RSS-AoA-Based Physical Layer Secret Key Generation for Mobile Wireless Nodes

Xiaohui Shang, Aijun Liu, HaoYin, Yida Wang and Yong Wang
The Army Engineering University of PLA, Nanjing 210014, China
E-mail: shangxiaohui1214@126.com

Abstract. For the future Internet of Things (IoT) with ubiquitous wireless connectivity, the physical layer secret key (PLSK) scheme has been recognized as an effective and lightweight way to achieve secure communications by exploiting the reciprocity of the wireless channel. Compared with channel state information (CSI)-based PLSK generation schemes, received signal strength (RSS)-based schemes are more advantageous in terms of the communication costs and mobility for the IoT applications. However, due to the vulnerability of predictable channel attacks, RSS-based schemes cannot always guarantee perfect security. In this paper, we combine angle of arrival (AoA) and received signal strength (RSS) to generate physical layer secret key (PLSK). In particular, we propose a novel measurement named effective key generation rate (EKGR) to comprehensively and directly evaluate a PLSK scheme. Meanwhile, we further simplify the conventional PLSK generation steps to meet the low-complexity demand of IoT devices. At last, numerical results demonstrate that comparing with RSS-based and AoA-based schemes, our proposed EKGR of the RSS-AoA-based scheme achieves 78\% or even 120\% performance improvement.

1. Introduction
Although large number of intelligent wireless devices in the IoT bring people great convenience, they also monitor people's daily lives. It may cause the leakage of privacy due to the inherent broadcast nature of wireless communications [1]. Traditionally, the transmitted information is secured by classic encryption schemes, which consist of symmetric encryption schemes and asymmetric encryption schemes [2], [3].

Unlike classic encryption schemes, the physical layer secret key (PLSK)-based security schemes had been regarded as an additional promising way. And due to the spatial decorrelation, the PLSK cannot be obtained by the other user at a third location, which is a few wavelengths away from legitimate nodes [4], [5]. Thus, PLSK-based security [6] is information-theoretically secure, lightweight and needs no aid from other users [7]-[9]. Specifically, the PLSK generation can be divided into four steps, i.e., channel probing, quantization, information reconciliation and privacy amplification [10].

Particularly, channel parameters are the most essential part of PLSK generation. Received signal strength (RSS) is the most common selection of channel parameters in the investigations of PLSK generation because it can be easily acquired from existing devices [11]-[14]. But RSS-based schemes are vulnerable to predictable channel attacks, and the corresponding key generation rate (KGR) is limited [15], [16]. Based on above, we propose a RSS-AoA-based PLSK generation scheme to adapt the low-cost and low-complexity characteristics of IoT devices.
2. System Model
We concatenate the RSS-based PLSK and AoA-based PLSK into a combined PLSK, i.e. RSS-AoA-based PLSK. We consider the case that a base station (Alice) and a mobile station (Bob) exchange information over wireless channel in TDD system with the presence of a passive and fixed eavesdropper (Eve). Meanwhile, $t_s$ denotes the switching time of up-downlink channels and $T$ denotes the PLSK generation cycle. Alice is fixed and its coverage radius is $D$.

At first, Bob sends the pilot signal from uplink channel to Alice in the original position of Bob(Original), which is distributed uniformly in the coverage of Alice. Then, during $t_s$, Bob moves with the speed of $v$ along a random direction from Bob(Original) to a new position, i.e. Bob(Moved). And Bob receives the pilot signal sent by Alice from downlink channel at Bob(Moved). At the same time, Eve receives the pilot signal sent by Alice in its fixed position, which is also distributed uniformly in the coverage of Alice. As such, when Bob(Original) is described by the polar coordinate, it can be expressed as $(l, \alpha)$, where $f(l) = 2l / D^2, l \in [0, D]$ and $f(\alpha) = \alpha / 2\pi, \alpha \in [0, 2\pi]$.

Meanwhile, the movement distance of Bob during $t_s$ can be denoted as $d_s = vt_s$. Specifically, Alice and Bob with Eve quantize the AoA measurements into $m$ AoA-based bits and $n$ RSS-based bits to store, which corresponds to $2^m$ equal-area sector quantization regions and $2^n$ equal-area ring quantization regions, respectively. And the outside radius of every RSS quantization region from inside to outside can be expressed as $r_i = \sqrt{i / 2^n} D, i \in 1, 2, \cdots, 2^n$. Thus, there are $2^{m+n}$ equal-area quantization regions as shown in Figure 1.

To acquire a reliable and identical RSS-AoA-based PLSK in Alice and Bob, not only the AoA quantization value but also the RSS quantization value is supposed to be the same, i.e., the position of Bob(Original) and Bob(Moved) should be located in the same quantization region as the green region in Figure 1. On the opposite, Bob should not be located in the same quantization region with the one of Eve as the red region in Figure 1, to ensure the security. In summary, the area of RSS-AoA-based quantization region should be set properly.

3. PLSK Performance Analysis

3.1. Consistency Probability
Let $P_c$ denotes the CP of RSS-AoA-based PLSK, which indicates the probability of the PLSK generated in Alice and Bob being identical. And in above models, the CP can be translated into the probability of Bob(Original) and Bob(Moved) being located in the same quantization region. Due to
the fact that RSS-AoA-based PLSK is the concatenation of RSS-based PLSK and AoA-based PLSK, we need to analyze the CP of AoA-based PLSK and RSS-based PLSK as follows:

3.1.1. AoA-based PLSK. To evaluate the performance of reliability of AoA-based PLSK, we denote $P_{e_1}$ as the inconsistency probability of AoA-based PLSK during $T$. And $P_{e_1}$ can be written as:

$$P_{e_1} = \sum_{k=1}^{2^m} p_k P_e^{(k)} = \frac{1}{2^m} \sum_{k=1}^{2^m} P_e^{(k)} = P^{(1)}_{e_1},$$

where $p_k$ is the probability of Bob(Original) being located in $k$ th AoA quantization region, $P_e^{(k)}$ is the probability of Bob(Original) being located in $k$ th AoA quantization region and Bob(Moved) being located in different AoA quantization regions. Due to the symmetry, $P_1 = P_2 = \cdots = P_{2^n} = 1/2^m$ and $P^{(1)}_{e_1} = P^{(2)}_{e_1} = \cdots = P^{(2^n)}_{e_1}$. Thus, for the derivation of $P_{e_1}$, it is necessary to derive $P^{(1)}_{e_1}$, i.e. $P_{e_1}$ in $\alpha \in \{0, 2\pi / 2^m\}$.

At first, consider $P_{e_1}$ under the condition that the position of Bob is fixed and $\alpha \in \{0, 2\pi / 2^m\}$, which is denoted as $P^{(e)}_{e_1}$. In this occasion, when $d_s$ is smaller, Bob cannot move away from the original AoA quantization region and the AoA-based PLSK generated in Alice and Bob are identical. However, with the increase of $d_s$, Bob is more likely to move to different AoA quantization regions and $P^{(e)}_{e_1}$ approaches to $1/2 - 1/2^m$. Therefore, $P^{(e)}_{e_1}$ can be expressed as follows:

$$P^{(e)}_{e_1} = \begin{cases} 
0, & \text{if } 0 < d_s \leq c_1 l \\
A_1 = \frac{1}{\pi} \cos^{-1} \left( \frac{c_1 l}{d_s} \right), & \text{if } c_1 l < d_s \leq c_2 l \\
A_2 = \frac{1}{\pi} \left[ \cos^{-1} \left( \frac{c_1 l}{d_s} \right) + \cos^{-1} \left( \frac{c_2 l}{d_s} \right) \right], & \text{if } c_2 l < d_s \leq l \\
A_3 = \left( \frac{1}{2} - \frac{1}{2^m} \right) + \frac{1}{2\pi} \left[ \cos^{-1} \left( \frac{c_1 l}{d_s} \right) + \cos^{-1} \left( \frac{c_2 l}{d_s} \right) \right], & \text{if } l < d_s 
\end{cases}$$

Where $c_1 = \sin \alpha$ and $c_2 = \sin \left( 2\pi / 2^m - \alpha \right)$.

Then, consider $P_{e_1}$ under the condition that $\alpha$ is fixed within $\{0, \pi / 2^m\}$, while $f(l) = 2l / D^2, l \in (0, D)$. According to the relation of $l$, $d_s$, $m$ and $D$, $P^{(0)}_{e_1}$ can be derived from $P^{(e)}_{e_1}$ as follows:
where $c_1 = \sin \alpha$, $c_2 = \sin \left(2\pi / 2^m - \alpha\right)$.

Finally, we can derive $P^{(1)}_{e1}$. It means $P_{e1}$ under the condition that $f(l) = 2l / D^2, l \in (0, D)$ and $f(\alpha) = 2^m / \pi, \alpha \in (0, \pi / 2^m)$. Similarly, with the growth of $d_s$, the probability of Bob moving to other AoA quantization regions increases and approaches to $1/2 - 1/2^m$. At the same time, greater $m$ leads to greater $P^{(1)}_{e1}$. Thus, $P^{(1)}_{e1}$ can be derived from $P^{(0)}_{e1}$ as follows:

$$P^{(1)}_{e1} = \begin{cases} 
\int_0^{a_1} B_2 f(\alpha) d\alpha + \frac{2\pi}{a_1} B_1 f(\alpha) d\alpha, & \text{if } 0 < d_s \leq c_3 D \\
\int_0^{a_2} B_2 f(\alpha) d\alpha + \frac{2\pi}{a_2} B_1 f(\alpha) d\alpha, & \text{if } c_3 D < d_s \leq c_4 D \\
\int_0^{a_3} B_3 f(\alpha) d\alpha, & \text{if } c_4 D < d_s \leq D \\
\int_0^{a_4} B_4 f(\alpha) d\alpha, & \text{if } D < d_s
\end{cases},$$

where $a_1 = \sin^{-1}(d_s / D), a_2 = 2\pi / 2^m - \sin^{-1}(d_s / D), c_3 = \sin(\pi / 2^m), c_4 = \sin(2\pi / 2^m)$.

3.1.2. RSS-based PLSK. Similarly, denote $P_{e2}$ as the inconsistency probability of RSS-based PLSK during $T$. Combined with $n$ and $N$, $P_{e2}$ can be derived as:

$$P_{e2} = (1 - P_{e2})^n.$$

Then, due to the uniform distribution of Bob(Original) and the different occasions of RSS quantization regions, $P_{e2}$ can be written as:
\[ P_{e2} = \frac{1}{2^n}(P_{e2}^{(1)} + \sum_{i=2}^{n-2} P_{e2}^{(2)} + P_{e2}^{(3)}) , \tag{6} \]

where \( P_{e2}^{(1)} , P_{e2}^{(2)} , P_{e2}^{(3)} \) are three different occasions of RSS quantization regions.

When Bob is located in the innermost circular RSS quantization region, corresponding to the RSS quantization region with radium less than \( r_1 \), greater \( d_s \) will lead to greater inconsistency probability,

\[
P_{e2}^{(1)} = \begin{cases} 
  \int_{r_1-d_s}^{r_1} (1-C_1)f(l)dl, & \text{if } 0 < d_s \leq r_1 \\
  \int_{r_1-d_s}^{r_1} (1-C_1)f(l)dl + \int_{0}^{d_1-r_1} f(l)dl, & \text{if } r_1 < d_s \leq 2r_1 \\
  \int_{r_1}^{d_1-r_1} f(l)dl, & \text{if } 2r_1 < d_s \leq \end{cases} 
\tag{7} \]

where \( C_1 = (1/\pi)\cos^{-1}\left[\left(l^2 + d_s^2 - r_1^2\right)/(2ld_s)\right] \).

By comparison, when Bob is located in the middle annular quantization region of RSS, corresponding to the RSS quantization region with radium between \( r_{i-1} \) and \( r_i \), \( i \in 2, \cdots, 2^n - 2 \), inward movement direction at certain \( d_s \) will lead to additional inconsistency probability, which can be expressed as follows:

\[
P_{e2}^{(2)} = \begin{cases} 
  \int_{r_{i-1}+d_i}^{r_{i-1}} C_{i-1}f(l)dl + \int_{r_{i-1}+d_i}^{r_i} (1-C_1)f(l)dl, & \text{if } d_1 < d_s \leq d_2 \\
  \int_{r_{i-1}+d_i}^{r_{i-1}} C_{i-1}f(l)dl + \int_{d_2-r_{i-1}}^{d_4-r_{i-1}} C_{i-1}f(l)dl, & \text{if } d_2 < d_s \leq d_4 \\
  \int_{r_{i-1}+d_i}^{r_{i-1}} C_{i-1}f(l)dl + \int_{d_4-r_{i-1}}^{d_5-r_{i-1}} C_{i-1}f(l)dl, & \text{if } d_4 < d_s \leq d_5 \\
  \int_{r_{i-1}+d_i}^{r_{i-1}} C_{i-1}f(l)dl, & \text{if } d_5 < d_s \leq d_3 \text{ or } d_3 \leq d_s \leq \end{cases} 
\tag{8} \]

where \( d_1 = (r_i-r_{i-1})/2 \) , \( d_2 = r_i - r_{i-1} \) , \( d_3 = 2r_{i-1} \) , \( d_4 = r_{i-1} + r_i \) , \( d_5 = 2r_i \) , \( C_i = (1/\pi)\cos^{-1}\left[\left(l^2 + d_s^2 - r_i^2\right)/(2ld_s)\right] \), \( i = 2, 3, \cdots, 2^n - 2 \).

In addition, when Bob is located in the outermost quantization region of RSS, corresponding to the RSS quantization region with radium greater than \( r_{2^n-1} \), only inward movement direction may lead to inconsistency, which can be expressed as follows:
3.1.3. RSS-AoA-based PLSK. Due to the fact that RSS-AoA-based PLSK is the concatenation of RSS-based PLSK and AoA-based PLSK, it is necessary to consider the CP of AoA-based and RSS-based PLSK for the derivation of CP of RSS-AoA-based PLSK. In essence, when there is any inconsistency in the AoA-based PLSK or RSS-based PLSK, the RSS-AoA-based PLSK will be inconsistent. Thus, combined with \( m, n \) and \( N, P_c \) can be derived as:

\[
P_c = \left[1 - \left(P_{e1} + P_{e2} - P_{e1}P_{e2}\right)\right]^{N_{m+n}},
\]

(10)

Evidently, \( P_c \) is relative directly with the PLSK generation cycle and the total length of PLSK.

3.2. Security Probability

Let \( P_s \) denotes the SP of RSS-AoA-based PLSK. The SP indicates the probability of the PLSK generated in Bob and Eve being different, which implies the security of the PLSK. If the quantization value in Bob(Moved) and Eve are the same, it will be supposed to be unsecure. In essence, SP can be reflected as the position relation of Eve and Bob(Moved), i.e. the probability of Eve and Bob(Moved) being located in different quantization regions as shown in Figure 1.

In each \( T \), Eve is distributed randomly and uniformly in the coverage area of Alice as Bob. Moreover, the area of Alice in RSS-AoA model is divided into \( 2^{m+n} \) equal-area quantization regions. Thus, SP of RSS-AoA-based PLSK can be expressed as follows:

\[
P_s = \left(1 - \frac{1}{2^{m+n}}\right)^{N_{m+n}},
\]

(11)

3.3. Key Generation Rate

Let \( R_g \) denote the KGR of RSS-AoA-based scheme. The KGR is the bit number of PLSK generated in unit time, which indicates the effectiveness of PLSK. Meanwhile, to ensure the randomness of PLSK, the generation cycle in KGR needs to be less than the channel correlation time. Thus, \( R_g \) can be expressed as:

\[
R_g = \frac{N}{T} \leq \frac{N}{m+n}, \quad \text{if } r_{x-1} \leq D \leq 2r_{x-1}
\]

(12)
where $T_c$ is the channel correlation time, which can be expressed as $\frac{9c}{16\pi f}$, $c$ is light velocity, $f$ is the communication frequency.

3.4. Effective Key Generation Rate

For evaluating a PLSK scheme more comprehensively and directly, we propose a new measurement named EKGR. Specifically, EKGR is defined as the generation rate that PLSK can be generated consistently in Alice and Bob, but cannot be acquired by Eve. We use $R_E$ to denote the EKGR, which can be expressed as:

$$R_E = P_c \cdot P_g R_g .$$

According to the above analysis, EKGR reconciles the contradiction of security, consistency and effectiveness due to the comprehensive consideration.

4. PLSK Generation Scheme

In this section, we will describe the novel RSS-AoA-based PLSK generation scheme for the mobile IoT. According to the analysis above, the generated RSS-AoA-based PLSK can acquire satisfactory performance of security, consistency and effectiveness in mobile environments.

Moreover, in order to adapt to the low-cost and low-complexity characteristics of IoT devices, our scheme introduces the discard pattern, compared with the conventional PLSK generation method. Meanwhile, as for the low-rate wireless communications in IoT scenarios, the discard pattern can also decrease the leakage probability of RSS-AoA-based PLSK without long time-delay. Specifically, in conventional PLSK generation, when the quantization bits generated in Alice and Bob are different, the bits will be processed by information reconciliation. However, information reconciliation is in need of high overhead, which is not suitable for IoT devices. In addition, during the information reconciliation, the leakage information may be exploited by Eve to crack the PLSK. Therefore, when the generated quantization bits during a generation cycle is inconsistent, the bits will be discarded and be regenerated in the next generation cycle.

And as a supplement, when Bob possesses the detection ability, Bob can further ensure the communications security in essence. Specifically, after the channel probing, Bob can determine its corresponding quantization region. At this time, when Bob detects any threat of Eve in its quantization region, Bob will not use the generated bits during the generation cycle and send a signal to inform Alice that the generated bits need to be discarded.

5. Numerical Results

In this section, we conduct some simulation results based on Monte Carlo method to demonstrate our proposed RSS-AoA-based PLSK generation scheme. Unless stated otherwise, we consider the coverage radius of Alice $D=50$, switching time of uplink-downlink channel $t_s=50ms$, require length of PLSK $N=128bits$, light velocity $c=3\times10^8 m/s$, communication frequency $f=900MHz$, generation cycle $T=\max\{t_s, 9c/16\pi f\}$. Specifically, in a simulation, a point is generated randomly in the coverage area of Alice and then moves along a random angle within $t_s$ to a new position in a certain movement speed of $v$, which represents the movement of Bob. At the same time, a point is generated randomly in the coverage area of Alice to represent the position of Eve. Every simulation is repeated 100000 times.
To validate the analysis of CP, we compare the theory values and simulation of CP against movement speed as shown in Figure 2. One can observe that the analytical and simulation results are in perfect match. Evidently, with the increase of $v$, $P_c$ decreases. And with the increase of $m$ and $n$, $P_c$ also shows a downward trend. Moreover, $P_c$ of RSS-AoA-based PLSK with proper constitution of $m$ and $n$ is higher than the one of RSS-based or AoA-based PLSK.

Figure 3. The relation of SP, CP and KGR at different quantization levels and movement speed.

Moreover, to illustrate the performance of KGR, we show the relation of KGR and RSS quantization level at different movement speeds in Figure 3. It is evident that $R_y$ increases with the ascend of $m$ or $n$, due to more bits being generated at the same time. Meanwhile, $R_y$ also increases with $v$ because of the fact that the mobility enriches the randomness of channel. Compared with CP and SP, with the increase of $m$ and $n$, $R_y$ and $P_s$ increases while $P_c$ declines, which implies the contradiction of the CP, SP and KGR.
To reconcile the contradiction of SP, CP and KGR, EKGR is proposed. And to imply the performance of EKGR, the optimal EKGR and corresponding quantization level at different movement speeds are shown in Figure 4. Meanwhile, the relation of EKGR and the quantization level at $v = 1.1 \text{ (m/s)}$ is shown in Figure 5. Firstly, it can be observed that it is feasible to find a peak value of EKGR at a certain $v$. Then, with the increase of $v$, optimal $R_E$ first ascends and then descends. Furthermore, optimal $R_E$ of RSS-AoA-based scheme is more advantageous than the one of RSS-based or AoA-based scheme at the same $v$. Concretely, compared with AoA-based scheme, the optimal $R_E$ of RSS-AoA-based PLSK increases by 78% to 120%. And compared with RSS-based scheme, the corresponding $R_E$ has a 196% or even 863% performance improvement. At the same time, the corresponding $m$ and $n$ decrease steadily with $v$.

6. Conclusion
For the future IoT with large-scale devices, it is necessary to find a lightweight and reliable solution to achieve secure communications in mobile IoT scenarios. Thus, we propose a novel RSS-AoA-based PLSK generation scheme for the mobile IoT. Particularly, in order to evaluate a PLSK scheme more comprehensively and directly, we define a new measurement named EKGR. Meanwhile, we introduce the discard pattern into the conventional PLSK generation method to adapt to the characteristics of IoT. It is worth noting that our proposed EKGR of the RSS-AoA-based scheme achieves 78% or even 120% performance improvement, compared with RSS-based and AoA-based schemes. The results are of great reference value to the future research for secure communications in the IoT.
References

[1] A. Mukherjee, “Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints,” Proc. IEEE, vol. 103, no. 10, pp. 1747-1761, Oct. 2015.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, 6th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2013.

[4] R. Ahlswede and I. Csiszar, “Common Randomness in Information Theory and Cryptography. I.Secret Sharing,” IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121-1132, Jul. 1993.

[5] U. M. Maurer, “Secret Key Agreement by Public Discussion from Common Information,” IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733-742, May 1993.

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey,” IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1550-1573, Aug. 2014.

[7] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, “Physical Layer Security in Wireless Networks: A Tutorial,” IEEE Wireless Commun., vol. 18, no. 2, pp. 66-74, Apr. 2011.

[8] S. Mathur et al., “Exploiting the Physical Layer for Enhanced Security [Security and Privacy in Emerging Wireless Networks],” IEEE Wireless Commun., vol. 17, no. 5, pp. 63-70, Oct. 2010.

[9] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[10] K. Zeng, “Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities,”IEEE Commun. Mag., vol. 53, no. 6, pp. 33-39, Jun. 2015.

[11] J. Zhang, T. Q. Duong, A. Marshall and R. Woods, “Key Generation From Wireless Channels: A Review,” IEEE Access, vol. 4, pp. 614-626, 2016.

[12] Y. Liu, S. C. Draper, and A. M. Sayeed, “Exploiting Channel Diversity in Secret Key Generation from Multipath Fading Randomness,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, pp. 1484-1497, Oct. 2012.

[13] H. Liu, Y. Wang, J. Yang, and Y. Chen, “Fast and Practical Secret Key Extraction by Exploiting Channel Response,” in Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM), Turin, Italy, Apr. 2013, pp. 3048-3056.

[14] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radiotelepathy: Extracting a Secret Key from An Unauthenticated Wireless Channel,” Proc. 14th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom), San Francisco, CA, USA, Sep. 2008, pp. 128-139.

[15] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, “On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments,” in Proc. 15th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom), Beijing, China, Sep. 2009, pp. 321-332.

[16] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, “ProxiMate: Proximity-based Secure Pairing Using Ambient Wireless Signals,” in Proc. 9th Int. Conf. Mobile Syst., Appl., Services (MobiSys), Washington, DC, USA, Jul. 2011, pp. 211-224.