International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 1, No 5, 2015. ISSN: 2348-6600
Reference ID: IJCS-095 PAGE NO: 542-548.

# Privacy In Opportunistic Network For Interest-Casting In Manets

Dr. S Prabhakaran,T Senthil Kumar,
Asst. Professor, Professor
Dept. Computer Science & Engineering
SRM University
Chennai-603203.

Ojaswani Dubey
Dept. Computer Science & Engineering
SRM University
Chennai-603203.

***Abstract*— Many mobile social networking applications are based on the concept, according to which two mobile users try to jointly estimate whether they have common friends, or share same interests, etc. Performing "friend detection" in a privacy-preserving way is fundamental to achieve widespread acceptance of mobile social networking applications. What so ever, the need of privacy preservation is often at odds with application-level performance of the mobile social networking application, since only profuse information about the other user's profile is available for optimizing performance, More specifically, it is considered a mobile social networking application for opportunistic networks called interest-casting. In this model, a user wants to exchange a piece of information to other users sharing similar interests, possibly through multi-hop forwarding. It is proposed that the privacy-preserving friend proximity detection scheme based on a protocol for solving the Yao's "Millionaire's Problem", and the three interest-casting protocols achieving different tradeoff between privacy and accuracy of the information forwarding process. The privacy versus accuracy adjudge is analyzed both analytical, and through simulations based on a real-world mobility trace.**

**Keywords— Opportunistic networks; Interest-casting; Social Networking; Privacy preservation.**

## I. INTRODUCTION

Computing is any goal-oriented activity requiring, benefiting from, or creating algorithmic processes - e.g. through computers. Computing includes designing, developing and building hardware and software systems; processing, structuring, and managing various kinds of information; doing scientific research on and with computers; making computer systems behave intelligently; and creating and using communications and entertainment media. "In a general way, we can define computing to mean any goal-oriented activity requiring, benefiting from, or creating computers. Thus, computing includes designing and building hardware and software systems for a wide range of purposes; processing, structuring, and managing various kinds of information; doing scientific studies using computers; making computer systems behave intelligently; creating and using communications and entertainment media; finding and gathering information relevant to any particular purpose, and so on. The list is virtually endless, and the possibilities are vast." Computing also has other meanings that are more specific, based on the context in which the term is used. For example, an information systems specialist will view computing somewhat differently from a software engineer. Regardless of the context, doing computing well can be complicated and difficult. Because society needs people to do computing well, we must think of computing not only as a profession but also as a discipline. The term "computing" has sometimes been narrowly defined, as: The discipline of computing is the systematic study of algorithmic processes that describe and transform information: their theory, analysis, design, efficiency, implementation, and application. The fundamental

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 5, 2015. ISSN: 2348-6600
Reference ID: IJCS-095 PAGE NO: 542-548.

question underlying all computing is "What can be (efficiently) automated?"

## II. MOBILE COMPUTING

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications.

A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET. A Mobile

Adhoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the node has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Figure 1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other however the node 2 can be used to forward packets between node 1and node 2. The node 2 will act as a router and these three nodes together form an ad-hoc network.

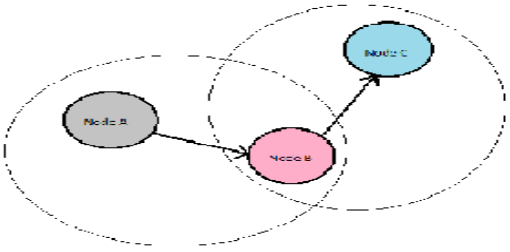

*Figure 1 Example of mobile ad-hoc network*

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has central controller information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. The P2P file sharing model makes large-scale networks a blessing instead of a curse, in which nodes share files directly with each other without a centralized server. The successful deployment of P2P file sharing systems and the aforementioned impediments to file sharing in MANETs make the P2P file sharing over MANETs (P2P MANETs in short) a promising complement to current Infrastructure model to realize pervasive file sharing for mobile users. As the mobile digital devices are carried by people that usually belong to certain social relationships, we focus on the P2P file sharing in a disconnected MANET community consisting of mobile users with social network properties. In such a file sharing system, nodes meet and exchange requests and files in the format of text and images in different interest categories.

## III. MANETS CHARACTERISTICS

### 3.1. Distributed operation

There is no background network for the central control of the network operations. The control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security

### 3.2. Multi hop routing

When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 5, 2015. ISSN: 2348-6600
Reference ID: IJCS-095 PAGE NO: 542-548.

3.3. Autonomous terminal
In MANET, each mobile node is an independent node, which could function as both a host and a router.

3.4. Dynamic topology
Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.

3.5. Light
In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

3.6. Shared Physical Medium
The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted

## IV. ADVANTAGES OF MANET

The advantages of an Ad-Hoc network include the following:

1. They provide access to information and services regardless of geographic position.
2. Independence from central network administration. Self-configuring network, nodes are also act as routers.
3. Less expensive as compared to wired network.
4. Scalable—accommodates the addition of more nodes.
5. Improved Flexibility.
6. Robust due to decentralize administration.
7. The network can be set up at any place and time.

## V. MANETS CHALLENGES

5.1. Limited Bandwidth
Wireless link continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

5.2. Dynamic Topology
Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

5.3. Routing Overhead
In wireless Adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

5.4. Hidden terminal problem
The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver

5.5. Packet losses due to transmission errors
Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, and frequent path breaks due to mobility of nodes.

5.6. Mobility-induced route changes
The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.

5.7. Battery constraints
Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

5.8. Security threats
The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

## VI. MANETS APPLICATIONS

Some of the typical applications include:

1. Military battlefield
Ad-Hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarter.

2. Collaborative work
For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

3. Local level
Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 5, 2015. ISSN: 2348-6600
Reference ID: IJCS-095 PAGE NO: 542-548.

4. Personal area network and Bluetooth

A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.

5. Commercial Sector

Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

## VII. RELATED WORKS

The increase in volume and sensitivity of data communicate and processed over the Internet has been accompanied by a corresponding need for e-commerce techniques in which entities can participate in a secure and anonymous fashion[1].Even simple arithmetic operations over a set of integers partitioned over a network require sophisticated algorithms. In this problem, each of the two participating parties has a number and the objective is to determine whose number is larger without disclosing any information about the numbers. This problem has direct applications in on-line bidding and auctions. Optimal solution for the secure multiparty computation of the 'less-or-equal' predicate exists in literature this protocol is not suited for practical applications. A comparison of two numbers can be carried out simply by examining the most significant bit in which they differ. Identical bits do not affect the result, while the effect of unequal low-order bits is overshadowed by the high-order bit. Problems of this nature are collectively known as secure multiparty computation problems. [2] Based on this principle, we can outline a protocol for securely comparing two numbers:

Alice creates two numbers for each bit of her number. One of the numbers encodes the result of the operation if this bit is the decisive one; the other is a dummy, having no effect on the outcome. The former must also cancel the effect of any other number corresponding to less significant bits, when combined with them. Bob secretly examines.

Only the numbers he is interested in and combines all the numbers he has seen to derive the result of the comparison. Of course, all the numbers must be encrypted, so that Bob does not get information about individual bits of Alice's number. Indeed, the above protocol allows Bob to build an encrypted version of the difference of the two numbers. In the final step, Bob is allowed to decrypt the sign of the difference, but nothing else. This encoding is built on pieces of information communicated from Alice, which individually or partially combined reveal, nothing to Bob, but the combination of all of them reveals the desired result. This is reminiscent of the well-known technique of secret sharing. [2]

With the proliferation of mobile devices, mobile social networks (MSNs) are becoming an inseparable part of our lives. [3]Leveraging networked portable devices such as smart phones and PDAs as platforms, MSN not only enables people to use their existing online social networks (OSNs) at anywhere and anytime, but also introduces a myriad of mobility-oriented applications, such as location-based services and augmented reality. Among them, an important service is to make new social connections/friends within physical proximity based on the matching of personal profiles. For example, MagnetU and E-Small Talker are MSN applications that match one with nearby people for dating or friend-making based on common interests. In such an application, a user only needs to input some (query) attributes in her profile, and the system would automatically find the persons around with similar profiles. The scopes of these applications are very broad, since people can input anything as they want, such as hobbies, phone contacts and places they have been to. However, such systems also raise a number of privacy concerns. The Two fully distributed privacy-preserving profile matching schemes Protocols used in [3] , one of them being a private set intersection (PSI) protocol and the other is a private cardinality of set-intersection (PCSI) protocol. However, solutions based on existing PSI schemes are far from efficient. Our system consists of N users (parties) denoted as P1, ..., PN, each possessing a portable device. We denote the initiating party (initiator) as P1. P1 launches the matching process and its goal is to find one party that best "matches" with it, from the rest of the parties P2, ..., PN which are called candidates. Each party Pi's profile consists of a set of attributes Si, which can be strings up to a certain length. P1 defines a matching query to be a subset of S1, and in the following we use S1 to denote the query set unless specified. Also, we denote $n = |S1|$ and $m = |Si|$, $i > 1$, assuming each candidate has the same set size for simplicity. Note that, we assume that the system adopts some standard way to describe every attribute, so that two attributes are exactly the same if they are the same semantically. There could be various definitions of "match". In this paper, we consider a popular similarity criterion, namely the intersection set size $|S1 \cap Si|$ (also used in [2]). The larger the intersection set size, the higher the similarity between two users' profiles. User P1 can first find out her similarity with each other users via our protocols, and then will decide whether to connect with a best matching user based on their actual common attributes. Assume devices communicate through wireless interfaces such as Bluetooth or WIFI. For simplicity, assume every participating device is in the communication range with each other. In addition, assume that a secure communication channel has been established between each pair of users. Do not assume the existence of a trusted third party during the protocol run; all parties carry out profile matching in a completely distributed way. They may cooperate with each other, i.e., when P1 runs the protocol with each Pi, a subset of the rest of parties would help them to compute their results.

Mobile phones have the potential to be useful agents for their owners by detecting and reporting situations that are of interest. Several

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 5, 2015. ISSN: 2348-6600
Reference ID: IJCS-095 PAGE NO: 542-548.

challenges emerge in the case of detecting and reporting "nice to know" situations. Being alerted of these events may not be of critical importance but may be useful if the user is not busy. For detection, the precision of sensing must be high enough to minimize annoying false notifications, despite the constraints imposed by the inaccuracy of commodity sensors and the limited battery power available on mobile phones. For reporting, the notifications cannot be too obtrusive to the user or those in the vicinity. Peripheral cues are appropriate for conveying information like proximity, but have been studied primarily in settings like offices where sensors and cueing mechanisms can be controlled. Explore these issues through the design of People Tones, a buddy proximity application for mobile phones. First contribute (1) an algorithm for detecting proximity, (2) techniques for reducing sensor noise and power consumption, and (3) a method for generating peripheral cues. Empirical measurements demonstrate the precision and recall characteristics of our proximity algorithm. A two-week study of three groups of friends using People Tones shows that our techniques were effective, enabling the study of how people respond to peripheral cues in the wild. Our qualitative findings underscore the importance of cue selection and personal control for peripheral cues. Vision for ubiquitous computing is a context-aware infrastructure that can simplify and enrich our lives by helping us with tasks that might otherwise be out of our reach. For example, location- based services such as Loops can detect the proximity of friends that are just out of sight or unnoticed [4]. Such applications can be useful for a variety of scenarios such as arranging Adhoc meetings. To date such wide-scale applications have depended on specialized phone and carrier capabilities to detect proximity, both at a real cost to the user. Moreover, the user must make a conscious effort to look at the phone to learn of friends' proximity, lessening usefulness. Realizing the ultimate vision depends on a ubiquitous mechanism for detecting such occurrences. For "nice to know" contextual information like the proximity of friends, we also need an unobtrusive mechanism for making us aware of them. To achieve true ubiquity – so that any two friends could be aware of their proximity – both must be achieved at little cost. the technologies of mobile phones and peripheral cues for the ubiquitous sensing and reporting of "nice to know" context through People Tones, an application for buddy proximity Commodity mobile phones satisfy the ubiquity criterion (and by extension the cost criterion).[5]. Moreover, mobiles possess both a number of sensors (e.g., microphone, camera, and GSM radio) and actuators (e.g., speaker and vibration motor), making phones a potentially ideal platform for ubiquitous computing. On the other hand, the sensors and actuators are of notoriously low quality, complicating precise sensing and high-fidelity actuation. Inference can be especially problematic when comparing readings between phones. For detecting proximity on phones, our algorithm compares cell towers seen by the mobile phone clients to estimate proximity. This privacy-friendly approach does not require knowledge of actual location. However, GSM's long range and random characteristics means that a phone will, for example, occasionally detect cell towers that are miles away. We filter the proximity data using a simple state machine based on a 2-bit counter [6]. The state machine also helps to conserve power by sampling more slowly when two phones are considered near or far away.

The Technique used is PROXIMITY DETECTION which works with the requirements as: there were two design requirements we felt were necessary for a buddy proximity detection algorithm. First, it should be widely deployable in many environments with many phones, doing so in a privacy-aware manner. Secondly, since buddy proximity is "nice to know" information, it is important that when cues are delivered, friends are actually near one another. If too many cues will be delivered when buddies are far away, users will stop using it. In the case of reporting when buddies are near, it is therefore important to maintain a high precision, even if this means lower recall.

1. Proximity Detection Algorithm

To run controlled tests on a few different proximity detection approaches, we collected a small sample of cell tower readings from three regions with different population densities. These were obtained by sampling cell tower information from each of 3 mobile phones, all on the same carrier. Each phone recorded two samples while positioned each location. We took samples 5 minutes apart to approximate realistic behavior where users might linger at a particular location. To eliminate potential caching effects that may occur when reading cell tower information from the phone's memory, we reset all the phones in-between samples. One phone was kept stationary while the other two were moved away from the stationary one at 0.2mi intervals. The i-mate SP3i (HTC Tornado) phones we used are capable of reporting up to 7 towers at once. In summary, we used 2 samples per phone per region, 2 phones, 7 distances, and 3 regions, resulting in 84 readings. The purpose of gathering these readings was to test different algorithms for proximity detection on a realistic set of data. In our initial experiments, we found that computing the ratio of common GSM cell towers between two readings provided the best real time proximity indicator. The intuition is that the closer two phones are, the more cell towers they will have in common. This ratio is simply the number of common towers between the two phones divided by the average number of towers seen.

2. Evaluating Cell Tower Ratio Algorithm for Proximity Detection

Evaluating our proximity ratio algorithm was less than straightforward. It was difficult to obtain a suitably large and appropriate dataset for modeling two stationary phones at a variety of locations. Ideally, we would have simultaneously recorded readings from many stationary phones all at different locations with some ground truth measurement. However this would be hard if not impossible to achieve for a large number of phones [7]. During this process, they collected cell tower data along with GPS coordinates by driving around the greater Seattle area, equipped with a laptop, 2 mobile phones per carrier and a GPS device. They sampled the phones and GPS device approximately once per second to record cell towers seen by the phones and GPS coordinates. Since two phones were used per carrier, valid comparisons could be made between cell tower readings seen by the two different phones.

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 5, 2015. ISSN: 2348-6600
Reference ID: IJCS-095 PAGE NO: 542-548.

People often seek information by asking other people even when they have access to vast reservoirs of information such as the Internet and libraries. This is because people are great sources of unique information, especially that which is location-specific, community-specific and time-specific. Social networking is effective because this type of information is often not easily available anywhere else. a wireless virtual social network which mimics the way people seek information via social networking.[8] PeopleNet is a simple, scalable and low-cost architecture for efficient information search in a distributed manner. It uses the infrastructure to propagate queries of a given type to users in specific geographic locations, called bazaars. Within each bazaar, the query is further propagated between neighboring nodes via peer-to-peer connectivity until it finds a matching query. The PeopleNet architecture can overlay easily on existing cellular infrastructure and entails minimal software installation. We identify three metrics for system performance: (i) probability of a match, (ii) time to find a match and (iii) number of matches found by a query. Here, described two simple models, called the swap and spread models, for query propagation within a bazaar. We qualitatively argue that the swap model is better with respect to the performance metrics identified and demonstrate this via simulations.

Method:

Assume that users have access to two kinds of network connectivity. Users can communicate over long distances using a fixed infrastructure such as the cellular system. Users can also communicate over short distances with nearby users using peer-to-peer interfaces such as Bluetooth. Users possess (and seek) information sought (and possessed) by other users. The PeopleNet architecture is a lightweight and scalable mechanism for such information exchange. The architecture on cellular (for long range propagation) and Bluetooth (for short range propagation) is implemented. However, PeopleNet can be overlaid on any infrastructure. A given area (say, a city) is divided into non-overlapping regions called bazaars. Each bazaar is dedicated to handle certain types of queries placed by users. As noted earlier, queries can be either requests or responses. For example, we could have a sports bazaar, an automobile bazaar, etc. Note that any user can place a query associated with any bazaar irrespective of where she is located.

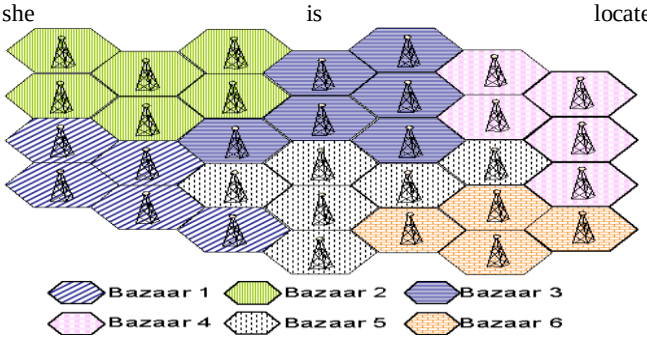


*Figure 2 Bazaar of Different Interests*

In other words, a user need not be physically located in the sports bazaar to ask a sports question. When a user places a query on her device (say a query Relating to sports), the query is propagated via the network infrastructure to k randomly selected users in the associated bazaar (sports bazaar). As these k users move around, they propagate the query to other users, who in turn further propagate the query via the peer-to-peer mode. When two matching queries are co-located on a single device, the device automatically informs the respective users about the match via the network infrastructure. For example this could be achieved by sending a text message or email message to the users who initially placed the queries. The intuition behind creating bazaars is that it speeds up the dynamics of PeopleNet.

The key idea is that it reduces the average initial distance between matching queries. Clearly, queries that start off geographically closer have a higher chance of finding each other than those that start off farther apart. This is precisely what creating bazaars do.

Wireless body sensor network (WBSN), as an emerging network paradigm in eHealthcare system aiming at providing patients with remote and continuous monitoring, has gathered great momentum from not only the governments but also the academia in our aging society[9].In our aging society, mHealthcare social network (MHSN) built upon wireless body sensor network

(WBSN) and mobile communications provides a promising platform for the seniors who have the same symptom to exchange their experiences, give mutual support and inspiration to each other, and help forwarding their health information wirelessly to a related eHealth center.

Typically, a WBSN consists of a number of medical sensor nodes accompanied by a wireless PDA communication device, where medical sensor nodes (either implantable or wearable) are equipped on a patient to periodically collect Patient Health Information (PHI) and forward them to the PDA device, then the PDA device serving as a gateway will report these PHI to the remote eHealth center. Based on this continuous PHI, medical professionals at eHealth center can remotely monitor the patient and quickly react to those life-threatening situations such as heart attacks. EHealthcare system can be divided into two categories: in-bed eHealthcare system and mobile eHealthcare (mHealthcare) system.[10]

REFERENCES

[1] An Efficient Protocol forYao'sMillionaires' Problem Ioannis Ioannidis and Ananth Grama Department of Computer Sciences, Purdue University, W. Lafayette, IN 47907.

[2] Andrew C.-C. Yao, Protocols for secure computation, Proc. 23rd IEEE Symposium on Foundations of Computer Science (FOCS), 1982, pp. 160 - 164.

[3] FindU:--- Privacy-Preserving Distributed Profile Matching in Proximity-based Mobile Social Networks Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, Ning Cao, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE.



Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 5, 2015. ISSN: 2348-6600
Reference ID: IJCS-095 PAGE NO: 542-548.

[4] People Tones: A System for the Detection and Notification of Buddy Proximity on Mobile Phones Kevin A. Li, Timothy Y. Sohn, Steven Huang, William G. Griswold Computer Science and Engineering University of California, San Diego La Jolla, CA 92093

[5] Chen, M., Sohn, T., Chmelev, D., et al. Practical Metropolitan-Scale Positioning for GSM Phones. In Proc of Ubicomp 2006.

[6] Loopt. http://www.loopt.com

[7] Chen M, Gonzalez S, Zhang Q, Li M, Leung V (2010) A 2g-rfid based e-healthcare system. IEEE Wirel CommunMag 17(1):37–43

[8] PeopleNet: Engineering A Wireless Virtual Social NetworkMehul Motani and Vikram Srinivasan Electrical & Computer Engineering National University of Singapore Pavan S. Nuggehalli Centre for Electronics Design & Technology Indian Institute of Science, Bangalore.

[9] A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network Rongxing Lu • Xiaodong Lin • Xiaohui Liang • Xuemin Shen

[10] Wang H, Peng D, Wang W, Sharif H, Chen HH, Khoynezhad A(2010) Resource-aware secure ECG healthcare monitoring through body sensor networks.