Communications Software Technical Committee – CommSoft

IEEE COMMUNICATIONS SOCIETY

IEEE

Communications Software Technical Committee - CommSoft

http://committees.comsoc.org/commsoft/policies.html

IEEE CommSoft E-Letters

Vol. 2, No. 1, May2013

CONTENTS

MESSAGE FROM COMMSOFT TC CHAIR

The Technical Committee on Communications Software (TC-COMMSOFT) examines methods and techniques devoted to advancement of the formal methods and tools, use of system analysis and design, methodology for development of communications protocols as well as application of general Software Engineering approaches for the purpose of development of communications applications. The issues addressed by the TC-COMMSOFT include domain-specific languages and practices of using them. Developing of "middleware" between networks and applications and the usefulness and usability of it is also a topic.

MOONet: A Metropolis-Oriented Opportunistic Networking System based on Bus

Jianwei Niu, Bin Dai, Chao Tong
School of Computer Science and Engineering, Beihang University, China
niujianwei@buaa.edu.com, daibin_buaa@hotmail.com

Opportunistic networks are a subclass of Delay Tolerant Networks (DTN) [1] where, most of the time, there does not exist an end-to-end path from the source to the destination. In Opportunistic networks, data transmission adopts the "store-carry-forward" mode. There are already many laboratory-level applications of opportunity networks, such as ZebraNet [2], CarTel [3], and PSN (pocket switched network). With the proliferation and increasing capabilities of hand-held and vehicle-mounted devices, pundits have predicted that a number of mobile applications will eventually be fielded, ranging from mobile advertisement, traffic information collection and disaster relief to military operations.

With the increase of the number of vehiches with short distance wireless interfaces, vehicle-based opportunistic networks (Fig.1) come into being gradually. It has great application potential in traffic safety, such as traffic accident warning, road condition detection and traffic jam forecast. Based on vehicle-mounted sensors, MIT developed a system called CarTel [3] for information collection and distribution.

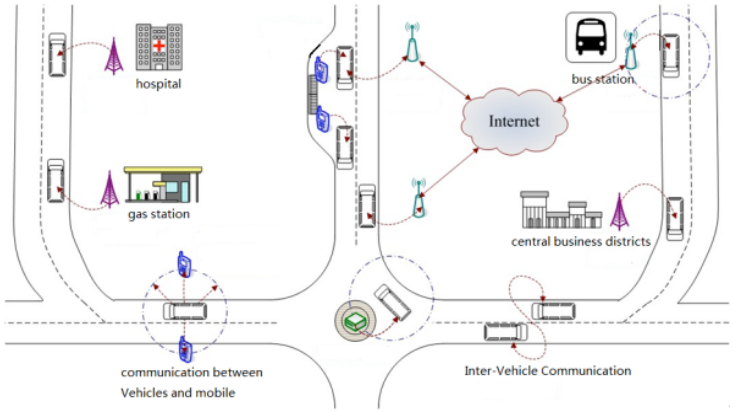


Figure 1 : Opportunistic networking based on buses.

Our system aims at transmitting data and acquiring information through opportunistic networks consisting of mobile devices, building a Metropolis Oriented Opportunistic Network System (MOONet). The system is a three-layer architecture consisting of sensor nodes on the first layer, bus mounted nodes on the middle layer and gateway nodes connected to Internet on the top layer. With regard to the hardware of the system, there are data collecting nodes developed by ourself, information publishing nodes, BIT (Bus-based Information Transceiver) nodes, gateway nodes, and data server. To tackle the problem of the short encountering time between vehicles, we analyzed and optimized the process of AP (Access Point) scanning, connection establishment and handoff mechanisms of WiFi interface, shortened the time of establishing WiFi connections between vehicles. Meanwhile, we proposed a rate adaptive algorithm based on prediction of vehicle movement, which can significantly improve the data transmission in MOONet.

MOONet is composed of three layers: the first layer, as the information source or utilizer, includes cell-phones, PDAs, information publishing devices and information collecting devices, such as environment monitoring sensors; the middle layer is equipped with BIT. Installed with Global Position System (GPS) modules, BIT devices move with buses in pre-designed lines; the top layer consists of gateways (APs), which are deployed at some fixed locations in cities. The gateway is connected to Internet by wired connection. These three layers build an ad-hoc, ubiquitous and heterogeneous opportunistic network, where the middle layer is the backbone network. Fig. 2 presents the three-layer structure.

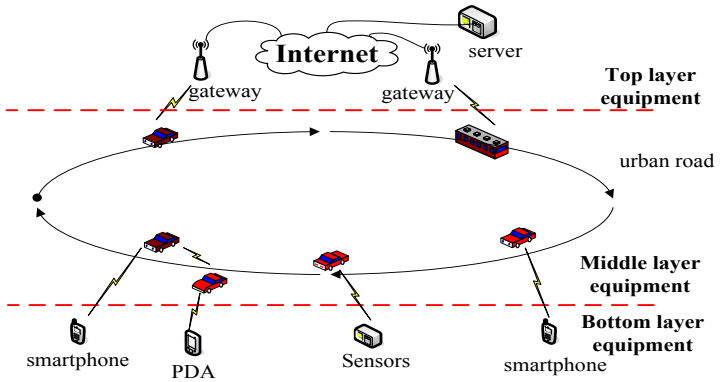


Figure 2 : Three-layer structure of MOONet.

We implemented the MOONet prototype system and deployed it on campus. We emulated the movement of buses by making a bus running in "stop-move" mode around our campus. We installed BIT nodes on the bus, and deployed gateway nodes in teaching buildings and libraries beside the roads which have Internet access. At the same time, we deployed information publishing nodes in dining halls, supermarkets and hospital, and deployed some sensors at the sports ground. The data servers have Internet access, are used to emulate the hosts that store collected data and send announcement messages over the Internet. Fig. 3 shows the main devices consists of MOONet.

Figure 1 : Devices of MOONet.

The optimization of the AP scan and connection process includes two parts: optimizing scanning parameters and simplifying scanning process.

Scanning parameter optimization. There are 11 channels for the WiFi system and at least 1,100 milliseconds are needed to scan all the channels in the passive mode. Survey [4] showed that 83% of users only open Channel 1, 6 and 11 for WiFi deployment. AP scanning time can be greatly shortened if users only scan those three channels.

Scanning process simplification. In order to simplify the scanning process, we improve the interactive process of the WiFi connection. By adjusting parameters of AP driver layer, WiFi driver can connect APs directly right after finishing scanning, reducing the interaction process. We also modified the notification method of the driver by creating a file node wifistatus through proc file system of Linux. Applications can obtain the current WiFi status by looking at the value of wifistatus. This will significantly reduce time consumption of the system.

We can see from Fig. 4 that after our optimization, the total connection-establishing time is decreased from 2850ms to 950ms. The improvement satisfies the requirements for WiFi connection establishment in VANET (Vehicular Ad-Hoc Network). Moreover, we also proposed a WiFi rate adaptive algorithm based on predicting the distance between AP and vehicle-mounted WiFi devices.

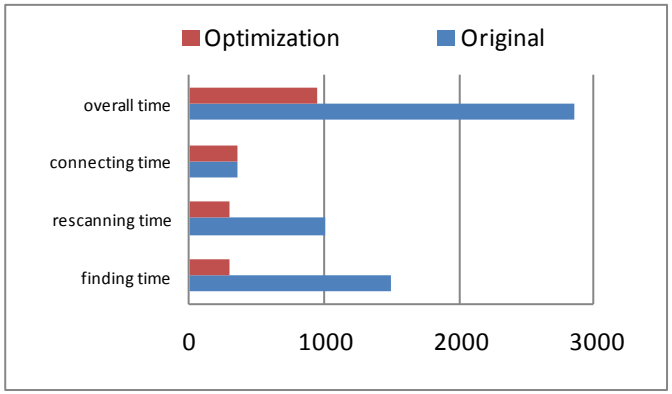


Figure 1 : Optimization of AP connection process.

Targeting the deployment of opportunistic networks based buses; this paper proposed MOONet, a three-layer architecture for data collection and distribution based opportunistic networking, and optimized the WiFi connection-establishing process. With the increasingly widespread distribution of open APs and the increase of vehicle-mounted WiFi devices, MOONet will have great potential deployment in cities in the near future.

References

[1] K. Fall. A Delay-Tolerant Network Architecture for Challenged Internets. In Proc. of 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, August 2003.

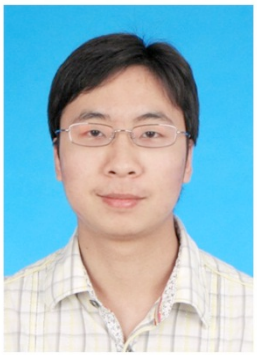
[2] P. Juang, H. Oki, Y. Wang. Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet. In Proc. of the 10th ASPLOS, October 2002.

[3] B. Hull, V. ychkovsky, Y. Zhang. CarTel: A Distributed Mobile Sensor Computing System. In Proc. of 4th International Conference on Embedded Networked Sensor Systems, November 2006.

[4] J. Eriksson, H. Balakrishnan, S. Madden. Cabernet: Vehicular Content Delivery Using WiFi. In Proc. of 14th ACM MOBICOM, September 2008.

Biography

Jianwei Niu received his M.S. and Ph.D. degrees in 1998 and 2002 in computer science from Beijing University of Aeronautics and Astronautics (BUAA, now renamed as Beihang University). He was a visiting scholar at School of Computer Science, Carnegie Mellon University, USA from Jan.28, 2010 to Feb. 1, 2011. He is a professor in the School of Computer Science and Engineering, BUAA. He is an ACM/IEEE member and has published more than 70 referred papers and filed more than 20 patents. His current research interests include pervasive and mobile computing.



Bin Dai is currently a graduate student in the School of Computer Science and Engineering from Beihang University. His main research interests are in the area of data mining, information spreading and the user behavior research in opportunistic & social networks.

Chao Tong received his Ph.D. degrees in 2009 in computer science from Beihang University. He is an assistant professor in the School of Computer Science and Engineering, BUAA. He is an ACM member. His current research interests include mobile computing and social networks analysis.

Review of CKN based Sleep Scheduling in Duty-Cycled Wireless Sensor Network

Chunsheng Zhu[1], Lei Shu[2], Xiping Hu[1], Laurence T. Yang[3], Victor C.M. Leung[1]
[1] Department of Electrical and Computer Engineering, The University of British Columbia, Canada
[2]Guangdong Petrochemical Equipment Fault Diagnosis Key Laboratory, Guangdong University of Petrochemical Technology, China
[3] Department of Mathematics, Statistics and Computer Science, St. Francis Xavier University, Canada
{cszhu, xipingh, vleung}@ece.ubc.ca, lei.shu@lab.gdupt.edu.cn, ltyang@stfx.ca

Abstract—In this paper, focusing on designing a comprehensive sleep scheduling scheme in wireless sensor network (WSN), we review the recently proposed four novel types of connected-*k* neighborhood (CKN) based sleep scheduling schemes: GSS (geographic routing oriented sleep scheduling), GCKN (geographic distance based CKN), SECKN (secured energy-aware CKN), EC-CKN (energy-consumption based CKN). Based on the analytical reviews, we further propose a data content oriented sleep scheduling (DSS) scheme and summarize CKN based sleep scheduling schemes.
Index Terms—Sleep scheduling; WSN; CKN; Duty-cycle

1 Review of CKN Based Sleep Scheduling Schemes

In [1], Nath *et al.* propose a connected-*k* neighborhood (CKN) sleep scheduling scheme to generate a favorable duty-cycled wireless sensor network (WSN) for geographic routing and the focus of CKN is to allow only a portion of sensor nodes to be awake to save energy consumption while the global network is still connected by those awake nodes. As the CKN pseudocode shown above, a random rank is picked by every node in CKN (Step 1 of CKN) and the asleep or awake status of every node is determined locally by itself based on the number and connectivity state of its currently awake neighbor nodes (Step 6 of CKN). Moreover, as shown in Fig. 1, at least some certain number (*k*) awake neighbors will be kept for every node after running CKN and the asleep nodes in the sensor network could be decreased by increasing the value of *k* in CKN.

Based on these desirable features of CKN, there are four novel types of CKN based sleep scheduling schemes designed recently: GSS (geographic routing oriented sleep scheduling) [2], GCKN (geographic distance based CKN) [3], SECKN (secured energy-aware CKN) [4], EC-CKN (energy-consumption based CKN) [5].

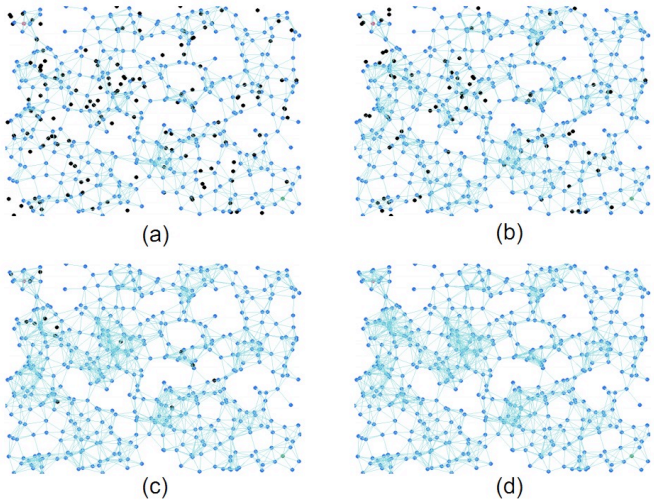


Fig. 1. One example of a CKN based WSN with different *k*. There are total 500 nodes and the *k* in CKN is 1, 2, 4, 8 in (a) (b) (c) (d), respectively. The red node is the source node and the green node is the sink node. The black nodes are asleep nodes and the blue nodes are awake nodes. The line between two nodes means they are neighbors. When the *k* in CKN increases, the number of asleep nodes decreases.

Pseudocode of CKN algorithm
(Run the following at each node u)

1. Pick a random rank $rank_u$.
2. Broadcast $rank_u$ and receive the ranks of its currently awake neighbors N_u. Let R_u be the set of these ranks.
3. Broadcast R_u and receive R_v from each $v \in N_u$.
4. If $|N_u| < k$ or $|N_v| < k$ for any $v \in N_u$, remain awake. Return.
5. Compute $C_u = \{v | v \in N_u \text{ and } rank_v < rank_u\}$.
6. Go to sleep if both the following conditions hold. Remain awake otherwise.
   - Any two nodes in C_u are connected either directly themselves or indirectly through nodes within u's 2-hop neighborhood that have $rank$ less than $rank_u$.
   - Any node in N_u has at least k neighbors from C_u.
7. Return.

Specially, the focus of GSS is to shorten the length of the first transmission path explored by TPGF (Two-phase geographic greedy forwarding) [6] in a CKN based WSN. To achieve this goal, as the pseudocode of GSS shown above, it considers the CKN requirement and geographic routing requirement 1 (i.e., the geographic routing requirement that sensor nodes will choose the neighbor node which is closest to the sink among all neighbor nodes to transmit data). Then it makes the potential nearest neighbor nodes to sink

continue to be awake (Step 6 of second part of GSS), even though the original CKN (the pseudocode without the underline) already determines the node to be asleep.

Pseudocode of GSS algorithm

First: Run the following at each node u.

1. Get its geographic location g_u.
2. Broadcast g_u and receive the geographic locations of its all neighbors A_u. Let G_u be the set of these geographic locations.
3. Unicast a flag to w, $w \in A_u$ and g_w is the closest to sink in G_u.

Second: Run the following at each node u.

1. Pick a random rank $rank_u$.
2. Broadcast $rank_u$ and receive the ranks of its currently awake neighbors N_u. Let R_u be the set of these ranks.
3. Broadcast R_u and receive R_v from each $v \in N_u$.
4. If $|N_u| < k$ or $|N_v| < k$ for any $v \in N_u$, remain awake. Return.
5. Compute $C_u = \{v | v \in N_u \text{ and } rank_v < rank_u\}$.
6. Go to sleep if both the following conditions hold. Remain awake otherwise.
   - Any two nodes in C_u are connected either directly themselves or indirectly through nodes within u's 2-hop neighborhood that have $rank$ less than $rank_u$.
   - Any node in N_u has at least k neighbors from C_u.
   - It does not receive a flag.
7. Return.

Pseudocode of GCKN algorithm

Run the following at each node u.

1. Get the geographic distance between itself and the mobile sink $grank_u$.
2. Broadcast $grank_u$ and receive the geographic distance ranks of its currently awake neighbors N_u. Let R_u be the set of these ranks.
3. Broadcast R_u and receive R_v from each $v \in N_u$.
4. If $|N_u| < k$ or $|N_v| < k$ for any $v \in N_u$, remain awake. Return.
5. Compute $C_u = \{v | v \in N_u \text{ and } grank_v < grank_u\}$.
6. Go to sleep if both the following conditions hold. Remain awake otherwise.
   - Any two nodes in C_u are connected either directly themselves or indirectly through nodes within u's 2-hop neighborhood that have $grank$ less than $grank_u$.
   - Any node in N_u has at least k neighbors from C_u.
7. Return.

In terms of GCKN, the attention is to reduce the transmission paths searched by TPGF in a CKN sleep scheduled WSN, when there is a mobile sink. For performing this aim, GCKN incorporates both the CKN requirement and geographic routing requirement 2 (i.e., there should be as more as possible closer neighbor nodes to the sink for each node so as to make geographic routing obtain more available nodes when the sink is mobile). Based on these two requirements, GCKN further first chooses the graphic distance between the node and the sink $grank_u$ for each node (Step 1 of GCKN). Futhermore, the subset C_u of u's currently awake neighbors having $grank_v < grank_u$ will be calculated (Step 5 of GCKN).

Pseudocode of SECKN algorithm

Run the following for the base station s to find s' secured neighborhood SN_s.

1. Pick the base station's ID i_s, geographic location l_s and a random nonce r_s.
2. Let N_s be the set of the base station's currently awake neighbors. Broadcast i_s, l_s and r_s. Receive the ID i_f, geographic location l_f, random nonce r_f and the authenticator a_f from each $f \in N_s$. $a_f = H_{2K_{f,s}}(r_s||r_f||1)$, $K_{f,s} = \hat{e}(LBK_f, H_1(l_s||i_s))$. Let I_s, L_s, R_s and A_s be the set of these properties.
3. Update I_s, N_s, L_s, R_s, A_s into $\hat{I_s}$, $\hat{N_s}$, $\hat{L_s}$, $\hat{R_s}$, $\hat{A_s}$ by eliminating any f satisfying $(l_{s_x} - l_{f_x})^2 + (l_{s_y} - l_{f_y})^2 > {t_r}^2$ from I_s, N_s, L_s, R_s, A_s.
4. Calculate verifiers $\hat{a_f} = H_{2K_{s,f}}(r_s||r_f||1)$, $K_{s,f} = \hat{e}(LBK_s, H_1(l_f||i_f))$ for each $f \in \hat{N_s}$.
5. Update $\hat{I_s}$, $\hat{N_s}$, $\hat{L_s}$, $\hat{R_s}$, $\hat{A_s}$ into SI_s, SN_s, SL_s, SR_s, SA_s by eliminating any f satisfying $\hat{a_f} \neq a_f$ from $\hat{I_s}$, $\hat{N_s}$, $\hat{L_s}$, $\hat{R_s}$, $\hat{A_s}$.

Run the following for each authenticated node beginning from any node $u \in SN_s$.

1. Pick the node's ID i_u, residual energy e_u, the node's geographic location l_u and a random nonce r_u.
2. Let N_u be the set of the node's currently awake neighbors. Broadcast i_u, e_u, l_u and r_u. Receive the ID i_v, residual energy e_v, geographic location l_v, random nonce r_v and the authenticator a_v from each $v \in N_u$. $a_v = H_{2K_{v,u}}(r_u||r_v||2)$, $K_{v,u} = \hat{e}(LBK_v, H_1(l_u||i_u))$. Let I_u, E_u, L_u, R_u and A_u be the set of these properties.
3. Update I_u, N_u, E_u, L_u, R_u, A_u into $\hat{I_u}$, $\hat{N_u}$, $\hat{E_u}$, $\hat{L_u}$, $\hat{R_u}$, $\hat{A_u}$ by eliminating any v satisfying $(l_{u_x} - l_{v_x})^2 + (l_{u_y} - l_{v_y})^2 > {t_r}^2$ from I_u, N_u, E_u, L_u, R_u, A_u.
4. Calculate verifiers $\hat{a_v} = H_{2K_{u,v}}(r_u||r_v||2)$, $K_{u,v} = \hat{e}(LBK_u, H_1(l_v||i_v))$ for each $v \in \hat{N_u}$.
5. Update $\hat{I_u}$, $\hat{N_u}$, $\hat{E_u}$, $\hat{L_u}$, $\hat{R_u}$, $\hat{A_u}$ into SI_u, SN_u, SE_u, SL_u, SR_u, SA_u by eliminating any v satisfying $\hat{a_v} \neq a_v$ from $\hat{I_u}$, $\hat{N_u}$, $\hat{E_u}$, $\hat{L_u}$, $\hat{R_u}$, $\hat{A_u}$.
6. Broadcast SE_u and receive SE_v from each $v \in SN_u$.
7. If $|SN_u| < k$ or $|SN_v| < k$ for any $v \in SN_u$, remain awake. Return.
8. Compute $SC_u = \{v | v \in SN_u \text{ and } e_v > e_u\}$.
9. Go to sleep if both the following conditions hold. Remain awake otherwise.
   - Any two nodes in SC_u are connected either directly themselves or indirectly through nodes within u's 2-hop secured neighborhood $SN2_u$ that have residual energy more than e_u.
   - Any node in SN_u has at least k neighbors from SC_u.
10. Return.

Regarding SECKN, it researches the issue that there could be potential insider attacks which may seriously affect or even destroy proper sleep scheduling operations and properties for WSN. Particularly, as the SECKN pseudocode shows, it applies the location-based key (LBK) management scheme [7] (including pairing key generation, neighbor node authentication and shared-key establishment) into CKN. During sleep scheduling, SECKN could secure the neighborhood by authenticating neighborhood identity. Also, it is capable of preventing some insider attacks (e.g., Sybil attack [8], Identity replication

attack [9], Sinkhole attack [10]) by utilizing location-based keys.

Pseudocode of EC-CKN algorithm

Step 1: Get the current residual energy $Erank_i$.
Step 2: Broadcast $Erank_i$ and receive the ranks of its currently awake neighbors N_i. Let R_i be the set of these ranks.
Step 3: Broadcast R_i and receive R_j from each $j \in N_i$.
Step 4: If $|N_i| < k$ or $|N_j| < k$ for any $j \in N_i$, remain awake. Go to Step 12.
Step 5: Compute $C_i = \{j | j \in N_i \text{ and } Erank_j > Erank_i\}$.
Step 6: Go to sleep if both the following conditions hold. Remain awake otherwise.
- Any two nodes in C_i are connected either directly themselves or indirectly through nodes within i's 2-hop neighborhood that have $Erank$ more than $Erank_i$.
- Any node in N_i has at least k neighbors from C_i.

Step 7: Return.

With respect to EC-CKN, it take accounts of the network lifetime of the resultant duty-cycled WSN and tries to offer a network lifetime prolonged duty-cycled WSN when designing sleep scheduling scheme. Specially, it studies the fact that the residual energy owned by the awake nodes determined by the sleep scheduling scheme should be more than that of the asleep nodes determined by the algorithm (Step 1, Step 5 and Step 6 of pseudocode of EC-CKN). Or else, the sleep scheduled WSN will not last long since some low energy reserved awake nodes will run out of energy very soon.

However, all above CKN based sleep scheduling schemes overlook one significant fact that the resultant sleep scheduled WSN may actually not be able to transmit the data which indicates the physical or environmental changes (e.g., temperature change, humidity change) in real time. The reason is that some sensors may collect a large data change (e.g., temperature change) but the sleep scheduling process does not consider the data content of the sensors. Although the asleep or awake status of a node cannot be always unchanged, these sensors which gather warning data (e.g., highest temperature) may be asleep for several epoches. When they have the opportunity to be awake to transmit their data, maybe the disaster (e.g., forest fire) is already impossible to be deal with.

2 Proposed data content oriented sleep scheduling (DSS) scheme

To solve the issue of the current CKN based sleep scheduling schemes, we further propose a data content oriented sleep scheduling (DSS) scheme. And the CKN requirement and the data content requirement are incorporated when designing the new DSS scheme. Particularly, we take account of the following four design elements: (1) a node should go to sleep assuming that at least *k* of its neighbors will remain awake so as to save energy consumption and keep it *k*-connected; (2) the outcome of the asleep or awake status of nodes should be capable of changing over epoches to make sure that all nodes own the opportunity to be asleep. This can avoid making any node always be awake, and the whole network lifetime are prolonged. (3) despite the fact that each node decides to be asleep or awake locally, the whole network should be globally connected so that data transmission can be conducted; (4) the sensor with more data scope should be awake so that these potential more important data indicating environmental changes can be transmitted.

The pseudocode of DSS is shown below. Specially, for each node *u*, the scope of the gathered data is obtained (Step 1 of DSS) and the subset C_u of *u*'s currently awake neighbors having $Drank > Drank_u$ is calculated (Step 5 of DSS). Before *u* can go to sleep, it has to make sure that (1) all sensor nodes in C_u are connected by nodes with $Drank > Drank_u$ (2) each of its neighbors owns at least *k* neighbors from C_u (Step 6 of DSS). The last design element of DSS is the extra factor and also unconsidered factor in contrast with the design factors of the previously proposed sleep scheduling schemes.

Pseudocode of DSS algorithm
(Run the following at each node u)

1. Get the scope of collected data $Drank_u$.
2. Broadcast $Drank_u$ and receive the data scope ranks of its currently awake neighbors N_u. Let R_u be the set of these ranks.
3. Broadcast R_u and receive R_v from each $v \in N_u$.
4. If $|N_u| < k$ or $|N_v| < k$ for any $v \in N_u$, remain awake. Return.
5. Compute $C_u = \{v | v \in N_u \text{ and } Drank_v > Drank_u\}$.
6. Go to sleep if both the following conditions hold. Remain awake otherwise.
   - Any two nodes in C_u are connected either directly themselves or indirectly through nodes within u's 2-hop neighborhood that have $Drank$ larger than $Drank_u$.
   - Any node in N_u has at least k neighbors from C_u.
7. Return.

3 Summary of CKN based sleep scheduling schemes

Connected-*k* neighborhood (CKN) based sleep scheduling schemes have a natural advantage of fulfilling the favorable characteristics of CKN. Based on the above analysis of all CKN based sleep scheduling schemes, as Table I shows, we can actually further observe that current CKN based sleep scheduling schemes focus on the following four aspects: 1) data content (by DSS) 2) data transmission path of TPGF (by GSS and GCKN) 3) sensor energy (by EC-CKN) 4) sensor security (by SECKN). DSS, GSS and GCKN pay particular attention to the data aspect, while EC-CKN and SECKN

concern the sensor itself. Moreover, GSS and GCKN are geographic routing oriented sleep scheduling schemes whereas others are not. In addition, GCKN is the only sleep scheduling scheme considering the mobility of the sink.

To propose a comprehensive sleep scheduling scheme for wireless sensor network (WSN) to fully take advantage of duty-cycle to save energy consumption, these four elements (i.e., data content, data transmission path, sensor energy and sensory security) are all crucial. While it may be difficult to consider all four factors to design a sleep scheduling algorithm since WSN is application specific, hybrid sleep scheduling schemes may be worth a try.

Table I. Comparison of CKN based sleep scheduling schemes

Scheme	Focus	Geographic routing oriented	Sink mobility considered
DSS	Data content	No	No
GSS	Data transmission path	Yes	No
GCKN	Data transmission path	Yes	Yes
EC-CKN	Sensor energy	No	No
SECKN	Sensor security	No	No

Acknowledgment

This work is supported by a Four Year Doctoral Fellowship from the University of British Columbia and by funding from the Natural Sciences and Engineering Research Council.

References

[1] S. Nath, and P. B. Gibbons, "Communicating via fireflies: Geographic routing on duty-cycled sensors," in *Proc. IPSN*, 2007, pp. 440–449.

[2] C. Zhu, L. T. Yang, L. Shu, J. J. P. C. Rodrigues, and T. Hara, "A geographic routing oriented sleep scheduling algorithm in duty-cycled sensor networks," in *Proc. ICC*, 2012, pp. 7001–7005.

[3] C. Zhu, L. T. Yang, L. Shu, L. Wang, and T. Hara, "Sleep scheduling towards geographic routing in duty-cycled sensor networks with a mobile sink," in *Proc. SECON*, 2011, pp. 158–160.

[4] C. Zhu, L. T. Yang, L. Shu, T. Q. Duong, and S. Nishio, "Secured energy-aware sleep scheduling algorithm in duty-cycled sensor networks," in *Proc. ICC*, 2012, pp. 1981–1985.

[5] L. Wang, Z. Yuan, L. Shu, L. Shi, and Z. Qin, "An energy-efficient ckn algorithm for duty-cycled wireless sensor networks," *International Journal of Distributed Sensor Networks*, 2012.

[6] L. Shu, Y. Zhang, L. T. Yang, Y. Wang, M. Hauswirth, and N. Xiong, "Tpgf: Geographic routing in wireless multimedia sensor networks," *Telecommunication Systems*, vol. 44, no. 1–2, pp. 79–95, 2010.

[7] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise tolerant security mechanisms for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 247–260, 2006.

[8] J. R. Douceur, "The sybil attack," in *Proc. IPTPS*, 2002, pp. 251–260.

[9] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proc. IPSN*, 2004, pp. 259–268.

[10] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc Networks*, vol. 1, no. 2, pp. 293–315, 2003

Biography

Chunsheng Zhu [S'12] is currently a PhD student in the Department of Electrical and Computer Engineering at The University of British Columbia in Canada from September 2012. He obtained a master degree in Computer Science from St. Francis Xavier University in Canada, in May 2012. And he received a bachelor degree in Network Engineering from Dalian University of Technology in China, in June 2010. His current research interests are mainly in the areas of wireless sensor networks and mobile cloud computing. He is a student member of IEEE.

Lei Shu [M'07] received the B.Sc. degree in Computer Science from South Central University for Nationalities, China, in 2002 and the M.Sc. degree in Computer Engineering from Kyung Hee University, Korea, in 2005 and the Ph.D. degree in Digital Enterprise Research Institute, from National University of Ireland, Galway, Ireland, in 2010.

He is currently a full professor in College of Electronic Information and Computer, Guangdong University of Petrochemical Technology, China, also the vice-director of the Guangdong Petrochemical Equipment Fault Diagnosis (PEFD) Key Laboratory. He was a specially assigned research fellow in Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, Japan. He has published over 150 papers in relat-

ed conferences, journals, and books. He had been awarded the MASS 2009 IEEE TCs Travel Grant and the Outstanding Leadership Award of EUC 2009 as Publicity Chair, the Globecom 2010 Best Paper Award. He has served as Editor-in-Chief for IEEE COMSOFT E-Letter, and editor for Wiley, European Transactions on Telecommunications, IET Communications, KSII Transactions on Internet and Information Systems (TIIS), Journal of Communications, Inderscience, International Journal of Sensor Networks, and Wiley, Wireless Communications and Mobile Computing. He has served as Co-Chair for more than 50 international conferences/workshops, e.g., IWCMC, ICC, ISCC; and TPC member of more than 150 conferences, e.g., ICC, GLOBECOM, ICCCN, WCNC, ISCC. His research interests include wireless sensor network, sensor network middleware, multimedia communication, and security. He is a member of IEEE and IEEE ComSoc.

Xiping Hu joined the UBC in September 2011, and he is now working towards his PhD at the Electrical and Computer Engineering department of UBC. Before that, he worked as a research assistant in the National Research Council of Canada - Institute for Information Technology (NRC-IIT) and UNB, and obtained his master degree in Computer Science from UNB in May, 2011. He is the winner of silver prizes in national Olympic competitions in mathematics and physics in China, and the Microsoft certified specialist in web applications and SQL server. Also, he participated in and as key member in several research projects, like web service security identification at Tsinghua University in China, SAVOIR project at NRC-IIT, and NSERC DIVA research strategy network at UBC. His research contributions has been published and submitted to series of international conferences and journals, such as Procedia CS, HICSS, IEEE TPDS, ACM MobiSys etc. His current research areas at UBC are mobile social networks, software architecture, crowdsourcing, and human computer interaction and so on.

Laurence T. Yang received the B.E. degree from Tsinghua University, China, and Ph.D. degree from University of Victoria, Canada.

He is currently a Professor in Department of Mathematics, Statistics and Computer Science, St. Francis Xavier University, Canada. He has published around 300 papers in related conferences, journals, and books. He served as the vice-chair of IEEE Technical Committee of Supercomputing Applications (TCSA) until 2004, currently is the chair of IEEE Technical Committee of Scalable Computing (TCSC), the chair of IEEE Task force on Ubiquitous Computing and Intelligence, the co-chair of IEEE Task force on Autonomic and Trusted Computing. He is serving as an editor for around 20 international journals and has been acting as an author/co-author or an editor/co-editor of 25 books from Kluwer, Springer, Nova Science, American Scientific Publishers and John Wiley & Sons. He has also been involved in more than 100 conferences and workshops as a program/general/steering conference chair and more than 300 conference and workshops as a program committee member. His research interests include high performance computing and networking, embedded systems, ubiquitous/pervasive computing and intelligence.

Victor C. M. Leung [S'75, M'89, SM'97, F'03] received the B.A.Sc. (Hons.) degree in electrical engineering from the University of British Columbia (UBC) in 1977, and was awarded the APEBC Gold Medal as the head of the graduating class in the Faculty of Applied Science. He attended graduate school at UBC on a Natural Sciences and Engineering Research Council Postgraduate Scholarship and completed the Ph.D. degree in electrical engineering in 1981.

From 1981 to 1987, Dr. Leung was a Senior Member of Technical Staff and satellite system specialist at MPR Teltech Ltd., Canada. In 1988, he was a Lecturer in the Department of Electronics at the Chinese University of Hong Kong. He returned to UBC as a faculty member in 1989, and currently holds the positions of Professor and TELUS Mobility Research Chair in Advanced Telecommunications Engineering in the Department of Electrical and Computer Engineering. Dr. Leung has co-authored more than 600 technical papers in international journals and conference proceedings, 26 book chapters, and co-edited 6 book titles. Several of his papers had been selected for best paper awards. His research interests are in the areas wireless networks and mobile systems.

Dr. Leung is a registered professional engineer in the Province of British Columbia, Canada. He is a Fellow of IEEE, a Fellow of the Engineering Institute of Canada, and a Fellow of the Canadian Academy of Engineering. He was a Distinguished Lecturer of the IEEE Communications Society. He is a member of the editorial boards of the IEEE Transactions on Computers, IEEE Wireless Communications Letters, Computer Communications, the Journal of Communications and Networks, and several other journals, and has previously served on the editorial boards of the IEEE Journal on Selected Areas in Communications – Wireless Communications Series, the IEEE Transactions on Wireless Communications and the IEEE Transactions on Vehicular Technology. He has guest-edited many journal special issues, and contributed to the organizing committees and technical program committees of numerous conferences and workshops. He is a recipient of an IEEE Vancouver Section Centennial Award and a 2012 UBC Killam Research Prize.

Locating using Prior Information: Wireless Indoor Localization Algorithm

Yuanfang Chen[1], Noel Crespi[1], Lin Lv[2], Wenzhe Zhang[2]
[1]Institut Mines-Telecom, France
[2]School of Software, Dalian University of Technology, China
yuanfang.chen@etu.upmc.fr, noel.crespi@mines-telecom.fr, lvlin1023@gmail.com, hanson-zhe@gmail.com

Indoor localization is of great importance for a range of pervasive applications, attracting many research efforts in the past fifteen years. Most indoor localization algorithms are Received Signal Strength (RSS)-based, in which RSS signatures of an interested area are annotated with their real recorded locations. However, according to our experiments, RSS signatures are not suitable as the unique annotations (like Fingerprints) of recorded locations. In this study, we investigate the characteristics of RSS first (e.g., how the RSS change as time goes on and between neighboring positions?). Then with user motions, we use novel sensors integrated in smartphones to construct the radio map of a floor plan as prior information. On this basis, we design LuPI, an indoor localization algorithm. LuPI exploits the characteristics of RSS. The deployment of LuPI is easy and rapid since little human intervention is needed. In LuPI, the calibration of radio map is crowd-sourced, automatic and scheduled. Experimental results show that LuPI achieves comparable location accuracy to previous approaches, even without the statistical information of site survey.

The last ten years could rightly be coined the decade of smart connected devices. In 2011, 494 million devices were sold [1].
Moreover, the popularity of mobile and pervasive computing stimulates extensive research on wireless indoor localization. Based on the potential functionality of these sensor-embedded mobile devices, many solutions are introduced to provide room-level location-based services, for example, locating a person or a printer in an office building. Even, data collection from mobile phones can be used to uncover regular rules and structure in behavior of both individuals and crowds.
In this paper we utilize the Received Signal Strength (RSS) and the sensor-based pedometer of smartphone to build a RSS variation space as prior information, first. Then based on this prior information, we can estimate the location of a mobile node.

RSS can be easily obtained from most off-the-shelf wireless network equipments (such as WiFi- or ZigBee-compatible devices) [2]. However the obtaining of RSS as a database to support indoor localization (e.g., RSS fingerprint space) is time-consuming and labor-intensive. Moreover RSS database is vulnerable due to environmental dynamics (Fig. 1). These weaknesses are inevitable for RSS-based approaches. For mitigating the influence of environmental changes on RSS absolute values, we use the relative change of RSS related to WiFi- or ZigBee-compatible devices.

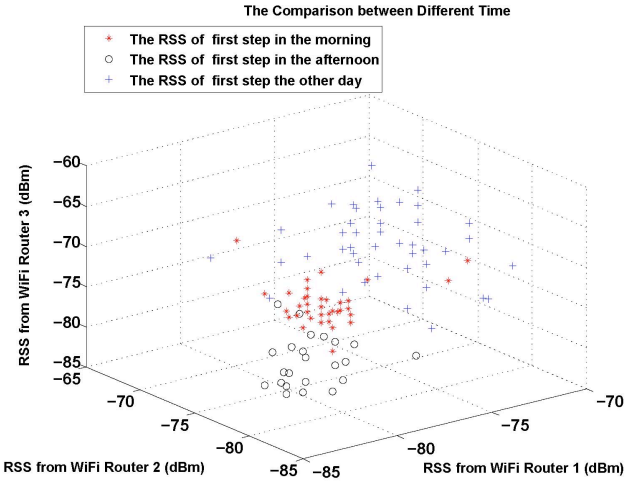


Figure 1: The Instability of RSS Values

Nowadays mobile phones possess powerful computation and communication capability, and are equipped with various functional built-in sensors. Along with the carrying of users is round-the-clock, mobile phones can be seen as an important information interface between users and environments. These advances are solid foundations of breakthrough technology for indoor localization. The pedometer is based on accelerometer which embedded in a smartphone. The pedometer can be used to record the number of footsteps, which can be accurately measured by smartphones nowadays, with respect to the displacement and directions of users' movements.
In this study, we propose LuPI (Locating using Prior Information), a wireless indoor localization algorithm. The key idea of LuPI is that human motions can be distinguished and recorded by radio information (e.g., RSS deviation) and pedometer. LuPI requires no prior knowledge of Access Point (AP) locations which are often unavailable in commercial or office buildings where

APs are installed by different organizations. In addition, accessing these APs by password is also unnecessary.

To estimate the performance of LuPI, we deploy a prototype system and conduct extensive experiments in a middle-size building (Fig. 2). Experiment results show that LuPI achieves comparable location accuracy to previous approaches, even without the statistical information of site survey.

Figure 2: Middle-size Building.

Many techniques have been proposed for indoor localization during the past two decades. Generally, they fall into two categories: fingerprinting-based and model-based.

The main idea of fingerprinting-based approaches is to collect the surrounding radio signatures at every location in the interested areas and then build a fingerprint database. The location is then estimated by mapping the measured fingerprints of database. All these approaches require site survey over interested areas to build a fingerprint database. In addition to the inflexibility to environment dynamics, the manual cost is considerable.

Model-based approaches trade the time-consuming measurement efforts (for increasing localization accuracy) with geometrical models. For several approaches based on AP locations and radio propagation models, the average localization error is greater than 5 meters [3].

Locating Using Prior Information (LuPI)

LuPI uses the RSS variation space as prior information. Based on the path attenuation effect (Fig. 3) the RSS variation space is built.

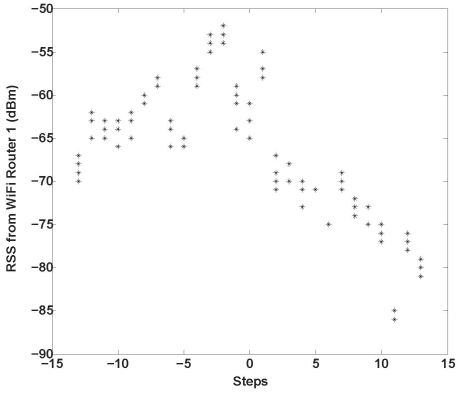


Figure 3: Path Attenuation Effect: RSS decreases along with the increase of the distance between the WiFi Router 1 and the mobile node.

The steps of LuPI are shown as follows.

Input: One hundred RSS sets from three different WiFi Routers at each step, $[RSS_1 = (rss_1, rss_2, rss_3), RSS_2, ..., RSS_{100}]$

Step 1: Build the RSS variation space: (1) Partition all RSS sets into k clusters in which each set belongs to the cluster with the nearest mean, using the k-means clustering, where the k is the number of steps. Moreover the cluster center can be obtained for each step. (2) Calculate the distance matrix $D = [d_{ij}]_{k \times k}$. The element of matrix D is the Euclidean distance between cluster centers, e.g., the d_{12} is the RSS set Euclidean distance between the step 1 and the step 2. (3) Calculate the relative coordinate matrix Y concerning all steps, using Multidimensional Scaling (MDS) algorithm [4], based on the distance matrix D. (4) Accumulate coordinates and construct the RSS variation space. The elements of matrix D and Y form the RSS variation space.

Step 2: Locate a mobile node using the RSS variation space. (1) Add the current RSS set of mobile node to the RSS variation space as a new element, and update the distance matrix D. (2) According to the new distance matrix, the new relative coordinate matrix Y can be calculated. The mobile node can be located with a relative coordinate in the RSS variation space.

Output: The location of a mobile node.

Performance Evaluation

We develop the prototype of LuPI on the increasingly popular Android OS which supports WiFi and accelerometer sensors. We conduct the experiment on the second floor of a typical academic building and two laboratories of the

building (Fig. 4). Three APs are installed, without location information.

Figure 4: Two laboratories Deployed the Prototype System based on LuPI

We sample the experiment area every two grids as a step (0.6m×0.6m for one grid). Only three volunteers are needed in the experiment. LuPI records the pedometer readings (how many steps) to count the walking distance, and at the same time LuPI picks up RSS values along the walking path.

We implement LiFS [5], and compare its performance with LuPI on the same experiment data. The average localization errors of LuIP are 1.39356 meters and 1.88574 meters for two laboratories, respectively, which are smaller than LiFS (5.88 meters). Even in the corridor the performance of LuPI is comparable to the state-of-the-art model-based approaches (larger than 5 meters) reported in [3], and outperforms EZ (larger than 7 meters) [6].

We estimate 248 localization queries on LuPI. For the big room we integrate all the localization results, as shown in Fig. 5.

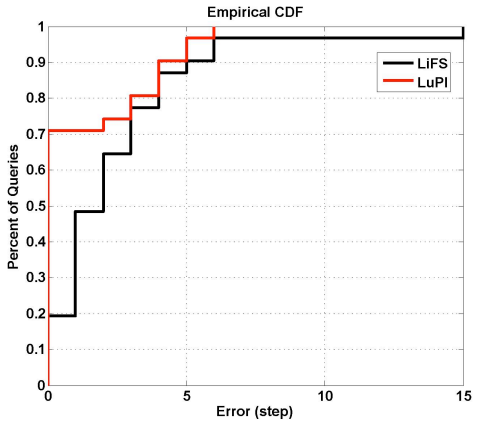


Figure 5: CDF of Localization Error in the Big Room

The integrated localization result for the small room is shown in Fig. 6.

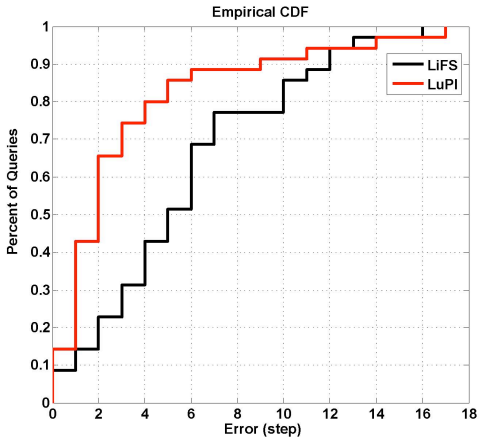


Figure 6: CDF of Localization Error in the Small Room

Fig. 7 shows the CDF (Cumulative Distribution Function) of localization error for the corridor.

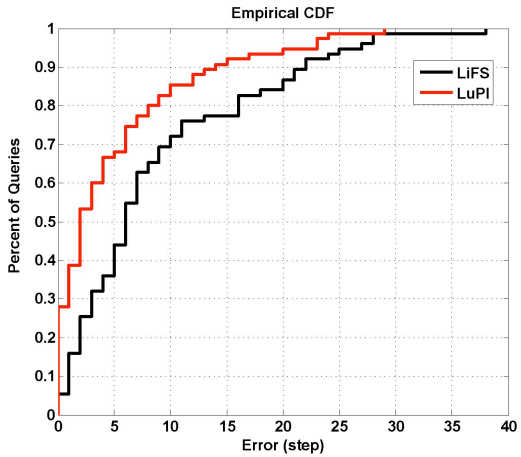


Figure 7: CDF of Localization Error in the Corridor

As shown in the Fig. 5, for the room, the localization error of 100% queries is under 7.2 meters while about 90% is under 4.8 meters. For the corridor localization error (Fig. 7): 69% queries is under 6 meters. The accuracy of LuIP is impressive, as LuIP needs no site survey and no specific infrastructure.

Conclusion

The average localization error is 5.91996 meters in the corridor, the average localization error is 1.39356 meters in the big room, and the average localization error is 1.88574 meters in the small room. So the localization accuracy of LuPI is room-level. Moreover, the localization errors of 50% localization queries are less than 2.4 meters in the corridor, and the localization errors of 90% localization queries are less than 4.8 meters in the big room, and the localization errors of 50% localization queries are less than 1.2 meters in the small room.

References

[1] I. D. C. (IDC), Worldwide Smart Connected Device Shipments, 2010-2016 (Unit Millions), March 27, 2012. [Online]. Available: http://www.idc.com/.

[2] M. Bshara, U. Orguner, F. Gustafsson, and L. Van Biesen, "Fingerprinting localization in wireless networks based on received-signal-strength measurements: a case study on wimax networks," Vehicular Technology, IEEE Transactions on, vol. 59, no. 1, pp. 283-294, 2010.

[3] D. Turner, S. Savage, and A. Snoeren, "On the empirical performance of self-calibrating wifi location systems," in Local Computer Networks (LCN), 2011 IEEE 36th Conference on, IEEE, pp. 76-84, 2011.

[4] I. Borg and P. Groenen, "Modern multidimensional scaling: Theory and applications," Springer, 2005.

[5] Z. Yang, C. Wu, and Y. Liu, "Locating in fingerprint space: wireless indoor localization with little human intervention," in Proceedings of the 18th Annual International Conference on Mobile Computing and Networking, ACM, pp. 269-280, 2012.

[6] K. Chintalapudi, A. Padmanabha Iyer, and V. Padmanabhan, "Indoor localization without the pain," in Proceedings of the sixteenth Annual International Conference on Mobile Computing and Networking, ACM, pp. 173-184, 2010.

Biography

Yuanfang Chen is a team member of Service Architecture Lab, Institut Mines-Télécom, Pierre and Marie Curie University-Paris 6, where she is currently pursuing her PhD on the issues of Internet of Things. She is working with Prof. Noel Crespi. Her research interests are wireless sensor networks and human dynamics. She received the M.Sc. degree in Dalian University of Technology, China. She received the B.E. degree in Zhejiang University of Technology, China. She is an assistant researcher in Illinois Institute of Technology (Xiang-Yang Li), U.S.A., from 2009 to 2010. She had been awarded the MASS 2009 IEEE Travel Grant, IWCMC 2009 and MSN 2010 Invited Paper. She has served as volunteer of Mobicom & Mobihoc 2010 and IEA-AIE 2012. She has been invited as the TPC member of ICCNT 2011, GPC 2011 & 2013 and ICCIT 2012; and the Publicity Co-Chairs of the International Symposium on Mobile and Wireless Network Security 2011. She has served as reviewer of journals and conferences, e.g., Ad Hoc & Sensor Wireless Networks. She is a student member of IEEE and ACM. Current Research: Yuanfang Chen focuses on localization algorithm and MAC layer performance optimization. Based on her previous experience, she has built a crowd model with the human behavior based on the location information of wireless networks. Moreover, the model can be used to analyze the social behavior of human (human dynamics; location-based human social behavior analysis).

Professor Noël Crespi holds Masters degrees from the Universities of Orsay and Canterbury, a Diplome d'ingénieur from Telecom ParisTech and a Ph.D and Habilitation from Paris VI University. From 1993-95 he worked at CLIP, Bouygues Telecom, before joining France Telecom R&D in 1995 where he was involved in Intelligent Network paradigms for value added services. For Orange he led the Mobicarte prepaid service project to define, architect and deploy an infrastructure that hosted more than 10 million mobile subscribers. He has played a key role in standardisation as a delegate in a number of committees and as the editor for CAMEL, the Intelligent Network standard for mobile networks. He was appointed as the coordinator for France Telecom's standardisation activities for Core Network and then for all GSM/UMTS standards at the ETSI plenary committee. In 1999, he joined Nortel Networks as telephony programme manager for France and Middle East-Africa. He was responsible for the evolution of the switching area, and led key programmes for the evolution of Nortel products. He has also worked for ETSI as an independent contractor. He joined Institut Mines-Telecom in 2002 and is currently Professor and MSc Programme Director, leading the Service Architecture Laboratory. He coordinates the standardisation activities for Institut Telecom at ETSI, 3GPP and ITU-T. He is also a visiting professor at the Asian Institute of Technology as well as adjunct professor at KAIST (Korea), and is on the 4-person Scientific Advisory Board of FTW (Austria). His current research interests are in Service Architectures, Communication Services, P2P Social Networks, and Internet of Things/Services. He is the author/co-author of more than 250 papers and contributions in standardisation and is an IEEE senior member.

The Performance Analysis of Robust Image Hashing Using Slant Transform

Delong Cui[1,2], Yunfeng Gong[2]
[1]Guangdong Petrochemical Equipment Fault Diagnosis Key Laboratory, Guangdong University of Petrochemical Technology, China
[2] College of Computer and Electronic Information, Guangdong University of Petrochemical Technology, China
delongcui@163.com, yunfenggong@126.com

In order to improve the efficient and simple the steps of generation an image hashing, a security and robustness image hashing algorithm based on Slant transform(ST) is proposed in this paper. By employing coefficients of Slant transform, a robust hashing sequence is obtained by preprocessing, feature extracting and post processing. The security of proposed algorithm is totally depended on the user-key which are saved as secret keys. For illustration, several benchmark images are utilized to show the feasibility of the image hashing algorithm. Experimental results show that the proposed scheme is robust against perceptually acceptable modifications to the image such as JPEG compression, mid-filtering, and rotation. Therefore, the scheme proposed in this paper is suitable for image authentication, content-based image retrieval and digital watermarking, etc.

With the rapid development of information-communication and personal computers, copyright protection of digital media as image, video and audio becomes a more and more important issue. Image hash as one of content-based image authentication techniques has become an important research topic recently. An image hash function maps an image to a short binary string based on the image's appearance to the human eye, so it can be used in authentication, content-based image retrieval and digital watermarking.

Security and robustness are two important requirements for image hash functions. By security, it means that one image should have different function values according to the different applications. By robustness, it means that the hash function should keep invariable by common image processing operations such as additive noise, filtering, compression, etc. The underlying techniques for constructing image hashes can roughly be classified into property-based, such as statistics; interaction relation of transform field decomposition coefficients; vision-based feature points, etc; and content-based, such as transform field significantly coefficients. Typical case of property-based image hash is proposed by Venkatesan et. al [1]., which gets statistics by using decomposition coefficients of discrete wavelet transform (DWT). A relation-based technique generates a hash sequence by employing invariant relation of image blocks, which is expect robust to JEPG compression. For sensitive to geometric attacks, the vision-based image hash is inefficacy under common image processing. On the contrary, the content-based algorithm for its super robustness performance became more and more popular, but an expensive search is needed to handle manipulations.

Researchers have recently shown an increased interest in Slant transform (ST) and acquired achievements. [2-5]. In this paper, an image hashing algorithm based on ST is proposed for certain application. The scheme extracts a robust feature vector to generate a content-based hash sequence, which includes three-step preprocessing, feature generation and post processing. To improve the security of the proposed scheme, the user-keys are used as the encryption keys. Experimental results show that the proposed scheme is robust against common image processing.

The concept of an orthogonal transformation containing Slant basis vector was introduced by Enomoto and Shibata [6]. The Slant vector is a discrete saw tooth waveform decreasing in uniform steps over its length. It has been seen that Slant vectors are suitable for efficiently representing gradual brightness change in a face image line.

Slant Matrix Construction:

If $S(n)$ denotes the $N \times N$ Slant matrix(N=2^n),then

$$S(1) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1}$$

The Slant matrix for N=4 can be written as

$$S(2) = \frac{1}{\sqrt{4}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ a+b & a-b & -a+b & -a-b \\ 1 & -1 & -1 & 1 \\ a-b & -a-b & a+b & -a+b \end{bmatrix} \tag{2}$$

where a and b are real constants to be determined subject to the following conditions:

(1) step size must be uniform

(2) S(2) must be orthogonal

The properties of Slant transform are as follows:

(1) The Slant transform is real and orthonormal

$$S = S^*, S^{-1} = S^t \tag{3}$$

(2) It is a fast algorithm reducing the complexity to $O(N \log_2 N)$ for $N \times 1$ vector

(3) It is very good in energy compaction for facial images. Very few coefficients are sufficient for recognizing the stored image of face in database.

The above Slant matrices are used to define the ST as

$$D_x(n) = S(n)X(n) \tag{4}$$

where

$$D_x(n)' = [D_x(0)D_x(1)\mathrm{L}\ \ D_x(N-1)] \tag{5}$$

$$X(n)' = [X(0)X(1)\mathrm{L}\ \ X(N-1)] \tag{6}$$

$S(n)$ is $N \times N$ Slant Matrix.

For analysis the performance of Slant transform in image hashing algorithm. An image hashing algorithm based on Slant transform is proposed in this paper. The image hash scheme can be constructed by preprocessing, extracting and post processing appropriate image features. In order to improve the property of feature extracting, the preprocessing of image is always used. The common image preprocessing includes applying a low-pass filter, rescaling, or adjusting the components of image, and so on. But in this paper, for analysis the performance of Slant transform, all the processing of image seemed as attacks to original image. To achieve robustness, security, and compactness, the feature extraction is the most important stage of constructing an image hash. A robust image feature extraction scheme should withstand various image processing that does not alter the semantic content. Various image hashing schemes mainly differ in the way randomized features and extracted. For post-processing, the aim is compression the length of hash sequence and without less the magnitude feature.

The framework of proposed hashing algorithm is shown in Fig.1, which includes the following steps:

Block image: block original image to $n \times n$ sub-images. For example, the blocks size is 8×8.

Slant transform: using the Slant transform to every block images.

Feature extraction: selected the middle-frequency coefficients by user-key.

Compression: compression the selected coefficients, and obtain the image hashing finally.

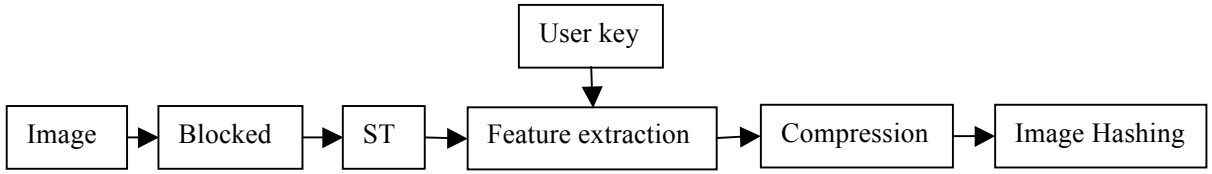


Figure 1 : The framework of proposed hashing algorithm

Performance metrics and experiment setup: to measure the performance of image hash, the normalized Hamming distance between the binary hashes is employed. The defined of normalized Hamming distance is:

$$d(h_1, h_2) = \frac{1}{L}\sum_{k=1}^{L} |h_1(k) - h_2(k)| \tag{7}$$

where $h_1(k)$, $h2(k)$ are different image hash sequence values; L is the length of image hash. The normalized Hamming distance d has the property that for dissimilar images, the expected of d is closed to 0.5, else the expected is closed to 0.

Several benchmark images (such as Lena, Baboon, Peppers, F16, Cameraman, etc) are used to test the performance of the proposed scheme. Images used in this paper are shown in Fig.2, and the experimental results in Tab.1.

1. 2. 3. 4.

5. baboon 6. cameraman 7. canal 8. elaine

9. 10. 11. 12.

13. frog 14. lena 15. peppers 16. sailboat

Figure 2 : Several benchmark images

Table 1 . Normalized Hammming Distances of proposed algorithm between benchmark image

attacks	factor	Normalization Hamming distance							
Jpeg comp.	2	0.0918	0.0811	0.1182	0.1289	0.1191	0.1182	0.0645	0.0713
	3	0.0869	0.0859	0.1348	0.1338	0.1084	0.1318	0.0586	0.0605
	4	0.0947	0.0977	0.1387	0.1387	0.1104	0.1533	0.0791	0.0742
	5	0.0928	0.0986	0.1523	0.1494	0.1162	0.1543	0.0801	0.0771
	6	0.0928	0.1484	0.1553	0.1611	0.1201	0.2031	0.1396	0.1348
	7	0.0928	0.5010	0.4326	0.4502	0.1094	0.5010	0.4883	0.4775
	8	0.4521	0.4990	0.2021	0.2021	0.1094	0.1611	0.1289	0.1260
	9	0.0928	0.4990	0.5674	0.5498	0.1094	0.4990	0.5117	0.5225
median-filter	3	0.0576	0.0459	0.0615	0.0654	0.0713	0.0703	0.0313	0.0410
	5	0.0723	0.0674	0.0908	0.0908	0.0859	0.0928	0.0479	0.0479
	7	0.0850	0.0684	0.1074	0.1006	0.0977	0.1055	0.0615	0.0527
	9	0.0967	0.0791	0.1162	0.1182	0.1025	0.1094	0.0664	0.0635
Gaussian low-pass	/	0	0	0	0	0	0	0	0
Gaussian noise	0.05	0.0474	0.0495	0.0481	0.0479	0.0479	0.0520	0.0501	0.0499
	0.01	0.0474	0.0495	0.0481	0.0479	0.0479	0.0520	0.0501	0.0499
Peppers and slat noise	/	0.0151	0.0174	0.0396	0.0424	0.0220	0.0277	0.0103	0.0121
Cut	1/8	0	0.0156	0.0156	0.0156	0	0.0117	0.0156	0.0156
Rescaling	0.5	0.0459	0.0898	0.0684	0.0947	0.0811	0.1299	0.0059	0.0459
	2	0	0	0	0	0	0	0	0
Rotation	10^0	0.0818	0.0501	0.0356	0.0364	0.0742	0.0567	0.0384	0.0388
	15^0	0.0765	0.0501	0.0354	0.0368	0.0698	0.0555	0.0394	0.0383

In this work, a novel robust image hash scheme for certain application is proposed. The Slant transform is used for constructing robust image hashes, and the user-key are used as the encryption key. The image is first blocked to sub-images, then after the Slant transform of every block image, feature vector is extracted from the transform field coefficients, finally the resulting statistics vector is quantized and the binary hashes sequence is obtained. Experimental results show that the proposed scheme is robust against common image processing such as JPEG compression, mid-filtering, and rotation. Therefore, the scheme proposed in this paper is suitable for image authentication, content-based image retrieval and digital watermarking.

Acknowledgments

The work presented in this paper was supported by both Guangdong University of Petrochemical Technologys Internal Project (No. 2012RC0106), and Maoming Municipal Science & Technology Program (No. 0008176170622027). Yunfen Gong is the corresponding author.

References

[1] S. Pei, J. Ding, “Closd-form Discrete Fraction and Affine Fourier Transforms”, IEEE Trans on Signal Processing, vol. 48, no.5, pp. 1338-1353, 2000.

[2] C. Hsieh, J. Lin, S. Huang, "Slant transform applied to electric power quality detection with field programmable gate array design enhanced", International Journal of Electrical Power & Energy Systems, vol.32, no.5, pp.428-432, June 2010.

[3] R. Bao,"Semi-fragile watermarking algorithm of color image based on Slant Transform and channel coding" , in 2011 4th International Congress on Image and Signal Processing (CISP), 2011,pp.1039-1043.

[4] H. B. Kekre and Kamal Shah, “Performance Comparison of Row, Column, Full Slant Transform and PCA for Face Recognition”, International Journal of Computing Science and Communication Technologies, vol. 2, no. 1, pp. 249-255,July 2009.

[5] N.B Patil, V.M Viswanatha, S. Pande MB, "SLANT TRANSFORMATION AS A TOOL FOR PRE-PROCESSING IN IMAGE PROCESSING", International Journal of Scientific & Engineering Research, Vol.2, no.4, pp. 1-7, April-2011.

[6] Enomoto, K. Shibata, “Ortogonal Transform Coding System for Televiison Signals”, IEEE Transaction On Electromegnetic Compitibility, vol.13. no.3, Aug. 1971.

Biography

Delong Cui is currently an associate professor in the School of Computer and Electronic Information, Guangdong University of Petrochemical Technology. He received his M.S. degree from Department of communication and information system, Southwest Jiao tong University in 2008. His research interests include multimedia security, data hiding, and image/audio watermarking.

Yunfen Gong, is currently a lecturer in the School of Computer and Electronic Information, Guangdong University of Petrochemical Technology. He received his M.S. degree from Department of Computer Software and Theory, Huazhong University of Science and Technology in 2008. His research interests include multimedia security, data hiding, and digital watermarking.

Report of Leading SIG activities

TC OFFICERS AND NEWSLETTER EDITORS

TC Officers

Names	Affiliation	Email
Joel Rodrigues	Institute of Telecommunications, University of Beira Interior	joeljr@ieee.org
Lynda Mokdad	University of Paris-Est, Créteil	lynda.mokdad@u-pec.fr
Hacene Fouchal	University of Reims Champagne-Ardenne, Reims	hacene.fouchal@univ-reims.fr

Editor-In-Chief

Names	Affiliation	Email
Lynda Mokdad	University of Paris-Est, Créteil	Lynda.mokdad@u-pec.fr
Lei Shu	Guangdong University of Petrochemical Technology, China	lei.shu@lab.gdupt.edu.cn

Co-Editors

Names	Affiliation	Email