International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 5, May - 2013

Wireless Mobile Health Care Service Using Body Sensors

B Victor Prem Sagar,
[II-M.Tech]-CSE,DrKVSRIT Kurnool,

K Kishore,
Asst.Prof in CSE Dep., DrKVSRIT Kurnool,

Abstract

Wireless sensor networks are moving from academia to real world scenarios. This will involve, in the near future the design and production of hardware platforms characterized by low-cost and small form factor. As a consequence the amount of resources available on a single node, i.e. computing power, storage, and energy, will be even more constrained than today. This paper faces the problem of storing and executing an application that exceeds the memory resources available on a single node. The proposed solution is based on the idea of partitioning the application code into a number of opportunistically cooperating modules each node contributes to the execution of the original application by running a subset of the application tasks and providing service to the neighboring nodes.

In this paper, we study the network LifetimeMaximization problem in Mobile healthcare sensor systems (LMM). For the healthcare system, we consider a dynamic scenario where users are mobile at their own wills and periodically report their personal health information (PHI) to a static sink, e.g. a powerful server, for further processing and distributing. The objective is to optimize the network lifetime by flow scheduling. The major difficulty lies in the time-dependent.

With network topologies. The pervasiveness of smart phones and the advance of wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently. However, the flourish of m-Healthcare still faces many challenges including information securityand privacy preservation. In this paper, we propose a secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency. With SPOC, smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure.

1. Introduction

In our aging society, Aging becomes a global trend and poses a major threat to healthcare/social service systems, especially in Japan. Theaging of Japan outweighs all nations with the highest proportion of elderly citizens. According to official reports from the Japanese government elderly population (aged 65 or older) of Japan is expected to increase from 20% (2006) to 40% by 2055. This phenomenon has already raised severeproblems that are related to issues like age-related disabilities, diseases and therefore caused heavy burden on healthcare service systems. To meet this challenge, recently wireless healthcare systemshave been exploited with the objective of providing variousreliable and real-time healthcare services to people in the daily life. In such systems, a number of small body sensorsattached to the human body keeps monitoring each mobile medical user's Personal Health Information (PHI), which should be delivered through single-hop or multi-hop wireless communication to the base station for further processing and distributing. Mobile Healthcare (m Healthcare) system has been envisioned as an important application of pervasive computing to improve health care quality and save lives, whereminiaturized wearable and implantable body sensor nodes and smartphones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease specifically, in an m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments. Instead, after being equipped with smartphone and wireless body sensor network (BSN) formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere. For example, as shown in Fig. 1, each mobile medical user's personal health information (PHI).

Such as heart beat, blood sugar level, blood pressure and temperature and others, can be first collected by BSN, and then aggregated by smart phone via Bluetooth. Finally, they are further transmitted to the remote healthcare center via 3G networks. Based on these collected PHI data, medical professionals at healthcare center can continuously monitor medical users' health conditions and as well quickly react to users' life-threatening situations and save their lives by dispatching ambulance and medical personnel to an emergencylocation in a timely fashion.

Although m-Healthcare system can benefit medical users by providing high-quality pervasive healthcare monitoring, the flourish of m-Healthcare system still hinges upon how we fully understand and manage the challenges facing in m- Healthcare system, especially during a medical emergency. Toclearlyillustrate the challenges in m-Healthcareemergency, we consider the following scenario.

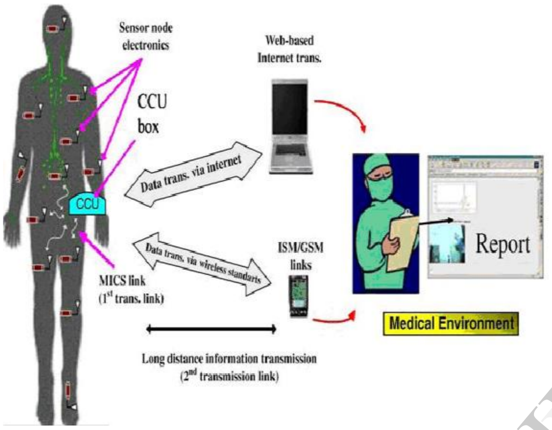


Fig 2: Pervasive health monitoring in m-Health care system

In general, a medical user's PHI should be reported to the healthcare center every 5 minutes for normal remote monitoring. However, when he has an emergency medical condition, for example, heart attack, his BSN becomes busy reading a variety of medical measures, such as heart rate, blood pressure, and as a result, a large amount of PHI data will be generated in a very short periodof time, and they further should be reported every 10 seconds for high-intensive monitoring before ambulance and medical personnel's arrival. However, since smartphone is not only used for healthcare monitoring, but also for other applications, i.e., phoning with friends, the smart phone's energy could be insufficient when an emergency takes place. Although this kind of unexpected event may happen with very low probability, i.e., 0.005, for a medical emergency, when we take into 10, 000emergency cases into consideration, the average event number will reach 50, which is not negligible and explicitly indicatesthe reliability of m-Healthcare system is still challenging in emergency. Recently, opportunistic computing, as a new pervasive computing paradigm, has received much attention Essentially, opportunistic computing is characterized by exploiting all available computing resources in an opportunistic environment to provide a platform for the distributed execution of a computing-intensive task.

In this paper, we propose a new secure and privacy preserving opportunistic computing framework, called SPOC, to address this challenge. With the proposed SPOC framework, each medical user in emergency can achieve the user-centric privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the high-reliability of PHI process and minimizing PHI privacy disclosure in m-Healthcare emergency. Specifically, the main contributions of this paper are threefold.

First, we propose SPOC, a secure and privacy-preservingopportunistic computing framework for m-Healthcare emergency. With SPOC, the resources available on other opportunistically contacted medical users' smartphones can be gathered together to deal with the computing intensive PHI process in emergency situation. Since thePHI will be disclosed during the process in opportunisticcomputing, to minimize the PHI privacy disclosure,SPOC introduces a user-centric two-phase privacy access control to only allow those medical users who have similarsymptoms to participate in opportunistic computing.

Second, to achieve user-centric privacy access control inopportunistic computing, we present an efficient attribute based access control and a novel non-homomorphic encryptionbased privacy-preserving scalar product computation(PPSPC) protocol, where the attributed-based access control can help a medical user in emergency toidentify other medical users, and PPSPC protocol can further control only those medical users who have similarsymptoms to participate in the opportunistic computingwhile without directly revealing users' symptoms. Notethat, although PPSPC protocols have been well studied in privacy-preserving data mining yet most of them are relying on time-consuminghomomorphicencryption technique. To the best of our knowledge, our novel non-homomorphic encryptionbased PPSPC protocol is the most efficient one in terms of computational and communication overheads.

Third, to validate the effectiveness of the proposed SPOCframework in m-Healthcare emergency, we also developed custom simulator built in Java. Extensive simulationresults show that the proposed SPOC framework canhelp medical users to balance the high-reliability of PHIprocess and minimizing the PHI privacy disclosure in m-Healthcare emergency.The remainder of this paper is organized as follows. In Section 2, we formalize the system model and security model, and identify our design goal.

2. SYSTEM MODELS

2.1System Architecture of M2M Communications for Healthcare

As in the general architecture of [1], we show the system architecture of M2M communication for healthcare in Fig. 1. Cellular type wireless systems such as 3rdgeneration partnership project (3GPP) long-term evolution(LTE) or LTE-advanced, and the Internet (i.e., cloudcomputing), serve as the M2M communication infrastructurefor healthcare. The medical center can collectrelated information from the networked cloud andinstruct machines in the reverse direction, as a bi-directionalcommunication network. In Fig. 1, the curve dotlines represent links of a cellular type system and thesolid black lines represent Internet access links as a partof a cloud. 3GPP currently is making a serious effort formachine-type communication (MTC) [2], and healthcareis one of the major applications.The remaining part of the system architecture relates tocommunication and networking from machines/sensorsto data aggregator. It is usually referred as the local networkin M2M communications. Sometimes, such communicationis known as communication for the “swarm”in cyber physical systems, which suggests a huge numberof machines in the system. This scenario, although itlooks simple, is actually very challenging as there may betrillions devices in this scenario, migrating from billionsof devices for wireless personal communications in pastdecades. Since the frequency bands lower than a fewGHz enjoy nice radio propagation and cost-effectivesemiconductor fabrication, such frequency bands arevery much preferred by M2M communications, particularlyfor healthcare. In addition to current wireless personalcommunications operating in this frequency range,the very limited available spectrum has to support a goodportion of these trillions devices. Spectrum efficient communicationand networking technologies are vital, whileenergy efficiency has to be satisfied as most machinessensors are operating by battery. In addition to the criticalspectrum efficiency and energy efficiency problems, M2Mcommunications faces the following technology challenges:

Large and dense networks: There should be trillionsdevices in M2M, a big jump from the billions devicesof today’s wireless personal communications. Consequently,the limiting behaviours of large and/or densewireless networks plays an important role, especiallyif there is a limited amount of available spectrum.

2.2Myths in M2M Communications for Healthcare

Typical M2M communications or sensor networks assume the following: 1) the networking nodes (i.e., machines or sensors) do not move, 2) the traffic volume of M2M communications for each purpose is low, with a small duty cycle.However, these assumptions do not hold in healthcareapplication scenarios. Fig. 1 depicts the M2M networkingstructure for healthcare. We can note the special featuresof M2M for healthcare, in terms of network topology.Since many sensors are installed according to the humanbody, the locations of these sensors/machines can actuallymove, due to human movement. In other words,locations of sensors relative to the data aggregator (DA)may vary, while the data aggregator may also move according to human movement. Consequently, the machinesare not static at all, which is similar to networking amongrobots. This is exactly like mobile networks. The immediatequestion to our minds would be “what does thechannel model look like?” as this heavily impacts networktopology and thus system/network design. The 400MHz, 600 MHz, 900 MHz, and 2.4 GHz channels werestudied by attaching sensors to different parts of the bodyand it was found that by simply modifying some parametersof the popular log-normal channel model in mobilecommunications we still apply this model in such a scenario.

If suchhealthcare applies to a good portion of population, we arefacing a bandwidth hungry situation in communicationsand networks.After understanding the truth behind these commonmyths, to develop solutions to the above-mentioned challengesin terms of spectrum-efficient and energy-efficientautonomous reconfigurable connectivity supporting density,mobility, configurability, will allow us to supply theM2M local network enabling healthcare applications andservices.

2.3Spectrum Sharing and Interference

To serve multiple communication scopes, such as differentranges and different data rates, adopting heterogeneouswireless networks, even in the same frequencyband is common in M2M communications forhealthcare. This introduces a new challenge toautonomously control the configurability of the local network.Please also recall that earlier heterogeneity furtherinduces another communication challenges: spectrum sharingamong heterogeneous wireless networks.

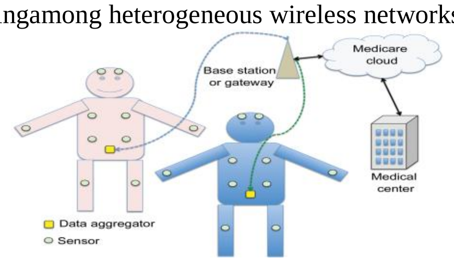


Fig. 2. System architecture of machine-to-machine communications for healthcare.

In case there exists a wireless network that has priorityto use the spectrum (say, a H2H system) in spectrumsharing wireless networks, we call that network the primarysystem (PS). The nodes of other wireless networkscan dynamically access the spectrum only if there existstransmission opportunities (i.e., nodes in the PS are not intransmission) as secondary users of the spectrum. We callsuch secondary nodes cognitive radios (CRs), which is a popular research subject to achieve spectrumefficiency nowadays

3. SECURITY ISSUES ANDCHALLENGES

Opportunistic computing can enhance the reliability for high intensive PHI process and transmission in m-Healthcare emergency. However, since PHI is very sensitive, a medical user, even in emergency, will not expect to disclose his PHI to all passing-by medical users. Instead, he may only disclose his PHI to those medical users who have some similar symptoms with him. In this case, the emergency situation can be handled by opportunistic computing with minimal privacy disclosure. Specifically, in our security model, we essentially define two-phase privacy access control in opportunistic computing, which are required for achieving high-reliable PHI process and transmission in m-Healthcare emergency.

Phase-I access control: Phase-I access control indicates thatalthough a passing-by person has a smart phone with enoughpower, as a non-medical user, he is not welcomed to participatein opportunistic computing1. Since the opportunisticcomputing requires smart phones that are installed with thesame medical software's to cooperatively process the PHI, if apassing-by person is not a medical user, the lack of necessarysoftware's does not make him as an ideal helper. Therefore,the phase-I privacy access control is prerequisite.

Phase-II access control: Phase-II access control only allowsthose medical users who have some similar symptoms toparticipate in the opportunistic computing. The reason is thatthose medical users, due to with the similar symptoms, arekind of skilled to process the same type PHI. Note that,the threshold th is a user self-control parameter. When theemergency takes place at a location with high traffic, thethreshold th will be set high to minimize the privacy disclosure.However, if the location has low traffic, the thresholdth should be low so that the high-reliable PHI process andtransmission can be first guaranteed.

4. PROPOSED SPOC FRAMEWORK

In this section, we propose our SPOC framework, which consists of three parts: system initialization, user-centric privacy access control for m-Healthcare emergency, and analysis of opportunistic computing in m-Healthcare emergency. Before describing them, we first review the bilinear pairing technique which serves as the basis of the proposed SPOC framework.

4.1 Bilinear Pairings

Let G, G^Tbe two multiplicative cyclic groups with the sameprime order q.Suppose G and $G^T$are equipped with a pairing,i.e., a non-degenerated and efficiently computable bilinear map$e$: G $\times$G $\rightarrow G^T$such that $e(g^a1, g^b2) = e(g1, g2)^{ab} \in G^T$for all$a$, $b \in Z*q$ and any $g1$, $g2 \in$G. In group G, the ComputationalDiffie-Hellman (CDH) problem is hard, i.e., given (g, g a, gb)for $g \in$G and unknown a, $b \in Z*q$, it is intractable to computegab in a polynomial time. However, the Decisional Diffie-Hellman (DDH) problem is easy, i.e., given (g, g^a, g^b, g^c)for g ∈ G and unknown a, b, c ∈ Z^*_q, it is easy to judge whether c = ab mod q by checking $e(g^a,g^b)?=e(g^c,g)$. We refer to for a more comprehensive description of pairing technique, and complexity assumptions.

Definition 1: A bilinear parameter generator Gen is a probabilistic algorithm that takes a security parameter κ as input, and outputs a 5-tuple (q, g,G,G^T , e), where q is a κ-bit prime number, G,G^T are two groups with order q, g ∈ G is a generator, and e : G × G → G^T is a non-degenerated and efficiently computable bilinear map.

4.2 Description of SPOC

4.2.1 System Initialization

For a single-authority m-Healthcare system under consideration, we assume a trusted authority (TA) located at the healthcare center will bootstrap the whole system. Specifically, given the security parameter κ, TA first generates the bilinearparameters (q, g,G,G^T, e) by running Gen(κ), and chooses a secure symmetric encryption algorithm Enc(), i.e., AES, and two secure cryptographic hash functions H and H', where H,H' : $\{0, 1\}^* \rightarrow Z^*_q$. In addition, TA chooses two random numbers (a, x) ∈ Z^*_qas the master key, two random elements (h1, h2) in G, and computes b = H(a), A = g^a, and $e(g, g)^x$. Finally, TA keeps the master (a, b, x) secretly, and publishes the system parameter params = (q, g,G,G^T , e,H,H', h1, h2,A, $e(g, g)^x$,Enc()).

Assume there are total n symptom characters considered in m-Healthcare system, and each medical user's symptoms can be represented through his personal health profile, a binary vector a'= (a1, a2,….., an) in the n-dimensional symptom character space, where a_i ∈ _a indicates a symptom character, i.e., a_i = 1 if the medical user has the corresponding symptom character, and a_i = 0 otherwise. Therefore, for each medical user U_i ∈ U, when he registers himself in the healthcare center, the medical professionals at healthcare center first make medical examination for U_i, and generate U_i's personal health profile a' = (a1, a2,…, an). Afterwards, the following steps will be performed by TA:

- Based on U_i's personal health profile a', TA first chooses the proper body sensor nodes to establish U_i's personal BSN, and installs thenecessary medical softwares in U_i's smart phone.
- Then, TA chooses two random numbers $(t_{i1},t_{i2}) \in Z^*_q$, and computes the access control key aki = $(g^{x+ati1}, g^{ti1}, g^{ti2}, h^{ti}_1\ 1\ h^{ti2}_2)$ for U_i.
- Finally, TA uses the master key b to compute the secret key $sk_i = H(U_i||b)$ for U_i.After being equipped with the personal BSN and key materials (ak_i, sk_i), U_i can securely report his PHI to healthcare center for achieving better healthcare monitoring by the following procedure.
- Ui first chooses the current date CDate, computes thesession key $k_i = H(sk_i||CDate)$ for one day, anddistributes the session key k_i to his personal BSN andsmartphone.
- Every five minutes, BSN collects the raw PHI data rPHIand reports the encrypted value Enc(ki, rPHI||CDate) tothe smart phone with bluetooth technology.
- Upon receiving Enc(ki, rPHI||CDate), the smart phone uses ki to recover rPHI from Enc(ki, rPHI||CDate).After processing rPHI, the smart phone uses the 3Gtechnology to report the processed PHI to healthcarecenter in the form of $U_i||CDate||Enc(k_i,PHI||CDate)$.

4.2.2 User-Centric Privacy Access Control for m- Healthcare Emergency

When an emergency takes place in m-Healthcare, e.g., user U0 suddenly falls down outside, the healthcare center will monitor the emergency, and immediately dispatch an ambulance and medical personnel to the emergency location. Generally, the ambulance will arrive at the scene around 20 minutes. During the 20 minutes, the medical personnel need high intensive PHI to real-time monitor U0. However, the power of U0's smart phone may be not sufficient to support the high-intensive PHI process and transmission. In this case, the opportunistic computing, as shown in Fig. 3, is launched, and the following user-centric privacy access control is performed to minimize the PHI privacy disclosure in opportunistic computing.

4.2.3 Analysis of Opportunistic Computing in m-Healthcare Emergency

Consider the ambulance will arrive at the emergency location in the time period t. To gauge the benefits brought by opportunistic computing in m-Healthcare emergency, we analyze how many qualified helpers can participate in opportunistic computing within the time period t, and how many resources can the opportunities computing provide. Assume that the arrival of users at the emergency location follows a Poisson process $\{N(t), t \geq 0\}$ having rate λ. For a given threshold th, Nq(t) = n and Nq(t) = m are respectively denoted as the number of qualified helpers and the number of non-qualified helpers within [0, t]. For any arriving user at time $\tau \in [0, t]$, the probability that the user is aqualified helper is $P(\tau)$.

5. SECURITY ANALYSIS

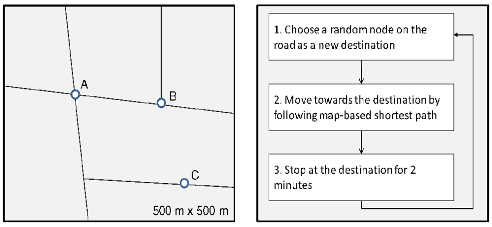
In this section, we analyze the security properties of the proposed SPOC framework. In specific, following the security requirements discussed earlier, our analyses will focus on how the proposed SPOC framework can achieve the user centric privacy access control for opportunistic computing in m-Healthcare emergency.

The proposed SPOC framework can achieve the phase-I access control. In the phase-I access control; the single attribute encryption technique is employed. Since e(g, g)xs can be recovered only by a registered medical user Uj ∈ U with his access key akj = (gx+atj1 , gtj1 , gtj2 ,htj11 htj22) from (C1 = gs,C2 = As ・ h−s1,C3=h−s2), if Uj can recover e(g, g)xs, he can be authenticated as a registered medical user. In addition, the timestamp in the returned Auth = H_(e(g, g)xs||timestamp) can also prevent the possible replaying attack. Therefore, the phase-I access control can be achieved in the proposed SPOC framework.

6. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposedSPOC framework using a custom simulator built in Java.The simulator implements the application layer under theassumptions that the communications between smart phones and the communications between BSNs and smartphones arealways workable when they are within each other's transmissionranges. The performance metrics used in the evaluationare

1. The average number of qualified helpers (NQH), whichindicates how many qualified helpers can participate in theopportunistic computing within a given time period, and
2. Theaverage resource consumption ratio (RCR), which is definedas the fraction of the resources consumed by the medical userin emergency to the total resources consumed in opportunisticcomputing for PHI process within a given time period. BothNGH and RCR can be used to examine the effectivenessof the proposed SPOC framework with user-centric privacyaccess control of opportunistic computing in m-Healthcareemergency.



(a) Simulation area (b) Mobility model

Fig 3: Simulation area and mobility model under consideration

7. SIMULATION RESULTS

In this section, we conduct simulations to verify the proposed algorithm and analysis. First, we use a sample to showthe performance gap between offline and online scenariosof the LMM problem. Then, we demonstrate that if theprediction of user mobility can be made, the performance canbe improved significantly.

In the simulations, total l users U = {U0, U1,…., Ul−1} are first uniformly deployed in an interest area of 500 m×500 m, as shown in Fig. 5(a). Each user Ui ∈ U is equipped with his personal BSN and a smartphone with a transmission radius of 20 meters, and independently moves along the road with the velocity v ∈ [0.5, 1.2]m/s in the area by following the mobility model described in Fig. 5(b). Assume that the symptom character space n = 16, each user is randomly assigned 6-8 symptom characters. Let the emergency of user U0 take place at time t = 0, he sets the threshold th as {3, 5}, and waits the qualified helpers participating in the opportunistic computing before the ambulance arrives in 20 minutes. Note that, in the simulations, we consider all users will stop when they meet U0’s emergency, and only the qualified helpers will participate in the opportunistic computing. To eliminate the influence of initial system state, a warm-up period of first 10 minutes is used. In addition, we consider U0’s emergency takes place at three locations, A, B, and C, in the map to examine how the factors l, th affect the NGH and RCR at different locations.The detailed parameter settings are summarized in Table 1.

Table 1. Simulation Settings

Parameter	Setting
Simulation area	500 m × 500 m
Simulation warm-up, duration	10 minutes, 20 minutes
Number, velocity of users	l = {40, 60}, v = 0.5 − 1.2 m/s
Similarity threshold	th = {3, 5}
Transmission of smart phone, BSN	20 m, 20 m
Raw PHI data generation interval	every 10 seconds
Emergency location	A, B, and C

7.1 Simulation Results

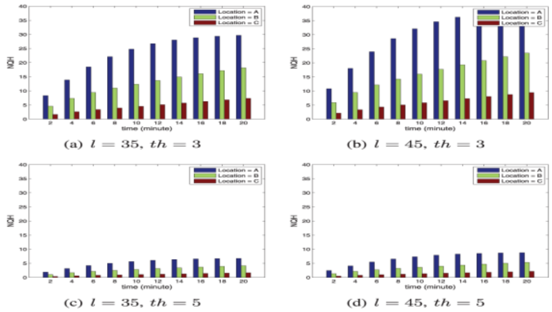


Fig 4: NQH varying with time under different l and*th*

In Fig. 6, we compare the average NQHs at locations A, B and C varying with time from 2 minutes to 20 minutesunder different user number l and threshold th. From thefigure, we can see, with the increase of time, the averageNQH will also increase, especially for the location A. Thereason is that, when all users move in the simulation areaby following the same mobility model, location A will havehigher traffic than locations B and C. In addition, when theuser number l in the simulation area increases, the user arrivalrate at locations A, B, and C also increase. Then, the averageNQH increases as well. By further observing the differencesof the average NQH under thresholds th=3 and th=5, wecan see the average NQH under th=5 is much lower thanthat under th=3, which indicates that, in order tominimizethe privacy disclosure in opportunistic computing, the largerthreshold should be chosen.

However, since the high reliability of PHI process is expectedin m-Healthcare emergency, minimizing the privacydisclosure in opportunistic computing is not always the firstpriority. In Fig. 7,

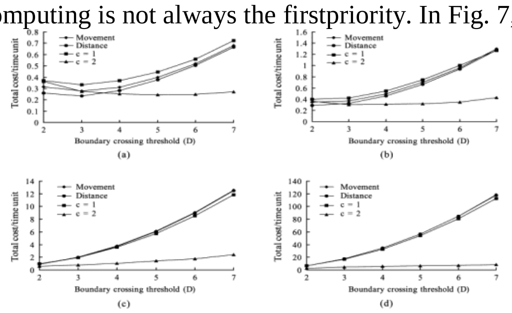


Fig. 5. RCR varying with time under different l and *th*

We plot the corresponding RCR varyingwith the time under different user number l and threshold th.

8. Related work

A technique that can be used in a middleware layer tosupport opportunistic pervasive computing applications forWSNs is presented in. The technique is based on the useof domain-oriented virtual machines that expose sensor andactuator resources to the programmer. Virtual machines arenode-specific, to reflect the specific sensors and actuatorsavailable on a given node. The proposed architecture pushesthe development of opportunistic applications as collectionsof cooperating and communicating mobile agents (executedby the virtual machines). Agents are implemented as a setof event handlers that are executed in response to events.This limits the complexity of the execution layer and makesagents compliant with the event-based programming modelof WSNs.Our approach shares with this solution the purpose ofsupporting the execution of opportunistic pervasive computingapplications, i.e. to take the best advantage of resourcesthat happen to be available in the network. However,while we deal with the problem of running applicationson homogeneous and limited hardware, the system describedin defines ontology and runtime support thatare useful when the network includes sensors and actuatorsof different nature.In the authors argue that sensor networks shouldbe programmed at global scale: proper tools should shieldthe developer from low-level details of resource management,concurrency and in-network processing.

9. FUTURE WORK

In this work, we propose an optimization framework withthe objective of maximizing the network lifetime by exploitingthe mobility management in mobile healthcare sensor systems.For the problem in offline scenario, where movements of usersare known, it has been formulated into a linear programmingform based on a novel temporal-spatial network model. Thusthe offline version could be solved in polynomial-time. However,for the online scenario, we prove that there exists no onlinealgorithm achieving a constant performance ratio comparedto the offline scenario due to lack of future information.

10. CONCLUSIONS

In this paper, we have proposed a secure and privacy preserving opportunistic computing (SPOC) framework for m-Healthcare emergency, which mainly exploits how to use opportunistic computing to achieve high reliability of PHI process and transmission in emergency while minimizing the privacy disclosure during the opportunistic computing. Detailed security analysis shows that the proposed SPOC framework can achieve the efficient user-centric privacy access control. In addition, through extensive performance evaluation, we have also demonstrated the proposed SPOC framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency. In our future work, we intend to carry on smart phone based experiments to further verify the effectiveness of the proposed SPOC framework. In addition, we will also exploit the security issues of PPSPC with internal attackers, where the internal attackers will not honestly follow the protocol.

11. REFERENCES

[1] M. R. Yuce, S. W. P. Ng, N. L. Myo, J. Y. Khan, and W. Liu, "Wireless body sensor network using medical implant band," Journal of MedicalSystems, vol. 31, no. 6, pp. 467–474, 2007.

[2] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, "Opportunistic computing for wireless sensor networks," in IEEE Proc. of MASS'07, pp.

[3] A. Passarella, M. Conti, E. Borgia, and M. Kumar, "Performance evaluation of service execution in opportunistic computing," in Proc. of ACM MSWIM '10, 2010, pp. 291–298.

[4] M. Conti, S. Giordano, M. May, and A. Passarella, "From opportunistic networks to opportunistic computing," IEEE Communications Magazine, vol. 48, pp. 126–139, September 2010.

[4] M. Conti and M. Kumar, "Opportunities in opportunistic computing," IEEE Computer, vol. 43, no. 1, pp. 42–50, 2010.

[5] J. Stankovic, Q. Cao, T. Doan, L. Fang, R. Kiran, S. Lin, R. Stoleru, A. Wood, and S. H. Son, "Wireless sensor networks for in-home healthcare: Potential challenges," in Workshop on High Confidence Medical Device Software and Systems, Philadelphia, USA, June 2005.

[6] L. Chen, Z. Cao, R. Lu, X. Liang, and X. S. Shen, "Epf: An event-aided packet forwarding protocol for privacy-preserving mobile healthcare social networks," in Proceeding of IEEE Globecom 2011, Houston, Texas, USA, Dec. 2011.

[7] X. Liang, R. Lu, L. Chen, X. Lin, and X. S. Shen, "Pec: A privacypreserving emergency call scheme for mobile healthcare social networks," Journal of Communications and Networks, vol. 13.

[8] X. Liang, X. Li, M. Barua, L. Chen, R. Lu, X. S. Shen, and H. Luo, "Enable pervasive healthcare through continuous remote health monitoring," to appear in IEEE Wireless Communications, 2012.

[9] R. Lu, X. Lin, and X. S. Shen, "Spoc: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," to appear in IEEE Transactions on Parallel and Distributed Systems, 2012.

About The Authors

Victor Prem Sagar Bochalla, received his B.Tech degree in Computer Science and Engineering from JawaharlalNehru TechnologicalUniversity, Anantapur, India, in 2010. Currently pursuing M.Tech in computer science and engineering at KVSR Institute of Technology, Kurnool, India.

K Kishore, received his MCA from Jawaharlal NehruTechnological

University, Hyderabad,India. 2006; M.Tech in Computer Science from Jawaharlal Nehru Technological University, Anantapur, India.in 2012. He is an Asst.Professor atDR.K.V.S.R.I.T, Kurnool, India.