
pair \(d_{1,i_2}\) can be formulated as the following optimization problem

\[
R_{p\cap s}(d_{1,i_2}) = \left\{ \begin{array}{l}
\forall r_{j_1,j_2} \in V_{p\cap s}: \alpha_{d_{1,i_2},r_{j_1,j_2}} \cdot \beta_{d_{1,i_2},r_{j_1,j_2}} = 1, \quad \text{Trust,} \\
\forall r_{j_1,j_2} \in V_{p\cap s}: \alpha_{d_{1,i_2},r_{j_1,j_2}} \cdot \gamma_{d_{1,i_2},r_{j_1,j_2}} = 1, \quad \text{Reciprocity,} \\
\forall r_{j_1,j_2} \in V_{p\cap s}: \alpha_{d_{1,i_2},r_{j_1,j_2}} \cdot \theta_{d_{1,i_2},r_{j_1,j_2}} = 1, \quad \text{Mixed.}
\end{array} \right.
\] (13)

Direct solving this challenging optimization problem for all the D2D pairs is intractable. Not least, different D2D pairs may have conflict-of-interest of wanting the same relay pair in order to maximize their individual achievable SKGRs. In the next section, we develop a coalition game framework to address the selection of the optimal relay pairs for all the D2D pairs efficiently.

III. COALITION GAME FRAMEWORK

A. Introduction to Game Formulation

Coalition game [40] is utilized to find the social-aware optimal relay pairs for D2D secure communications. For notational convenience, we denote the set of D2D pairs by \(D = \{d_i, 1 \leq i \leq N_{pa}\}\) and the set of potential relay pairs by \(R = \{r_i, 1 \leq i \leq M_{pa}\}\). In this coalition game, the players are D2D pairs who seek coalition with relay pairs that can offer them higher SKGRs. Specifically, The formulation of coalition game is outlined by the quartet \(G = (D, R, X_N, \mathcal{V})\), in which

- Players: In our proposed game, the D2D pairs are the game players, who seek coalition with the potential relay pairs.
- Cooperation Strategy: \(X_N\) represents the space of feasible cooperation strategies among all players in the coalition with all potential relay pairs.
- Characteristic Function: In our proposed game, game players use the characteristic function \(\mathcal{V}\) to map every nonempty subset \(U \subseteq R\) onto a subset of feasible cooperation strategies \(\mathcal{V}(U) \subseteq X_N\).
- Coalition Partition: The players set a coalition partition \(U = \{U_1, U_2, \cdots, U_{N_{pa}}\}\), where \(\forall i, \mathcal{V}(U_i) \subseteq X_N\), while \(U_i \cap U_{i'} = \emptyset\), for \(i \neq i'\), and \(\bigcup_{i=1}^{N_{pa}} U_i = R\). This represents the best cooperation strategy among the players in coalition with \(R\).

The procedure in coalition partition formulation is to enable the players in the formation to seek coalition based on the well-defined preference order. Specifically, each player should be able to compare and order its potential coalitions based on which to choose its preferred coalition members. Hence, we need to define the conception of preference order [40].

**Definition 1:** For any D2D pair \(d_i \in D\), the preference order \(\succ_{d_i}\) is defined as the reflexive, complete and transitive binary relation over the set of whole possible relay pairs \(R_j \in R\) so that the D2D pair \(d_i\) can form the cooperative coalition \(U_i \subseteq R\), which satisfies

\[U_i \cap U_{i'} = \emptyset, \forall i \neq i', \quad \text{and} \quad \bigcup_{i=1}^{N_{pa}} U_i = R.\] (15)

In our coalition partition formation, D2D pair \(d_i\) prefers the relay pair \(\bar{r}_j\) over the relay pair \(\bar{r}_{j'}\) if and only if selecting \(\bar{r}_j\) can offer higher SKGR than \(\bar{r}_{j'}\). Therefore the preference order in our proposed game is defined by

\[\bar{r}_j \succ_{d_i} \bar{r}_{j'} \iff \mathcal{V}(\bar{r}_j) > \mathcal{V}(\bar{r}_{j'}).\] (16)

B. Coalition Formation Algorithm for Selecting Optimal Relay Pairs

We are now ready to present our proposed coalition formation algorithm for selecting optimal relay pairs, which is summarized in Algorithm 1. Specifically, at Stage 1 of Algorithm 1, every D2D pair \(d_i\) forms the initial coalition \(U_i\) with the relay pairs by randomly selecting those relay pairs who can offer it higher SKGRs than its direct secrete rate of no relay assistance. The crucial Stage 2 of Algorithm 1 is based on coalition formation game, where D2D pairs make new coalitions with the relay pairs to enhance their SKGRs based on the preference order defined in (16). More specifically, in every iteration, a randomly selected D2D pair \(d_i\) compares a randomly picked relay pair from its current coalition, \(\bar{r}_j \in U_i\), with a randomly selected relay pair from a different coalition, \(\bar{r}_{j'} \in U_{i'}\), \(i' \neq i\). If the preference order \(\bar{r}_j \succ_{d_i} \bar{r}_{j'}\) is not satisfied, the D2D pair \(d_i\) switches its coalition with \(\bar{r}_j\), i.e., deselects \(\bar{r}_j\) from \(U_i\), and forms a new coalition with \(\bar{r}_{j'}\), i.e., adds \(\bar{r}_{j'}\) in \(U_i\). This preference order based switching operation enables every D2D pair to find a preferred relay pair and to form a new preferable coalition. After repeating switching operations based on preference order, the coalition formation game will converge to a stable and optimal coalition partition, which allows all the D2D pairs collaboratively find their optimal relay pairs, namely, cooperatively solve the optimization problem (14).

It can be observed that the switch operation in this coalition game relies on ‘local’ D2D pairs instead of all the D2D pairs of the system. Hence, the complexity of Algorithm 1 is lower than a centralized solution. After finite number of switching operations, the system partition will converge to the final Nash-stable partition, which is analyzed in the next section.

IV. THEORETICAL ANALYSIS

We now analyze the stability and convergence rate of the proposed coalition formulation game, Algorithm 1, as well as the optimality of the solution obtained.
Algorithm 1. Coalition formation algorithm for selecting optimal relay pairs

1: **Initialization**
2: Construct the physical graph and social graph to compute all $\alpha_{d_i,r_j}^\beta$ and $\beta_{d_i,r_j}^\gamma$ and $\gamma_{d_i,r_j}^\delta$, $\forall i, j$;
3: Set the iteration index $t = 0$; Set $U_t = \emptyset$, $\forall i$;
4: **end initialization**

**Stage 1: Relay nodes selection**

5: if Flag $= 1$ ——— Social link
6: repeat
7: Set $t = t + 1$.
8: Randomly select D2D pair $d_i \in D$;
9: Randomly select $r_j \in R$;
10: **Check** for social trust, social reciprocity or mixed social trust and reciprocity;
11: Compute $\mathcal{R}_{KG}(d_i|r_j)$;
12: if $\mathcal{R}_{KG}(d_i|r_j) > \mathcal{R}_{KG}(d_i|\text{no relay})$ —— $U_t = U_t \cup \{r_j\}$;
13: Go to step 6;
14: else
15: go to step 9;
16: **end if**
17: until All D2D pairs select their relay nodes;
18: else Flag $= 0$, $\forall d_i$, compute $\mathcal{R}_{KG}(d_i|\text{no relay})$;
19: **end if**

**Stage 2: Optimal relay pairs selection**

20: repeat
21: Randomly select coalition $U_t$, i.e., $d_i$ and $r_j \in U_t$;
22: Randomly select another coalition $U_{t'}$, $t' \neq t$;
23: Check preference order of $d_i$ for $r_j \in U_t$ and $r_{j'} \in U_{t'}$ based on (16);
24: if (16) NOT satisfies
25: go to step 29;
26: else
27: go to step 22;
28: **end if**
29: D2D pair $d_i$ splits from its current coalition and forms a new coalition;
30: Update the current coalition;
31: until Convergence to the final Nash-stable partition.

**A. Stability and Convergence Rate**

First, we have the following well-known concept of Nash-stability.

**Definition 2:** A coalition formation $U = \{U_1, U_2, \cdots, U_N\}$ is Nash-stable if $\forall d_i \in D$ and $\bigcup_{i=1}^N U_i = R$, $\forall r_j \in U_i$ and $\forall r_{j'} \in U_i \setminus U_i$ hold.

According to Definition 2 and the concepts of hedonic games [41], it can be shown that the final coalition partition calculated by Algorithm 1 is Nash-stable.

**Theorem 1:** Starting from any random initial coalition partition $U(0)$, the proposed coalition formulation algorithm will converge to the Nash-stable coalition partition $U^{(ns)}$ in a final number of random switching operations with probability one.

**Proof:** In every switching process of Algorithm 1, the new partitions are formed according to the selected relay pairs. Since the relay pairs in the set $R$ are final, the number of partitions for the given set of D2D pairs $D$ is a Bell number [29]. Consequently, the random switching operations will end with probability one. Thus, the algorithm converges to or stops at a final coalition partition $U^{(ns)}$ after finite random switching operations with probability one.

Next we prove $U^{(ns)} = \{U_1^{(ns)}, U_2^{(ns)}, \cdots, U_N^{(ns)}\}$ is Nash-stable by contradiction. Assume that $U^{(ns)}$ is not Nash-stable. Then there exists a D2D pair $d_i \in D$, $r_j \succ d_i$ $r_{j'}$ does not hold for some $r_j \in U_i^{(ns)}$ and some $r_{j'} \in U_i^{(ns)} \setminus U_i^{(ns)}$. Thus D2D pair $d_i$ should and can switch coalition. This contradicts to the fact that no more switching of coalition can be found. This completes the proof. ■

**B. Optimality of Solution**

**Theorem 2:** The final coalition partition $U^{(ns)} = \{U_1^{(ns)}, U_2^{(ns)}, \cdots, U_N^{(ns)}\}$ obtained by Algorithm 1 according to coalition game $G$ for the social link based relay pair selection scheme represent the optimal relay pairs for the set of D2D pairs $D$.

**Proof:** For any $d_i \in D$, its coalition set of the selected relay pairs is $U_i^{(ns)}$. Since we have
\[
\mathcal{R}_{KG}(d_i|r_j) > \mathcal{R}_{KG}(d_i|r_{j'}), \quad \forall r_j \in U_i^{(ns)}, \forall r_{j'} \in U_i^{(ns)} \setminus U_i^{(ns)},
\]
(17)
the selected relay pairs in the coalition \( U^{(ns)}_i \) with \( \hat{d}_i \) are optimal for the D2D pair \( d_i \). Hence, through coalition game \( G \), all the D2D pairs have collaboratively found their optimal relay pairs, in terms of SKGRs.

V. PERFORMANCE EVALUATION

We evaluate the performance of the proposed cooperative D2D key generation method with the aid of the selected relay nodes in a simulation study. In particular, we evaluate the security enhancement gained by the social-ties based relay pair selection. In the simulation, we consider randomly scattered nodes in the square area of \( 1000 \times 1000 \text{m}^2 \). We set \( \sigma_d^2 = \sigma_r^2 = 1 \) and thus all the channel gains are generated according to the normal distribution of \( N(0, 1) \), and we further set \( \sigma_n^2 = 1 \) for all the AWGNs. The users’ transmission power during training is set to \( p = 23 \text{dBm} \), and the channel coherence time \( T_c \) spans the duration of 20 symbols. We construct the physical graph by setting \( \alpha_{di}^p, \alpha_{d, r}^p = 1 \), if and only if the distance between the D2D pair \( d_i \) and the relay pair \( r_j \) is not greater than a threshold of 500 m. The relatively large distance threshold is set due to the fact that the detection of neighboring relay pairs can be significantly enhanced with the assistance of the base station in D2D communications [42]. The minimum and maximum distances between the node pairs are taken to be 10 m and 500 m, respectively. For the social graph model, we consider Erdős-Rényi (ER) graph model [43]. In ER graph model, a social link exists between nodes with a probability of \( P_{sl} \). For a given value of the social link probability \( P_{sl} \), we average the results over 1000 random runs. As the benchmark, we also compute the direct SKGRs between D2D nodes without considering relay pair. Unless otherwise stated, we use \( P_{sl} = 0.5 \) in most of the simulation experiments. But we also vary the value of \( P_{sl} \) to evaluate the impact of the social link density of the social graph [43] to the achievable SKGR performance.

Fig. 3 depicts the number of social links formed in the social graph as the function of the number of nodes in the network or physical graph. We assume that half of the network nodes are D2D nodes and the other half are relay nodes. It can be seen clearly from Fig. 3 that the number of social links increases exponentially as the number of network nodes increases. Obviously, more users enable more social links to be constructed in the social graph based on the social ties relationship among these nodes. These increased social connections in turn can be utilized by D2D users to form coalition with relay nodes in order to improve their SKGRs. Therefore, Fig. 4 describes the average coalition size with respect to the number of nodes. Not surprisingly, we observe that as the number of nodes increases, the average coalition size increases. To recap, as the number of nodes increases, the number of social link increases. Consequently, the average coalition sizes increases. This means that D2D users have more opportunities to select and make coalition with their respective relay pairs to enhance their SKGRs.

Fig. 3. Number of social links increases with the number of nodes.

Fig. 4. Average coalition size by varying the number of nodes.

In Fig. 5, we compare the average user’s SKGRs for various schemes by considering the secrecy constraints for different number of relay nodes. The upper-bound average user SKGR in Fig. 5 is the maximally achievable average user SKGR under the idealized conditions of the maximum social link probability \( P_{sl} = 1 \) and the maximum system signal to noise ratio (SNR) with \( p \rightarrow \infty \). Observe from Fig. 5 that the average user key rates of the social ties based relay pair selection schemes increase with the number of network nodes. This is because more cooperation opportunities among the D2D users and relay pairs are available when the number of
network nodes increases. Furthermore, all the social ties based relay selection schemes outperform the direct SKG generating scheme without the assistance of relay pairs. Even the relay assisted scheme under the socially non-trusted environment achieves a significantly higher average user SKGR than the direct SKG generating scheme. Not surprisingly, the relay assisted SKG scheme under the social trust environment attains the best performance. Specifically, its average user SKGR is 10% higher than the relay assisted scheme under the mixed social trust and non-trust environment, 16% greater than the relay pair selected scheme under the social non-trust environment, and 70% greater than the direct SKG. Observe from Fig. 5 that the upper bound can only be approached from below under a near idealized socially trusted environment of sufficiently large number of nodes that trust each other and are willingly cooperate with each other.

![Average Users' SNR (dB)](image1)

**Fig. 6.** Comparison of average user’s SNRs with and without assistance of relay pairs.

Fig. 6 compares the average user’s SNR achieved with the assistance of relay pairs with that achieved without the assistance of relay pairs. Note that in the case of relay assistance, the social ties of the selected relay pairs with the D2D pairs do not influence the average user’s SNR. Therefore, in Fig. 6, we only have two curves, the one with assistance of relay pairs and the other without assistance of relay pairs. Observe from Fig. 6 that the average user SNR increases dramatically with the increase of network nodes in the both cases. This is because in a denser network, the average distance between communicating D2D users is shorter, which results in higher SNR. Moreover, the average user’s SNR with the assistance of relay pairs is 25% to 40% higher than that without the assistance of relay pairs. Evidently, in a denser network, not only the distance between communicating D2D users is shorter but also the distance between D2D users and their relays is shorter. Consequently, the SNR gain of the relay assistance case over the case of no relay assistance is higher for denser network.

Next, we simulate a network with 300 D2D nodes and 300 relay nodes, and investigate the impact of the social link probability $P_{sl}$ on the achievable average user’s SKGR. Fig. 7 shows the average user’s SKGRs as the functions of $P_{sl}$ for various schemes. Obviously, the social link probability $P_{sl}$ has no influence on the direct SKG scheme, while the upper-bound SKGR is obtained with $P_{sl} = 1$. Clearly, larger $P_{sl}$ results in more social connections in the social graph. This provides more and better opportunities for D2D users to collaborate with relay pairs, which in turn leads to better SKGR performance for all the three relay assisted scenarios, as can be seen clearly from Fig. 7. In particular, at $P_{sl} = 1$, the SKGR performance of the social trust, social reciprocity, and mixed social trust and social reciprocity based relay-pair selection schemes are 63%, 60% and 55% higher than the direct SKG scheme, respectively.

![Average Users' KGR (Bits per channel use)](image2)

**Fig. 7.** Impact of social link probability $P_{sl}$ on average user’s SKGR. The network has 300 D2D nodes and 300 relay nodes.

The physical constraints of the network or the connections of the physical graph clearly have significant impact on the achievable average user’s SKGR. Fig. 8 depicts the influence of the distance threshold on the average user’s SKGR, where the network has 200 D2D nodes and 200 relay nodes. For a large distance threshold, the physical graph contains connections with long distances. These long-distance connections have low SNR values and therefore, the average user SKGR calculated based on these low-SNR connections will also be low. This explains the phenomenon shown in Fig. 8, where we observe that the average user SKGRs decrease as the distance threshold increases for all the four schemes. In Fig. 8, the lower-bound SKGR is obtained at the minimum SNR corresponding to the largest distance threshold of 500 m and without the cooperation of relay pairs, i.e., $P_{sl} = 0$. Again and not surprisingly, the average SKGR performance of the three relay assisted scenarios are significantly higher than the
direct SKG scheme, and the social trusted scenario attains the best performance.

**Summary of the results:** Evidently, denser network not only provides more and better physical connections but also offers more and better social connections, both factors will contribute to higher SKGR performance. The results clearly show that the relay assisted SKGR performance under the socially trusted environment is better than those under the socially non-trusted environment and the partially trusted environment. More importantly, our study has convincingly revealed that under all the three social ties environments, the relay assisted SKGR performance is significantly higher than the direct SKGR obtained without the assistance of relays. This demonstrates the effectiveness of our proposed social-aware secret key generation approach for secure D2D communications via trusted and non-trusted relays.

VI. Conclusions

In this paper, we have investigated how to improve information confidentiality through social secret key generation for D2D communications by introducing relay pairs based on social ties relationship. We have presented physical-layer security issues on both physical and social domains in order to meet physical constraints for D2D cooperation and to exploit social relationship among devices for securing D2D communications. More specifically, by leveraging social ties, we have exploited three social phenomena, namely, social trust scenario, social reciprocity and mixed social trust and social reciprocity, for secure D2D communications with the assistance of relay pairs. Moreover, we have utilized coalition game theory and have proposed an algorithm to select the optimal relay pairs for improving SKGR, while protecting the keys secret from both eavesdropper and non-trusted selected relays. Our analytical and numerical results have demonstrated that the proposed SKG generating scheme with the assistance of the relay pairs selected based on social ties relationship achieves substantially higher SKGR than the direct SKG scheme without relay assistance. In our future work, we will combine authentication of higher layer and information confidentiality via PLS technique for securing data transmission to overcome the problem of impersonation attack.

APPENDIX

A. Proof of Equation (8)

**Proof:** Since \( h_{1,d_1} \sim N \left(0, \sigma_d^2 + \frac{2\pi \sigma_n^2}{pT_e} \right) \) for \( i = 1, 2 \), the entropies

\[
H \left( h_{1,d_1} \right) = \log_2 \left( 2\pi e \left( \sigma_d^2 + \frac{2\pi \sigma_n^2}{pT_e} \right) \right), \quad i = 1, 2.
\]

On the other hand, the correlation coefficient between \( h_{1,d_1} \) and \( h_{1,d_2} \) is given by

\[
E \left[ g_d + \frac{X_{d_1}}{\| X_{d_2} \|^2} n_{d_1} \right] \left( g_d + \frac{X_{d_2}}{\| X_{d_1} \|^2} n_{d_2} \right) = E \left[ g_d^2 \right] = \sigma_d^2.
\]

Therefore the covariance matrix of the joint Gaussian variables \([h_{1,d_1}, h_{1,d_2}]^T\) is

\[
\Sigma = \begin{bmatrix}
\sigma_d^2 & \frac{2\pi \sigma_n^2}{pT_e} \\
\frac{2\pi \sigma_n^2}{pT_e} & \sigma_d^2 + \frac{2\pi \sigma_n^2}{pT_e}
\end{bmatrix}, \quad (20)
\]

and the entropy

\[
H \left( h_{1,d_1}, h_{1,d_2} \right) = \log_2 \left( (2\pi e)^2 \det (\Sigma) \right)
= \log_2 \left( (2\pi e)^2 \frac{4(\sigma_d^4 + \sigma_n^2 \sigma_d^2 p T_e)}{p^2 T_e^2} \right). \quad (21)
\]

The MI can be computed by the entropy method [20], [44], [45] as

\[
I \left( h_{1,d_1}; h_{1,d_2} \right) = H \left( h_{1,d_1} \right) + H \left( h_{1,d_2} \right) - H \left( h_{1,d_1}, h_{1,d_2} \right). \quad (22)
\]

Substituting (18) and (21) into (22) leads to

\[
I \left( h_{1,d_1}; h_{1,d_2} \right) = \log_2 \left( 1 + \frac{\sigma_d^4 p^2 T_e^2}{4(\sigma_d^4 + \sigma_n^2 \sigma_d^2 p T_e)} \right). \quad (23)
\]

B. Proof of Equation (11)

**Proof:** Denote \( K_2 = X, K_4 \oplus K_5 = Y, \) and \( K_2 \oplus K_4 = Z \). Then we have

\[
I \left( (K_2, K_4 \oplus K_5); K_2 \oplus K_4 \right) = I \left( X, Y; Z \right) = I \left( X; Z \right) + I \left( X; Y | Z \right), \quad (24)
\]

where the last equality is according to the chain rule of MI [45]. Since \( X \) and \( Y \) are independent and, therefore, they are conditional independent given \( Z \). Thus we have \( I \left( X; Y | Z \right) = 0 \). Clearly, \( K_2 \) and \( K_4 \) are independent. Since \( X = K_2 \) is completely unpredictable from \( Z = K_2 \oplus K_4 \) and vice versa, we conclude that \( X \) and \( Z \) are independent [46]. Thus, \( I \left( X; Z \right) = 0 \). This completes the proof.

REFERENCES


Sheng Chen (M’90-SM’97-F’08) received his BEng degree from the East China Petroleum Institute, Dongying, China, in 1982, and his PhD degree from the City University, London, in 1986, both in control engineering. In 2005, he was awarded the higher doctoral degree, Doctor of Sciences (DSc), from the University of Southampton, Southampton, UK. From 1986 to 1999, He held research and academic appointments at the Universities of Sheffield, Edinburgh and Portsmouth, all in UK. Since 1999, he has been with the School of Electronics and Computer Science, the University of Southampton, UK, where he holds the post of Professor in Intelligent Systems and Signal Processing. Dr Chen’s research interests include adaptive signal processing, wireless communications, modelling and identification of nonlinear systems, neural network and machine learning, intelligent control system design, evolutionary computation methods and optimisation. He has published over 600 research papers. Dr. Chen is a Fellow of the United Kingdom Royal Academy of Engineering, a Fellow of IET, a Distinguished Adjunct Professor at King Abdulaziz University, Jeddah, Saudi Arabia, and an ISI highly cited researcher in engineering (March 2004).