WiFace: A Secure GeoSocial Networking System Using Wi–Fi Based Multihop MANET

Lan Zhang[1], *Xuan Ding*[1], *Zhiguo Wan*[1], *Ming Gu*[1], *and Xiangyang Li*[2]
(1. Key Laboratory of Information System Security, Tsinghua University;
2. Department of Computer Science, Illinois Institute of Technology)

Abstract: A number of mobile Online Social Networking (OSN) services have appeared in the market in recent times. While most mobile systems benefit greatly from cloud services, centralized servers and communications infrastructure is not always available. Nor are location–based services offered to mobile devices without GPS. To take advantage of cloud and to address these problems, a Wi–Fi based multihop networking system called MoNet is proposed. On top of MoNET we propose a privacy–aware geosocial networking service called WiFace. Where there is no infrastructure, a distributed content sharing protocol significantly shortens the relay path, reduces conflicts, and improves data availability. Furthermore, a security mechanism is developed to protect privacy. Comprehensive experiments performed on MoNet show that the system is more than sufficient to support social networking and even audio and video applications.

Keywords: Wi–Fi; social network; privacy; MANET; WiFace

I Introduction

At the end of 2010, the number of mobile devices worldwide was about 5 billion. In conjunction with an Internet marketing company, we conducted a survey involving 215 respondents. The sample included people from a variety of professions with a wide range of educational backgrounds. 52% of respondents already had Wi–Fi interface, and 87% of the remainder had intentions of using a Wi–Fi enabled phone.

This work is supported by National Natural Science Foundation of China under Grant No. 90818021, and 9071803.

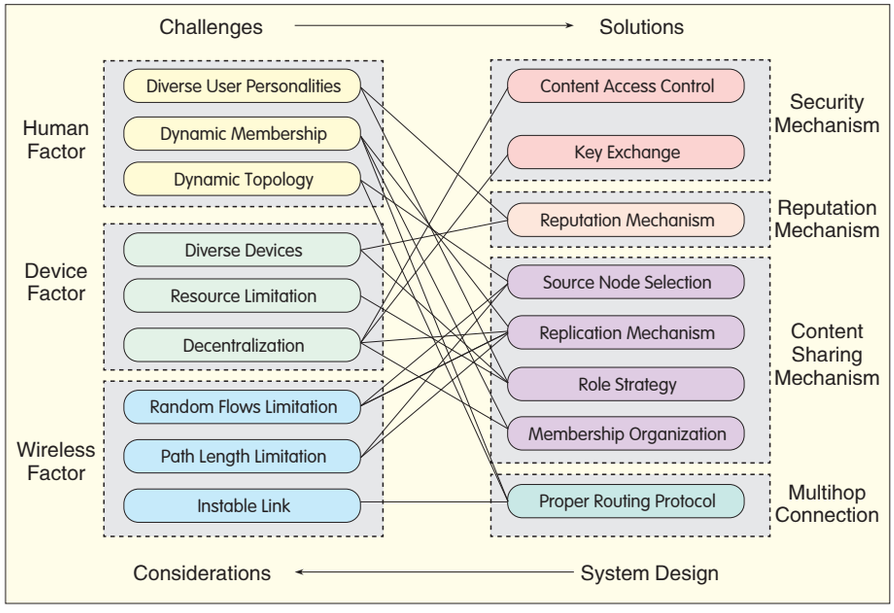
The work of Li is supported by Tsinghua National Laboratory for Information Science and Technology(TNList), NSF CNS0832120, National Natural Science Foundation of China under Grant No. 60828003, National Basic Research Program of China ("973" Program) under grant No. 2010CB328100, and the National High Technology Research and Development Program of China ("863" Program) under grant No. 2007AA01Z180.

According to Schelling [1], [2], people who share mutual interests like to communicate and collaborate, and similar people tend to gather at the same places. Both our survey and [3] show that people in the same location tend to communicate and share information about their surroundings via mobile devices. Because these applications involve social relationships and sharing private information, 99% of respondents thought that privacy protection is necessary. In this paper, we focus on geographically co–located social networks, also called "geosocial" networks.

More and more Online Social Networking (OSN) sites are available on mobile phones. Typically, OSNs rely on centralized servers and the Internet, or on cellular networking access. This implies cost to end–users and access may not always be available for all users. Location techniques and devices are also required for these OSNs; and even with GPS, devices may still have problems with indoor use.

To meet application demands and address these problems, a secure geosocial networking system called WiFace is proposed. WiFace works when only some users have access to the cloud component, and it can also operate without any networking infrastructure or GPS module. In this paper, we address the problem of unavailable infrastructure for some or even all users. Multihop Mobile Ad hoc Network (MANET) [4] may be the best choice of network structure because it can be constructed easily using widely available mobile devices. Limited multihop coverage implies that end users are co–located. However, for many reasons, MANET is not practical for social networking applications without servers. Fig. 1 shows challenges on the left with solutions provided by WiFace on the right. These challenges include:

(1) Finding a suitable routing protocol: Due to dynamic topology and



▲Figure 1. Challenges to design and implement a mobile geosocial networking system based on MANET (on the left), and our system solutions (on the right).

unstable link quality, it is difficult but crucial to find a suitable routing protocol that has been evaluated in real–life mobile scenarios.

(2) Limited capacity of MANET: Throughput and delay significantly decrease the number of hops in a MANET path [5], [6]. Gupta and Kumar [7] have shown that the asymptotic per–flow unicast capacity with n random flows of n nodes inside a unit square is $\theta(W/\sqrt{n \log n})$. These limitations require a carefully designed content sharing mechanism to shorten path length and reduce conflicts.

(3) Diverse devices and limited resources: Ordinary mobile devices usually have limited disk space, network bandwidth, and power. The condition of devices may also differ greatly. Thus full advantage must be made of resource–filled clouds and cooperation must be improved by role strategies.

(4) Dynamic membership and decentralization: Without a server or trusted third party, fast–changing membership and decentralization brings about great difficulty in managing membership, keeping content available, confirming identity, and authorizing access.

In the face of these challenges, we have designed and implemented a geosocial networking system consisting of a Wi–Fi based multihop network platform for personal mobile devices (called MoNet) and a distributed geosocial networking application with a security mechanism (called WiFace). This geosocial networking system works efficiently indoors and outdoors, with or without infrastructure or GPS module. The system was deployed in Tsinghua University for use by more than one hundred people, and comprehensive field experiments were conducted to evaluate its performance. The results show that MoNet can sufficiently support geosocial networking applications and even audio and video applications.

2 Application Description

As well as MoNet, two other applications were designed and implemented: WiFace and WiMarket. In this paper, WiFace is discussed in detail.

WiFace is a co–located social networking application with a security mechanism. It supports common social networking activities such as status updating, blogging, adding friends, and chatting. It also allows sharing of photos, videos, and documents and offers special co–located services. Take a mall for example. Stores can broadcast electronic product advertisements, hot sales, and discounts to customers in or around the mall. Customers can request or filter promotional information about a certain category of product or search surrounding stores. Interestingly, customers could also source others who wish to make a group purchase and perhaps get a better price. WiFace could also be used in a train, an international conference, an exhibition, or on a spring outing.

WiMarket is an online fleamarket application implemented on MoNet. One hundred and six heterogeneous mobile nodes including mobile phones and laptops were deployed in a 1200 m × 800 m area on campus. Experiments carried out on WiMarket are detailed in Section 4 of this paper.

Results show that MoNet has reasonably good network performance; thus, more audio and video applications can be implemented. MoNet can also be easily deployed and expanded greatly via the Internet and can be used as the basic network structure for wired range mobile communications—such as making a free transpacific call by mobile phone.

3 Architecture and Design

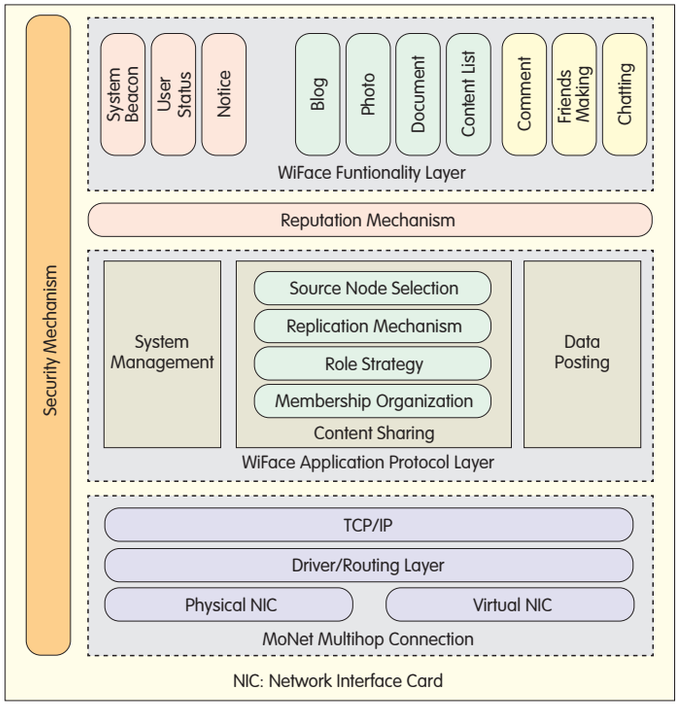
As illustrated in Fig. 2, the WiFace system consists of MoNet network platform and WiFace application built on top.

3.1 Network Formulation

The MoNet platform is based on a TCP/IP Reference Model and contains two primary layers:

(1) A Physical and Virtual Network Interface Card (NIC) Layer corresponding to the physical and data link layers. The virtual NIC is designed to support multihop communication as an additional network link without affecting other physical NICs.

(2) A Driver/Routing Layer located between the link and network layers that serves as a standard interface for them. This layer is the core of the



◀Figure 2. WiFace application structure.

MoNet platform. After MoNet has been installed, a virtual NIC is generated with a 48 bit virtual Ethernet address. Using the 48 bit virtual address for routing, the multihop routing protocol deals with frames from all network interfaces and sends them via the corresponding physical interface to the routing result. So the scope of MoNet can be expanded through physical links such as Internet, Bluetooth, and sensor. Mobile devices of MoNet can access the cloud as long as any one of them can connect to the servers.

3.1.1 Routing Protocol

Numerous routing protocols for MANET have been proposed and well studied. These include Ad hoc On-Demand Distance Vector (AODV) [8] and Dynamic Source Routing (DSR) [9]. A combination of link-state and DSR-style on demand querying was inspired by Mesh Connectivity Layer (MCL) [10]. However, most evaluations of these routing protocols are based on stationary nodes and simulations. To find a suitable routing protocol for MoNet, real mobile devices need to be evaluated and experiments carried out in typical scenarios. Performance is tested based on different link metrics—such as HOP, Round Trip Time (RTT), Expected Transmission Count (ETX) [11], and Weighted Cumulative Expected Transmission Time (WCETT) [12]. Since the per-hop RTT metric performs poorly due to self-interference [10], DSR is applied with three link quality metrics: HOP, ETX, and WCETT.

(1) Indoors

The main cause for reduced network capacity is collisions. Fig. 3 and Table 1 show indoor test results and, in this case, HOP performs the best. ETX performs almost the same as HOP but causes more probe overheads to the network and the metric calculation. Performance in an indoor mobile scenario was also evaluated. In this case, a sender carrying a mobile phone walks along a corridor to a receiver in the meeting hall at a speed of 1 m/s. Three other nodes are evenly placed along the corridor. Fig. 3 shows the maximum throughput of the TCP transfer between the sender and receiver during the 1 minute walk. The throughput of HOP increases by steps while ETX and WCETT have relatively smaller and more unstable throughput.

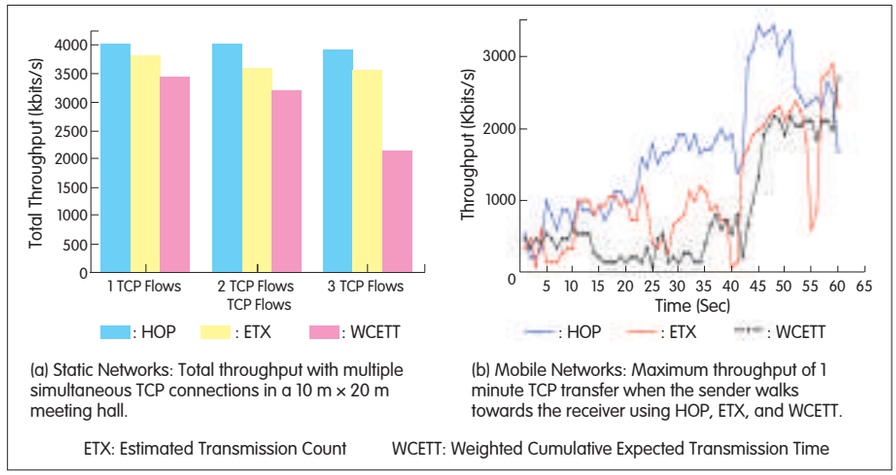
(2) Outdoors

Since users are usually moving around, node mobility is the main consideration. The test was conducted on a standard athletic field surrounded by a 400 m track. Four nodes were placed at the verteces of a square with sides 50 m located in the middle of the field. A sender and receiver on opposite sides of the track both move clockwise at the same speed of 1 m/s. The average throughput of HOP is 1.45 Mbit/s, ETX is 1.04 Mbit/s, and WCETT is only 316 kbit/s.

According to these results, the DSR protocol with HOP as the link metric is a more suitable choice for typical WiFace application.

3.1.2 Network Scope Expansion

The design of MoNet enables all mobile devices to access the cloud if any one of them has a connection with



(a) Static Networks: Total throughput with multiple simultaneous TCP connections in a 10 m × 20 m meeting hall.

(b) Mobile Networks: Maximum throughput of 1 minute TCP transfer when the sender walks towards the receiver using HOP, ETX, and WCETT.

ETX: Estimated Transmission Count WCETT: Weighted Cumulative Expected Transmission Time

▲Figure 3. Indoor test results based on different link metrics.

▼Table 1. Average path length and route change frequency with multiple 100 seconds simultaneous TCP connections in a 10 m × 20 m meeting hall

	Average Path Length (Hop)			Route Change Frequency (Time)		
	HOP	ETX	WCETT	HOP	ETX	WCETT
1 TCP Flow	1	1	1.46	0	0	2
2 TCP Flows	1.01	1.08	1.16	2	3	5.5
3 TCP Flows	1	1.14	1.64	2	2.25	22.5

ETX: Estimated Transmission Count WCETT: Weighted Cumulative Expected Transmission Time

the server. It also enables the scope of MoNet to be expanded through other physical links. Since most mobile devices do not have a globally unique IP address, a wired VPN can connect MoNets in different locations to greatly increase the scope (Fig. 4). In this way, the design and implementation of MoNet does not need to be modified, and no equipment is required other than an Internet computer with a globally unique IP address as the VPN server. This brings high expansibility to MoNet.

3.2 Application Design

The WiFace application layer is based on the connection of MoNet. System management, content sharing protocol, and data posting protocol are implemented to support respective upper layer functionalities (Fig. 2). Efficient lightweight security mechanisms across all layers are designed to protect user privacy.

3.2.1 Content Sharing Protocol

For mobile devices that cannot access the cloud, effective content sharing is crucial and challenging in a mobile geosocial networking system. This is due to highly dynamic topology and decentralization. Although systems like Gnutella [13] and FreeHaven [14] are purely decentralized, they are proposed for the Internet. In MANET, performance depends strongly on the path hop number. Recently, BitTorrent-like systems such as BitHoc [15] and BlueTorrent [16] have been adaped to wireless ad hoc networks. But they can suffer from single point failure of the initial seed, and the peer overlay is constructed on demand so that multihop capacity limitation and node mobility are not taken into consideration. Some algorithms of these systems are sophisticated but too complex for mobile devices with limited resources.

In WiFace, an active cooperative content sharing protocol is designed for mobile devices. To address the challenges in Section 1, this protocol takes advantage of short paths, resource-full devices (including servers when the cloud is accessible), and node mobility to offer efficient content sharing and good availability. By listening to other broadcast messages, every node maintains a member list (that records the behavior of all the other nodes) and a whole network content list. Queries are based on TTL limited flood, and a source node with a replica is chosen according to its distance and role level.

(1) Role Strategy and Reputation: A novel role strategy is proposed to improve cooperation among diverse devices by giving them different role levels. A node with more resources has a higher role level and automatically replicates more content items. When the cloud is accessible, a server holds the highest role level and replicates all content. The node with shorter hop path and higher role level is prioritized as the source node. To prevent a node from changing its role level, a reputation value is calculated based on its behavior recorded in other members' lists. A WiFace user spends his reputation points as currency on some functionalities and location-based services.

(2) Replication Mechanism: To keep content available in decentralized dynamic membership, a content item is not only stored by the creator but may also be replicated automatically by nodes with a role level greater than zero.

Both theoretical analysis and experiments show that the content sharing protocol can significantly decrease retrieval path length and prolong the content persistence time. Details about the content sharing protocol can be found in [17].

3.2.2 Security Mechanism

According to our survey, about half the respondents were worried about eavesdropping on private communications and/or content exposure to unauthorized people. In WiFace, different types of keys are used to protect private content and control content access.

(1) Friend Key Exchange: In WiFace, a pair of friends exchange a confidential symmetric key to form a secure channel for private communication and content sharing. Considering the limited computational capability of mobile devices, a lightweight scheme was designed

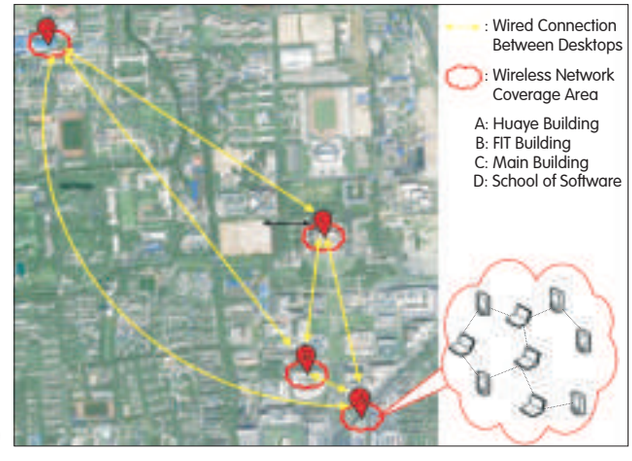


Figure 4. MoNet experiment network topology with wired network connection. (Here, 106 nodes in 4 different buildings in Tsinghua university are connected using MoNet.)

▼Table 2. Maximum throughput and loss rate change with distance between two nodes

Distance	1 m	5 m	15 m
Throughput (Kbit/s)	4800	4680	2225
Loss Rate (%)	0.5	1.4	6.13
Distance (m)	30	40	45
Throughput (Kbit/s)	612	431	103
Loss Rate (%)	8.17	9.67	71.33

▼Table 3. Broadcast arrival rate

Node Number	10	20	50
Arrival Rate	99.8%	99.5%	96.9%

▼Table 4. Multihop maximum throughput and RTT

	1-Hop	2-Hop	3-Hop	4-Hop
Max Throughput (Kbit/s)	4318	2048	1142	323
RTT (ms)	18	49	105	340

RTT: Round Trip Time

based on shared knowledge. It combines two-party Elliptic Curve Diffie-Hellman (ECDH) [18],[19] and interlock protocol [20] to construct a friend key without a trusted authority. This can prevent Man-in-the-Middle (MITM) attacks to a certain extent.

The protocol for establishing keys between two individuals, Alice and Bob, works as follows:

- Alice sends a friend request message to Bob.
- Bob knows Alice in real life and receives the request. Bob then sends back an OK message to Alice; otherwise, he rejects the request (maybe sending a NO message).
- Alice and Bob generate the same confidential key k through ECDH. They formulate and send a friend challenge question to each other based on their shared private knowledge, which only the other should be able to answer.
- Alice encrypts her correct answer R_a with k and sends the first encrypted half to Bob. Bob waits to receive the first half of encrypted R_a then sends the first half of his encrypted answer R_b encrypted with k to Alice.
- Alice sends the other half to Bob until she receives Bob's first half.
- Bob decrypts the whole R_a and checks. If it is correct, he sends the other half of encrypted R_b to Alice, or else the exchange fails. Alice decrypts the whole R_b and checks. If it is correct, she sends an ACK, or else the exchange fails.

Only when they complete the whole protocol can they determine that the channel is secure. Then they bind the friend key k to each other's identity and communicate privately under the protection of k. If any step fails, the channel may have been compromised by an attacker.

(2) Content Access Control: After completing the process of making friends, each pair of friends shares a confidential 128 bit friend key, and every user has a friend key list. If a user wants to create friends-only content, a key is generated to encrypt the content and then the content key is encrypted and attached with the keys of authorized friends. In this way, the distributed authorization mechanism can be used to control content access efficiently.

4 Experiments and Evaluation

4.1 MoNet Performances

MoNet was evaluated based on 802.11b, which is supported by most mobile phone wireless interfaces.

(1) One-hop throughput and loss rates: Table 2 lists maximum throughput for one hop and loss rates according to the distance between two PDAs on a playground. The one-hop transmission range of PDAs is about 40 m.

Broadcast arrival rate: In this test, every node in a 10 m × 20 m room broadcasted 1 kb messages every second for 1000 seconds. Table 3 shows the broadcast arrival rate with different numbers of broadcasting nodes. The stable arrival rate means that system beacons and notices in WiFace are effective.

(2) Multihop performance: To test the multihop performance of MoNet, PDAs were arranged in a chain topology. As shown in Table 4, throughput decreases and latency increases significantly as path length increases.

Multiple simultaneous TCP connections: The total throughput of multiple simultaneous TCP connections was tested in a 10 m × 20 m meeting hall with 10 nodes, and the result is shown in Fig. 3. Even if there are 3 concurrent TCP flows in such a small area, the total throughput is about 4 Mbit/s with more than 1 Mbit/s for each connection. This shows that MoNet is capable of data stream applications like visual communication or video sharing.

4.2 Content Sharing Protocol of WiFace

This content sharing protocol was evaluated in two typical scenarios.

In scenario 1, there were 20 users in a playground. Three users published blogs at random times and the others read them randomly. This scenario shows that the content protocol can shorten the average path length from 3.1 hops to 2.3 hops without role strategy, saving 25% bandwidth and extra energy consumption. Furthermore, with role strategy the protocol can shorten the average path length from 2.9 hops to 0.7 hops, and even result in 0 hop path (requesting content from one's own replicas). This obviously enhances user experience.

In scenario 2, only one source node was used to publish a blog in the beginning. The result demonstrates that the content sharing protocol can significantly improve content persistence and availability in the

changing population.

4.3 Real Usage Results

The WiMarket application on top of MoNet was also implemented, and real usage of MoNet was evaluated. Fig. 4 shows the experimental scenario; 106 heterogeneous mobile nodes were deployed in four buildings in Tsinghua University for the purposes of online trading. Four co–located MoNets in different buildings were connected by wired VPN connections. The average maximum throughput of a 3 hop path with a wired link between two nodes in different buildings is about 3.8 M. Eighty three trades were successfully completed within a 3 hour period.

5 Related Work

MoNet is a novel geosocial networking system that works efficiently with or without central servers or Internet access. It is also a wireless ad hoc network that is different from others. There have already been numerous attempts to address the problems of wireless ad hoc networks. These have contributed greatly to wireless ad hoc network research; however, most of them are indoor testbeds and not systems used in real life. This means they cannot be deployed on ordinary mobile phones and have less consideration of node mobility. There is still a lack of implementation and evaluation of wireless ad hoc networks for real use mobile devices. MoNet is a large–scale MANET composed of ordinary personal mobile devices and can be easily deployed indoors or outdoors to support real use applications. These experiments on MoNet can provide a new perspective on MANET.

6 Conclusions

In this paper, a secure geographical social networking system based on multihop MANET is discussed. Compared with existing social networking systems, this system can be easily constructed and can operate efficiently without relying on a central server or Internet access. Furthermore, it offers location–based services to low end mobile phones indoors or outdoors without the need for GPS modules. A distributed content sharing protocol with a role strategy and lightweight security mechanism deal with the challenges posed by a wireless connection, device constraints, and user behaviors. Privacy is also protected. The system was deployed in Tsinghua University and comprehensively evaluated. Results show that with a proper system architecture and well–designed protocols, social networking over MANET is feasible, and MoNet is even sufficient for audio and video applications.

References

[1] T. Schelling, "Models of segregation," *American Economic Review*, vol. 59, no. 2, pp. 488–493, May, 1969.
[2] T. Schelling, "Dynamic models of segregation," *Journal of Mathematical Sociology*, vol. 1, no.2, pp. 143–186, 1971.
[3] M. Matuszewski, N. Beijar, J. Lehtinen, and T. Hyyrylainen, "Understanding attitudes towards mobile peer–to–peer content sharing services," in *PORTABLE'07*, Orlando, FL, pp. 1–5.
[4] Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations, IETF network working group RFC 2501, 1999.
[5] J. Li, C. Blake, D. De Couto, H. Lee, and R. Morris, "Capacity of ad hoc wireless networks," in *ACM MobiHoc 2001*, Long Beach, CA, pp. 61–69.
[6] X. Li, "Multicast capacity of wireless ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 3, pp. 950–961, Jun. 2008.
[7] P. Gupta and P. Kumar, "The capacity of wireless networks," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[8] C. Perkins and E. Royer, "Ad–hoc on–demand distance vector routing," in *WMCSA 1999*, New Orleans, LA, pp. 90–100.
[9] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, T. Imielinski and H. Korth, Eds., New York: Kulwer Academic Publishing, 1996, pp. 153–181.
[10] R. Draves, J. Padhye, and B. Zill, "Comparison of routing metrics for static multihop wireless networks," in *ACM SIGCOMM 2004*, Portland, OR, pp. 133–144.
[11] D. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high throughput path metric for multihop wireless routing," in *ACM MobiCom 2003*, San Diego, CA, pp. 134–146.
[12] R. Draves, J. Padhye, and B. Zill, "Routing in multiradio multihop wireless mesh networks," in *ACM MobiCom 2004*, Philadelphia, PA, pp. 114–128.
[13] Gnutella. [online] Available: http://gnutella.wego.com
[14] R. Dingledine, M. Freedman and D. Molnar, "The Free haven project: Distributed anonymous storage service," in *Proc. of the Workshop on Design Issues in Anonymity and Unobservability*, Berkeley, CA, 2000. pp. 67–95.
[15] A. Krifa, M. Sbai, C. Barakat, and T. Turletti, "Bithoc: A content sharing application for wireless ad hoc networks," in *PerCom 2009*, Galverston, TX, pp. 1–3.
[16] S. Jung, U. Lee, A. Chang, D. Cho, and M. Gerla, "Bluetorrent: Cooperative content sharing for bluetooth users," In *PerCom 2007*, New York, NY, pp. 47–56.
[17] L. Zhang, X. Ding, Z. WAN, M. Gu, and Xiang Y. Li, "WiFace: a secure geosocial networking system using Wi–Fi based multihop MANET," in *Proc. 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond*, San Fransisco, CA, 2010, pp. 1–8.
[18] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 388–404, Mar. 2000.
[19] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.
[20] R. Rivest and A. Shamir, "How to expose an eavesdropper," *Commun. of the ACM*, vol. 27, no. 4, pp. 393–395, 1984.

Biographies

Lan Zhang (zhanglan03@gmail.com) has a B.S. degree in computer software from Tsinghua University. She is currently a Ph.D. candidate at the Department of Computer Science and Technology, Tsinghua University. Her research interests include mobile ad hoc networks and mobile social networks.

Xuan Ding (dingx04@gmail.com) has a B.S. degree in computer software from Tsinghua University. He is currently a Ph.D. candidate at the Department of Computer Science and Technology, Tsinghua University. His research interests include mobile social networks, social network privacy and anonymity, and graph anonymity.

Dr. Xiangyang Li (xli@cs.iit.edu) is an associate professor of computer science at the Illinois Institute of Technology. He is also a visiting professor of Microsoft Research Asia from 2007 to 2008. He is recipient of China NSF Outstanding Overseas Young Researcher (B). The research of Dr. Li has been supported by USA NSF, HongKong RGC, and China NSF. His research interests span the wireless sensor networks, game theory, computational geometry, and cryptography and network security. He is a senior member of the IEEE and served various positions (as chairs and TPC members) at numerous international conferences.

Zhiguo Wan (wanzhiguo@mail.tsinghua.edu.cn) has B.S. degrees from the Departments of Automotive Engineering and School of Software, Tsinghua University. He received his Ph.D. degree in Computer Science from the National University of Singapore in 2006. From 2006 to 2008, he undertook postdoctoral work in the Computer Security and Industrial Cryptography research group, Catholic University of Louvain. He is currently a lecturer in the School of Software, Tsinghua University. His research interests include network security, security and privacy, and wireless security.

Ming Gu (guming@mail.tsinghua.edu.cn) has a B. S. degree in computer software from the National University of Defense Technology, China. She also has an M.A. degree in computer software from Graduate University of Chinese Academy of Sciences. She is currently the vice–director of the School of Software, Tsinghua University, and vice–director of Ministry of Education Key Laboratory of Information Security. Her research interests include software formal methods, trustworthy software, and middleware technology.