ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

An Enhanced Protocol H-Tooth for Opportunistic Computing Followed in Body Sensor Networks

Santhosh J[1], Raji N[2]

Assistant Professor, Department of Computer Science, Sree Narayana Guru College, K.G Chavadi, Coimbatore, Tamil Nadu, India

M.Phil. Research Scholar, Department of Computer Science, Sree Narayana Guru College, K.G Chavadi, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: - Mobile e-Health or m-Health broadly encompasses the use of mobile telecommunication and multimedia technologies as they are integrated within increasingly mobile and wireless health care delivery systems. The field broadly encompasses the use of mobile telecommunication and multimedia technologies in health care delivery. M-Health is one aspect of e-Health that is pushing the limits of how to acquire, transport, store, process, and secure the raw and processed data to deliver meaningful results. M-Health offers the ability of remote individuals to participate in the health care value matrix, which may not have been possible in the past. Participation does not imply just consumption of health care services. In many cases remote users are valuable contributors to gather data regarding disease and public health concerns such as outdoor pollution, drugs and violence. The project develops a new protocol named as H-TOOTH (HEALTH TOOTH) to effectively transmit the data.

KEYWORDS: m-Health, opportunistic computing, smart phone, body sensor, energy

I. INTRODUCTION

The m-Health field operates on the premise that technology integration within the health sector has the great potential to promote a better health communication to achieve healthy lifestyles, improve decision-making by health professionals, patients and enhance healthcare quality by improving access to medical and health information and facilitating instantaneous communication in places where this was not previously possible. It follows that the increased use of technology can help reduce health care costs by improving efficiencies in the health care system and promoting prevention through Behavior Change Communication (BCC). The m-Health field also houses the idea that there exists a powerful potential to advance clinical care and public health services by facilitating health professional practice and communication and reducing health disparities through the use of mobile technology.

Efforts are ongoing to explore how a broad range of technologies, and most recently m-Health technologies, can improve such health outcomes as well as generate cost savings within the health systems of low- and middle-income countries. In some ways, the potential of m-Health lies in its ability to offer opportunities for direct voice communication of particular value in areas of poor literacy rates and limited local language-enable phones and information transfer capabilities that previous technologies did not have. Overall, mobile communication technologies are tools that can be leveraged to support existing workflows within the health sector and between the health sector and the general public.

Within the m-Health space, projects operate with a variety of objectives, as stated by the UN Foundation and Vodafone Foundation's report on *m-Health for Development*:

- increased access to healthcare and health-related information particularly for hard-to-reach populations
- improved ability to diagnose and track diseases
- timelier, more actionable public health information
- Expanded access to ongoing medical education and training for health workers.

DOI: 10.15680/IJIRCCE.2016. 0403210

1.2 Applications in the m-Health Field

While others exist, the UN Foundation and Vodafone Foundation report presents six application categories within the m-Health field.

- Education and awareness
- Helpline
- Diagnostic and treatment support
- Communication and training for healthcare workers
- Disease and epidemic outbreak tracking
- Remote monitoring
- Remote data collection

Each application category as well as specific project within the category will be described.

II. LITERATURE REVIEW

[1] Advertising on mobile devices has large potential due to the very personal and intimate nature of the devices and high targeting possibilities. We introduce a novel B-MAD system for delivering permission-based location-aware mobile advertisements to mobile phones using Bluetooth positioning and Wireless Application Protocol (WAP) Push. [2] In this paper collective neighbour discovery is proposed to reduce latency period and accomplish the discovery more efficiently. To achieve this purpose each node will be active during recommended neighbours' active time to attain rapid neighbour discovery. [3] Personal computing devices, such as smart-phones and PDAs, are commonplace, bundle several wireless network interfaces, can support compute intensive tasks, and are equipped with powerful means to produce multimedia content. Thus, they provide the resources for what we envision as a human pervasive network: a network formed by user devices, suitable to convey to users rich multimedia content and services according to their interests and needs. [4] Opportunistic computing has emerged as a new paradigm in computing, leveraging the advances in pervasive computing and opportunistic networking. Nodes in an opportunistic network avail of each others' connectivity and mobility to overcome network partitions. In opportunistic computing, this concept is generalized, as nodes avail of any resource available in the environment. Here we focus on computational resources, assuming mobile nodes opportunistically invoke services on each other. Specifically, resources are abstracted as services contributed by providers and invoked by seekers. [5] The increasing popularity of the Internet has made distribution of information via the Network increasingly common. Therefore, networks have become complex and bulky. The work of the network administrator is also increasingly important. In the conventional centralized network administration method, a host must exchange messages and data with clients. However, large networks increase workload which in turn increases net dataflow. [6] Opportunistic networks enable the emerging concept of opportunistic computing. The key observation of opportunistic computing is that the environment around (mobile) users, features a steadily increasing set of heterogeneous resources available on fixed and mobile devices with wireless networking capabilities. Resources include heterogeneous hardware components, software processes, multimedia content, sensors and sensory data. While not all resources can be available on any single device, they can be collectively available to anyone through the deployment of effective middleware in such a pervasive networking environment. [7] In this paper, we formulated the problem of fine-grained private (profile) matching for proximity-based mobile social networking and presented a suite of novel solutions that support a variety of private-matching metrics at different privacy levels. Detailed performance analysis and evaluation confirmed the high efficiency of our protocols over prior work under practical settings. Our future work is to implement our protocols as real smartphone applications and make them available for the public. [8] The security and privacy protection of the data collected from a WBAN, either while stored inside the WBAN or during their transmission outside of the WBAN, is a major unsolved concern, with challenges coming from stringent resource constraints of WBAN devices, and the high demand for both security/privacy and practicality/usability. In this article we look into two important data security issues: secure and dependable distributed data storage, and fine-grained distributed data access control for sensitive and private patient medical data. We discuss various practical issues that need to be taken into account while fulfilling the security and privacy requirements. Relevant solutions in sensor networks and WBANs are surveyed, and their applicability is analyzed. [9] CoolSpots enable a wireless mobile device to automatically switch between multiple radio interfaces, such as WiFi and Bluetooth, in order to increase battery lifetime. The main contribution of this work is an exploration of the policies that enable a system to switch among these interfaces, each with diverse radio characteristics and

different ranges, in order to save power – supported by detailed quantitative measurements. The system and policies do not require any changes to the mobile applications themselves, and changes required to existing infrastructure are minimal. [10] Devices in disruption tolerant networks (DTNs) must be able to communicate robustly in the face of short and infrequent connection opportunities. Unfortunately, one of the most inexpensive, energy-efficient and widely deployed peer-to-peer capable radios, Bluetooth, is not well-suited for use in a DTN. Bluetooth's half-duplex process of neighbor discovery can take tens of seconds to complete between two mutually undiscovered radios. This delay can be larger than the time that mobile nodes can be expected to remain in range, resulting in a missed opportunity and lower overall performance in a DTN.

PROBLEM DEFINITION

Mobile healthcare emergency services posses an important role but the data transmission and privacy disclosure is still a problem. 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.

- The Opportunistic computing have to wireless sensor network to solve the problem of storing and executing an application that exceeds the memory resources available on a single sensor node.
- Energy based considerations
- Security and privacy consideration

III. PROPOSED SYSTEM

In the proposed H-TOOTH (HEALTH TOOTH) framework aims at the security and privacy issues, and develops a user-centric privacy access control of opportunistic computing in m- Healthcare emergency. Advantages Shift from a clinic-oriented, centralized healthcare system to a patient oriented.

Distributed healthcare system Reduce healthcare expenses through more efficient use of clinical resources and earlier detection of medical conditions Challenges Performance, Reliability, Scalability, Quos, Privacy, Security. More prone to failures, caused by power exhaustion, software and hardware faults, natural disasters, malicious attacks, and human errors etc.

ARCHITECTURE DIAGRAM

The mHealth or mobile health system extents a network comprised of individual health monitoring systems that connect through the Internet to a medical server layer that resides at the top of this hierarchy. The top layer, centered on a medical server, is optimized to service thousands of individual users, and encompasses a complex network of medical personnel, interconnected services, and healthcare professionals. Each patient wears a number of sensors that are deliberately placed on his/her body. The most important functions of these sensor nodes are to discreetly sample Biosignals and transfer the relevant data to a personal server through wireless personal network implemented using Bluetooth or ZigBee. The mobile base unit, implemented on a PDA, smart phone, or personal computer, controls the WBAN and provides audio or graphical interface to the user, and handovers the statistics about health status to the medical server through the Internet or mobile phone networks (e.g., GPRS, 3G). The medical server keeps medical records of listed users and provides various services to the users, informal care givers and medical personnel. It is the responsibility of the medical server to authenticate users, accept health monitoring session data uploads, format and insert this session data into corresponding records, analyze the data patterns, recognize serious health abnormalities in order to contact emergency care givers, and forward new directives to the users.

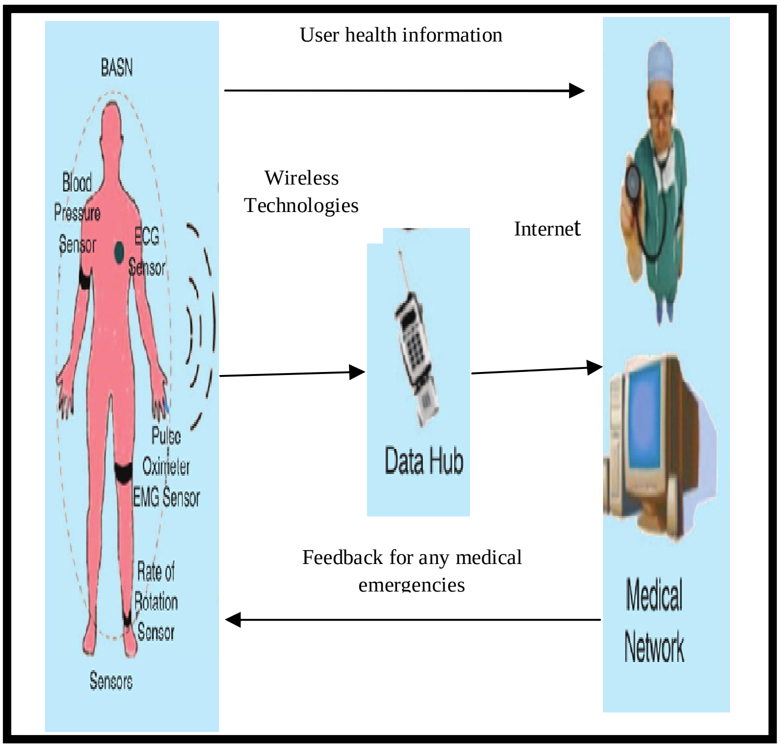

Fig 1: Architecture of Body area network

MODULES FOLLOWED

Patient details entry

In this module we are going to maintain the details of the medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and others. 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 emergency location in a timely fashion.

Supporter Node Management:

The system will find the supporter node among the possible other nodes who are having the same resource. Graphic tools are used by the mobile node for the specification, management, and installation of profiles and policies.

Mobility pattern: Each user randomly needs to register with the PHI system with their unique id. The user health record will be monitored frequently.

Base Station: The base station displays all the details about the nodes such as energy, status, and data which have been received. The base station has been created to receive the data from each node. This will helps to aggregate all results.

Emergency situation: Suppose that a patient suddenly has an emergency and he loses his mobility at all. The patient's health details will immediately disseminate an emergency message to their neighboring users until the first nearby physician/paramedic arrives at the emergency location. The data will be transmitted as SMS format.

Resource availability: Resource level will be updated frequently. This will help to identify the desire or needed resource. If the resource level is too low then the data will be sent through the neighbor node. The nearest and highest resource availability is more important in the neighbor selection.

Encryption and data transmission: Every message will be analyzed at the local node and the emergency data alone will be encrypted before sending. AES technique has been used for encryption.

IV. RESULTS AND DISCUSSION

Comparison with Existing System:
We measure the average transmitting time of the wireless hub (smart phone) in the network for eDiscovery. Existing eDiscovery mechanism is compared with the proposed H-TOOTH (HEALTH TOOTH) mechanism to show the efficiency of the proposed system and the below chart shows the average transmitting time taken in the existing and proposed system.

No of BSN	H-TOOTH	eDiscovery
Reading 1	1.45	4.34
Reading 2	1.65	3.71
Reading 3	3.41	9.43
Reading 4	3.94	12.44
Reading 5	4.32	15.90

Fig 2: Experiment table of eDiscovery and H-TOOTH

The below Chart describes about the transmit time comparison between the existing system with the proposed system. The implementation values are marked in the table and the chart is deployed based on the table value and it clearly shows that the proposed H-Tooth is working better than the existing system.

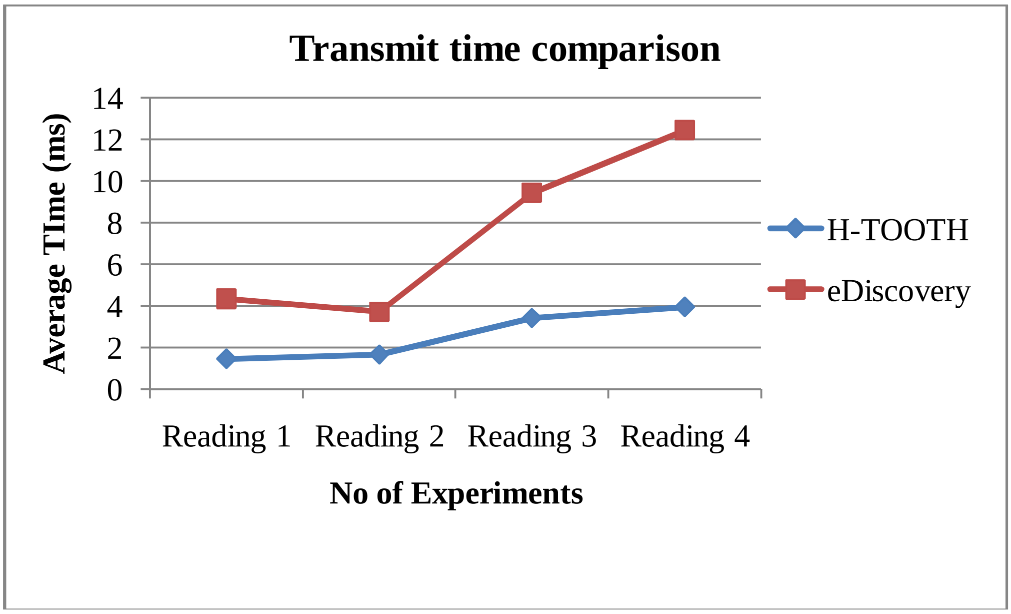

Fig 3: Transmit time comparison Chart

V. CONCLUSION

In this paper, proposed an enhanced secure and privacy-preserving opportunistic computing which is named as H-TOOTH (HEALTH TOOTH) 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 H-TOOTH

(HEALTH TOOTH) framework can achieve the efficient user-centric privacy access control. In addition, through extensive performance evaluation, also demonstrated the proposed H-TOOTH (HEALTH TOOTH) framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency.

FUTURE ENHANCEMENT

In future work, intend to carry on Smartphone based experiments to further verify the effectiveness of the proposed H-TOOTH framework. In addition, will also exploit the security issues of AES and H-TOOTH with internal attackers, where the internal attackers will not honestly follow the protocol.

REFERENCES

[1] Aalto, Lauri, et al. "Bluetooth and WAP push based location-aware mobile advertising system." *Proceedings of the 2nd international conference on Mobile systems, applications, and services*. ACM, 2004.
[2] Bakht, Mehedi, Matt Trower, and Robin Hilary Kravets. "Searchlight: won't you be my neighbor?." *Proceedings of the 18th annual international conference on Mobile computing and networking*. ACM, 2012.
[3] Conti, Marco, et al. "From opportunistic networks to opportunistic computing." *Communications Magazine, IEEE* 48.9 (2010): 126-139.
[4] Lu, Rongxing, Xiaodong Lin, and Xuemin Shen. "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency." *Parallel and Distributed Systems, IEEE Transactions on* 24.3 (2013): 614-624.
[5] Lu, Rongxing, Xiaodong Lin, and Xuemin Shen. "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency." Parallel and Distributed Systems, IEEE Transactions on 24.3 (2013): 614-624.
[6] Passarella, Andrea, et al. "Minimum-delay service provisioning in opportunistic networks." *Parallel and Distributed Systems, IEEE Transactions on* 22.8 (2011): 1267-1275.
[7] Zhang, Rui, et al. "Fine-grained private matching for proximity-based mobile social networking." *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012.
[8] Li, Ming, Wenjing Lou, and Kui Ren. "Data security and privacy in wireless body area networks." *Wireless Communications, IEEE* 17.1 (2010): 51-58.
[9] Pering, Trevor, et al. "Coolspots: reducing the power consumption of wireless mobile devices with multiple radio interfaces." *Proceedings of the 4th international conference on Mobile systems, applications and services*. ACM, 2006.
[10] Liberatore, Marc, Brian Neil Levine, and Chadi Barakat. "Maximizing transfer opportunities in bluetooth dtns." *Proceedings of the 2006 ACM CoNEXT conference*. ACM, 2006.

DOI: 10.15680/IJIRCCE.2016. 0403210