

WEHealth: A Secure and Privacy Preserving eHealth Using NOTICE

Gongjun Yan* Ye Wang† Michele C. Weigle* Stephan Olariu* Khaled Ibrahim*

* Computer Science Department

Old Dominion University

Norfolk, VA 23529

{ygongjun,mweigle,olariu,ibrah_k }@cs.odu.edu

† Lister Hill Center

National Institute of Health

Bethesda, Maryland 20894

wangye@mail.nih.gov

Abstract—Electronic health service on roads is an important issue in next generation electronic health service. Innovative health service systems are needed to provide and support individualized electronic health service for medical needs on roads. In this paper, we integrate a novel, secure and privacy preserving wireless electronic health system based on the concept and framework of NOTICE [WO07](a secure and privacy-aware architecture for the notification of traffic incidents) and PHR (Personal Health Record). The proposed system, called WEHealth, is a service-oriented PHR system through which drivers can consult and edit the health information in traffic, especially under emergency situations. More importantly, WEHealth is a secure and privacy-aware electronic health system. The proposed infrastructure prevents most security/privacy attacks.

Index Terms—Vehicular ad hoc network, eHealth, PHR, EHR.

I. INTRODUCTION

The dawn of the 21st Century sparks our ambition of using electronic health information to improve the healthcare on roads. People need health record on roads. In urgent situations, for example traffic accidents, healthcare and medical assistance can be extremely helpful in saving lives as traffic accidents are the major causes of people's injuries and deaths each year. In regular situations, people are concerned with their health more than before. For example, they want to record and monitor their everyday health conditions, like blood pressure, body temperature, etc., even if they are in a car, to prevent some accident like heart attack. Today electronic Health (eHealth) research open the door. The National Institute of Health (NIH) has started to deploy the Personal Health Record (PHR) system which is the core of eHealth. In 2000, the Networking and Information Technology Research and Development Act addressed the needs of applying information technology to healthcare services.

But health services on roads are challenging. The biggest barriers are security and privacy issues because most medical data are about individual patients and therefore highly sensitive [AJ07]. Attackers can eavesdrop, modify and delete the health care messages in communication between healthcare service providers and patients. For example, suppose a traffic accident was happened and people were injured. Healthcare messages from the healthcare provider are transmitted to these patients. The attackers may eavesdrop the messages and obtain sensitive medical information of people. Moreover, the identities of the patients are exposed to attackers who

can record and track the patients' privacy information. The attackers can sell this private information. In a word, both security and privacy breaches can cause serious legal and financial consequences.

This paper was motivated by the need to provide a secure and privacy preserving eHealth system on roads. For example, people in the cars can wear some devices can monitor their early warning signs for heart attacks like heart rate, blood pressure, etc. These signs can be sent to their health record system where heart attack model can predict the heart attack. If heart attack is most possible, urgent life saving procedures can be activated. We presents an initial effort to propose an architectural framework of eHealth in vehicular wireless networks. The proposed framework is a platform to access the PHR and provide other medical/health care.

In this paper, we (1) propose an architectural framework through which users in Wireless vEhicular network can access to Health (WEHealth) record system. This WEHealth architecture integrates the framework of NOTICE [WO07](a secure and privacy-aware architecture for the notification of traffic incidents) and PHR (Personal Health Record, for example, the one developed by NIH); (2) address the method of authentication and authorization by using the belts of NOTICE as the infrastructure of PKI; (3) state the method of privacy preserving through pseudonymization (the process of replacing real identities with artificial pseudonyms). We use the belts of NOTICE as the infrastructure to distribute the pseudonyms. The pseudonyms hide the real identities of users. Therefore, by using the belts as infrastructure, we can not only enhance security but also prevent identity attacks, for example Sybil Attacks [Dou02].

It is possible that some simple infrastructure could be used to provide a certain level of security and privacy protection. For example, a service provider could act as a service proxy which will offers pseudonyms for vehicles and publishes the service public key for vehicles. However, there are some risks. One example is the phishing attack which is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and personal health record.

Our proposal is based on NOTICE which uses vehicles' physical pressure on belts to avoid security attacks for example Sybil attacks and enhance privacy protection. All authentication, privacy preserving and security process are

performed on infrastructure without human interaction. The risks are much lower than a software based solution. One drawback is that it is more expensive because we have infrastructure. But the advantage is to provide stronger security and privacy protection. Since we are concerned with personal health records which are highly sensitive information, it is reasonable to use NOTICE as infrastructure. In addition, NOTICE can easily disseminate the accident alarms to the successor vehicles to avoid more severe accident which often result serious medical problems, because vehicles have to pass the belts which will disseminate the latest accident messages to vehicles passing by. Therefore NOTICE can actively feed alarm messages to the vehicles. Other methods like radio broadcasting, local wireless broadcasting, etc., are passive schemes. If the vehicles are not in the specific channel, they cannot receive the alarm messages.

This study makes contributions that include (1) developing an integrated electronic health system that people can use to access the PHR system, query medical questions among other people and provide medical rescues in emergency; (2) demonstrating the use of the NOTICE infrastructure to enhance the security of electronic health records and to protect the privacy of users.

II. RELATED WORK

The field of electronic healthcare has boomed since its inception in the early 1990s. However, few efforts have been focused on Healthcare on roads even with the fact that road accidents are the major causes of people's injuries and deaths each year.

A survey of research topics and trends on eHealth systems can be found in [KG06] which reviews the barriers and challenges and the current status of eHealth. Dokovsky et al. [DvHW03] proposed remote monitoring system by using 2.5/3G wireless networks. Zhao et al. [ZFD⁺04] have designed and developed a VitalPoll Telemedicine system using Bluetooth and Internet technologies with client server architecture. Environmental and health monitoring system in paper [MLLM08] is based on the wireless sensor network formed by MicaZ motes. Other similar eHealth systems using wireless sensor networks are BigNurse [BPS⁺06], CodeBlue [LMFJ⁺04], MoteCare [LLN06], and ReMoteCare [MLLM08]. Kargl et al. [KLFL08] analyzed legal ramifications, and security/privacy requirements of eHealth monitoring systems which use wireless sensor networks. For the legal ramifications, different countries have different regulations. The security of eHealth includes integrity, confidentiality and availability of data. The major privacy issue is localization. But the monitoring systems are deployed in a fixed place, such as at clinic or at home. Vehicles move along the road. It is impossible to deploy all the roads with sensors.

Slamanig et al. stated the privacy issues in eHealth [SS08]. Addition to the traditional attacks, the author proposed trivial disclosure attack and the statistical analysis of metadata. The authors proposed the pseudonymization of medical data,

identity management, anonymous authentication, etc. However, the Sybil attack can cause a problem. The concept of k-anonymity proposed by Samarati et al. [SS98], generalized a tolerable privacy by linking a user to at least k records. The Cricket location system considered the privacy as an initial design criterion [PCB00]. In this system location data can be delivered to a personal digital assistant only by the user rather than anyone else. Another location privacy discussed in [BS03] is addressed by using a new concept of mix zone which creates equal metric by collecting and reordering packets. The concept of anonymous authentication was proposed by using anonymity set [JKC⁺03], [Tze06]. Each user has a set of anonymity using which can hide the real identity information.

Elmufti et al. [EWR⁺08], and Weerasinghe et al. [WERR07] use time stamp to authenticate the electronic health records. The advantage of using time stamp includes timeliness and uniqueness guarantees, time-limited access privileges, and prevention of replay authentication message. The time stamp is useful especially when cellular system is used because the costs of mobile phone calls are based on the connection time.

III. NOTICE

The *underlying philosophy* of NOTICE [WO07], [AOW08] is that the decision about traffic-related information dissemination should rest with the infrastructure and not with individual vehicles that may have incorrect or incomplete information about the road.

The infrastructure in NOTICE is obtained by embedding sensor belts in the road at regular intervals (e.g., every mile or so), as illustrated in Figure 1. Our basic assumption is that the NOTICE is temper-proofed. If attackers want to crack the belts, the belts will alarm the maintenance team immediately. A new belt will replace the alarmed one. Each belt consists of a collection of piezoelectric pressure sensors, a simple aggregation and fusion engine, and a few small transceivers. The pressure sensors in each belt allow every message to be associated with a physical vehicle passing over the belt, eliminating the need for vehicles to be uniquely identified while avoiding the security problems outlined in the VANET literature [HvL04], [ABD⁺06]. There are two immediate benefits of using belts over roadside infrastructure. First, the belts are far less prone to tampering and, second, they are better placed to detect passing cars and to interact with them in a simple and secure fashion.

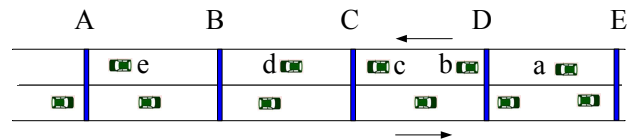


Fig. 1. A collection of belts on a two-lane road. Belts are labeled with capital letters, and cars are labeled with lowercase letters. The figure is not drawn to scale as belts are placed at least 1 km apart.

Vehicles in NOTICE are fitted with a Tamper-Resistant Device (TRD), for example, *Event Data Recorder* (EDR)

[YOW08], [HvL04], much like the well-known black-boxes on-board aircraft. All of the vehicle's sub-assemblies, including the wireless transceiver unit, speedometer, gas tank reading, tire pressure sensors, and sensors for outside temperature, feed their own readings into the TRD. As a consequence, given a time interval I of interest, the TRD can store information such as the highest and lowest speed during I , the position and time of the strongest deceleration during I , as well as location p , time t and target lane in a lane change.

A. Belt to belt communications

Each belt is fitted with a few transceivers and the belts do not communicate with each other directly. Instead, adjacent belts rely on passing vehicles to communicate. Referring to Figure 1 featuring a two-lane roadway, where each lane on the roadway has its own dedicated belt. For example, belt C consists of two *logical sub-belts*, each serving the lanes in one direction. In the case of a divided highway, belts on opposite sides of the median are connected by direct wired connection under the median.

If belt C has a message m to the next belt, B , it will encrypt m . To pass the encrypted message m to belt B , belt C will upload m onto passing car d (as will be described below). When car d reaches belt B , the message m will be dropped off and decoded by belt B . In turn, belt B may decide to send a message to belt A . This would be done using the symmetric key $\mu(B, A, t)$, known only to belts B and A .

B. Belt to car communications

Referring to Figure 1, once the pressure sensors in belt C have detected the front wheels of car c , a radio transceiver in the belt will send, at a very low power a "Hello" beacon on a standard control channel containing the ID, C , of the belt, as well as handshaking information. If there is traffic-related information that concerns car c , belt C will upload this information to the car. Belt C may also upload a message m destined for the next belt, B . Message m is encrypted. The communication time between a belt and a car has been proven to be sufficient [AOW08].

C. Car to car communications

Referring again to Figure 1, assume that belt D has an emergency message to convey to belt C . Belt D having encrypted the message will upload the message unto car b and will also set the "urgent" bit indicating that car b must try to contact cars traveling in the direction toward C forwarding the encrypted message by radio.

IV. ARCHITECTURE

Each vehicle is deployed with a short range wireless transceiver and a simple processor. The transmission range is $1m$. It can be one of the current short range devices, such as ZigBee devices or infrared devices. Both the wireless transceiver and processor are fitted into the TRD.

As shown in Figure 2, the infrastructure for WEHealth consists of a wireless base station transceiver, NOTICE belts

(shown as B_i, B_{i+1}, B_{i+2} , etc.), check station belts (shown as S_i, S_{i+1} , etc.), Internet and service servers (shown as PHR Server and Query Server). The wireless transceiver can be part of a Wireless LAN (WLAN) network. The check station belts can be multiple miles apart, for example 3 miles. The check station belts are authentication centers and pseudonyming proxies.

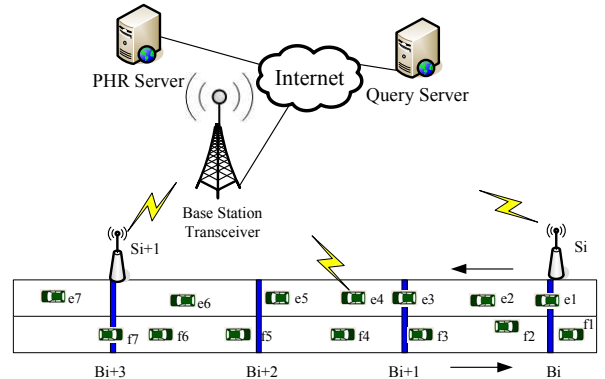


Fig. 2. The system architecture includes NOTICE infrastructure, a PHR server, a query server, wireless transceivers.

V. AUTHENTICATION AND AUTHORIZATION

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. The belts with transceiver, called check station belts shown as S_i, S_{i+1} , etc., act as the authentication belts. Both the servers and the vehicles will be authenticated through the authentication center since both of them can be compromised. If the server is valid, the vehicle will provide user ID, user password and vehicle public key to the server. Then the server can authenticate the vehicles.

Vehicles can authenticate the server in the following. The server, for example PHR server, will transmit the public key to the check station belts using a symmetric encryption method. The belts will provide the public key of the PHR server to vehicles. Vehicles pick the public key from one of the belts when vehicles pass it and encrypt a timestamp using the picked public key. The ciphertext is sent to the PHR server. If the PHR server is real, it will decrypt the timestamp and send it back to the vehicle. The vehicle can check if the timestamp from server is identical with the original one generated by itself. As shown in Figure 3, the authentication base station is the service server which will generate both public key and private key. The public key is transmitted to the check station belts S_i, S_{i+1} , and so on, where i is less than the total amount of check station N , i.e. $i \in N$. Vehicles which are new to this road will need the public key to communicate with the service server. When the front wheels of vehicles press on the check station belt S_i , the public key will be sent to the vehicles. Vehicles then generate a timestamp and encrypt the timestamp by using the public key, i.e. $PK(r)$. The ciphertext $PK(r)$ is transmitted to the service server. At the service server, the ciphertext is

decrypted by using the private key, shown as $DPK(r)$ and the service server obtains the timestamp from the ciphertext. The service server sends the timestamp back to the vehicle. On the vehicle, if the timestamp from the server is identical with the timestamp on the vehicle, the server is valid. The successor operations proceed. Otherwise, the operations will be terminated.

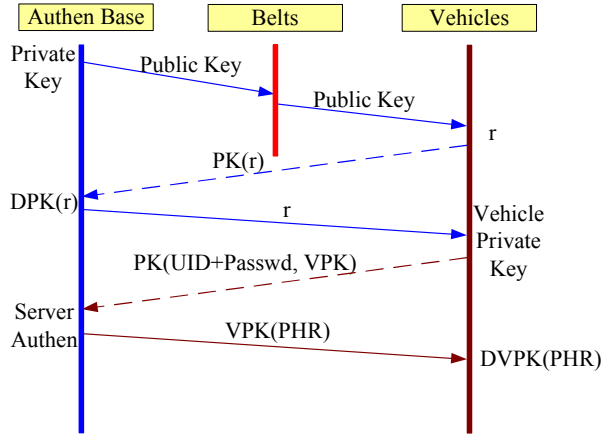


Fig. 3. The authentication scheme. Both service server and vehicles generate public key and private keys. Belts are used to distribute the server's public key. Once the server is authenticated, vehicles send the user ID, password and vehicle public key to the server for future data encryption.

The server can authenticate vehicles by checking the user ID and password pair. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password and a User ID (UID). On each subsequent use, the user must know and use the previously declared password. The user's password is encrypted by the public key of the server. Therefore nobody can decrypt it except the server. One example of such authentication is that PHR system authenticate its users. Each PHR user registers the PHR system and login PHR by using user name and password. Once the user is logged in, the user can access the health records. In Figure 3, vehicles which have authenticated the service server, i.e. the server is valid, will encrypt UID-password and Vehicle's Public Key (VPK) by using the server's public key, shown as $PK(UID + Passwd, VPK)$. The ciphertext is transmitted to the service server. The service server will first decrypt the ciphertext by using private key and then validate if the user is really in the system by checking user ID and password pair. If the user is valid, the service contents (for example, PHR) are encrypted by using the vehicles' public key, shown as $VPK(PHR)$. This ciphertext is transmitted to the vehicle and decrypted by using the vehicle private key at the vehicle.

Once the server and the user are authenticated, the authorization of communications between the server and the user can be ensured. If the server tries to send messages to the user, the server use the vehicle public key to encrypt the message. If the user tries to send message to the server, the

user encrypt the message by using the server's public key.

VI. PRESERVING PRIVACY

The messages exchanged among vehicles will expose the driver/user privacy, for example, the location of the user, the identifier, the speed, the mobility patterns, etc. Therefore anonymity and privacy of users must be protected, in particular location privacy and anonymity. The location privacy means that the location of a user can be linked to its identity. Inappropriate disclosures of those data cause privacy breaches to users, which in turn lead to serious legal and financial consequences.

The basic idea of privacy preserving is pseudonymization. Pseudonymization is a procedure by which all personal identities within a data record is replaced by one artificial identifier. The artificial pseudonym allows tracking back of data to its origins from anonymized data where all person-related data has been purged. Although we only discuss the pseudonymization on application layer, the idea can be used on lower layers to prevent identity tracking from lower layers. We therefore require an pseudonymizing proxy which will assign a pseudonym to vehicles. Vehicles will hide their real names and use the pseudonym in later communication. The check station belts are pseudonymizing proxies that generate artificial identities for the vehicles. When vehicles' front wheels press on one check station belt, vehicles receive a beacon from the belt. If the vehicle is new to this area/road, it sends a hello message, for example, "Hello, I am new." The belts will obtain the vehicle's ID by monitor the physical ID of the transceiver. If the ID is new, it will generate a pseudonym for this vehicle with a Time-To-Live (TTL) value and transmits this pseudonym-TTL message to both the vehicle and the service server. Otherwise, it will discard the pseudonym request. Once vehicles obtain the pseudonym, they can use this artificial ID to communicate with service server.

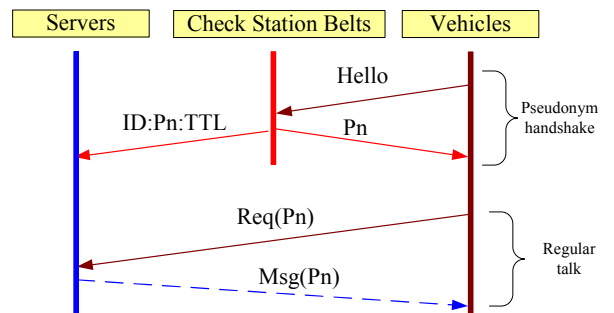


Fig. 4. Check station belts (S_i, S_{i+1} , etc.) generate pseudonyms (Pn) for new vehicles and update the server. The Time-To-Live (TTL) is used to manage the pseudonyms. All messages are encrypted by PKI.

One possible attack is Sybil attack which creates a large number of pseudonymous entities, using them to gain a disproportionately large influence. The attacker generates multiple pseudonymous IDs at each ID proxy belt (i.e. check station belts S_i, S_{i+1} , etc.) However, we can prevent this

type of attacks. The ID proxy belts will synchronize the ID list among ID proxy belts and service servers every a period of time, i.e. proactively synchronize the ID list among the system. Since the ID is the physical ID of vehicle's transceiver, it is unique and tamper-proof. The Sybil attacker can not lie about this ID. If a ID proxy finds the ID existing in the ID list, it will discard the pseudonym request. The Figure 5 shows that the ID list is synchronized among ID proxy belts and the service server. One vehicle can only obtain one valid pseudonym during the TTL period.

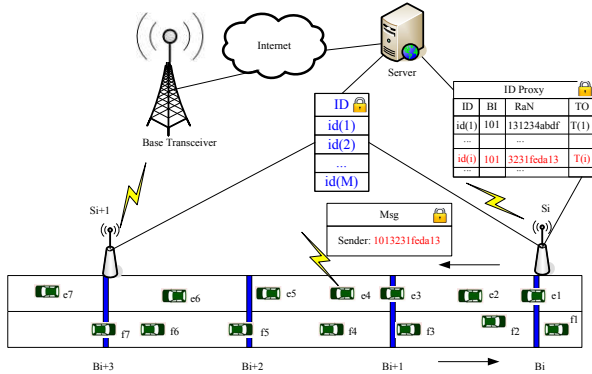


Fig. 5. Belt S_i acts as a ID proxy which converts the Real Name (RN) into a temporary name. The temporary name consists of Belt Id (BI) and a Random Number (RaN).

One concern is the semantic of belts. The semantic of belts is that belts are simple infrastructures. The original proposal of NOTICE does not expect that belts can do encryption and decryption because the hardware of belts are simple and cheap. However, there are some single chip solution for the encryption and decryption. Wong et al. [WWD98] proposed the symmetric encryption/decryption has been implemented on the Xilinx XC4000 chip which is mature and cheap (unit price less than \$5). Therefore, we can enable the encryption/decryption capability without increasing the cost much.

VII. PERSONAL HEALTH RECORD ACCESS

A. Personal Health Record System

PHR (Personal Health Record) is a computerized application that stores an individual's personal health information. There are several types of PHRs, for example, PC-based, Internet-based, and Portable-Storage PHR. We are interested in Internet-based PHR. The National Institute of Health (NIH) of U.S.A is developing such a Internet-based PHR which is accessed and edited via a Web browser. The PHR includes patient medical history, drug allergies, care plans, allergy, surgery, medical test, etc.

B. PHR Access

WEHealth provides a way to access PHR system while people drive on roads. Since the access to PHR requires multiple interactive operations, the drivers are not recommended to operate. But the other people in the vehicle can do the

access operations. Vehicles installed with a cellular mobile station which can access the cellular base station. The base station can connect to the PHR servers through Internet.

Due to the bandwidth limit, we have to make sure that some bandwidth is preserved for life saving situations. Therefore the vehicle will get a bandwidth quota from the belts before starting the PHR access. Once there is enough bandwidth for the PHR, the access is initiated and the user can operate it through the vehicle's screen. The user will login to the PHR system using the user name and password. Once logged into the system, the user can view and edit the health records. A screenshot of the PHR system is shown in Figure 6. For example, the user can click the "drugs" button to expand it and to check the drugs which should be taken.



Fig. 6. The PHR system

VIII. MEDICAL QUERY

Medical queries can be propagated in the system. Users can query other people about medical questions through the belts, for example, "Where are the nearby hospitals?", "Are there any doctors?". These queries will be uploaded to the belts. Other vehicles will pick these queries from the belts. If some users know the answer, they can answer it and upload the question-answer pair to the belts. For every several miles, we have a check station S_i , which is shown in Figure 2. The check stations will collect all the questions/question-answer pairs and transmit these messages to the query server. The query server posts these messages on the Internet. Internet users as well as the online medical experts can post answers. The requester of the query can login to the query server and access the answers while on the road or at home. Since the user account are nicknames, the identity of user is not exposed.

IX. APPLICATION EXAMPLE: MEDICAL ATTENTION AFTER AN ACCIDENT

When an accident occurs, there is often an urgent need for medical attention. WEHealth can provide prompt medical attention in three ways. The NOTICE infrastructure can help disseminate the accident alarm and medical help queries. The cellular system can immediately report the accident to law

enforcement and nearby medical centers. The traffic accident rescue expert can guide the remote rescue as well. The PHR system can provide the health records of the patients. The three systems can seamlessly combine together and parallelly operate at the same time.

The implementation of this example is shown Figure 7. To simplify the implementation, we use the cellular system (including cellular base stations and mobile stations) as the wireless communication network. The mobile stations are installed on each vehicle and the NOTICE check station belt. The mobile stations on vehicles can be basic cell phones. We can use a cell phone as the terminal user interface. The text message can be the content which is shown on cell phone's screen. Since almost all cell phones can receive and send text message, it will work as the basic interface. For smart phones, laptops, or other devices that have enhanced features like bigger screen, faster process, or more storage, we can provide an enhanced user interface like a web portal. The gateways, switches, and routers between the cellular base stations and the servers (like PHR servers, query servers, etc.) do not need to be modified. When an accident happens,

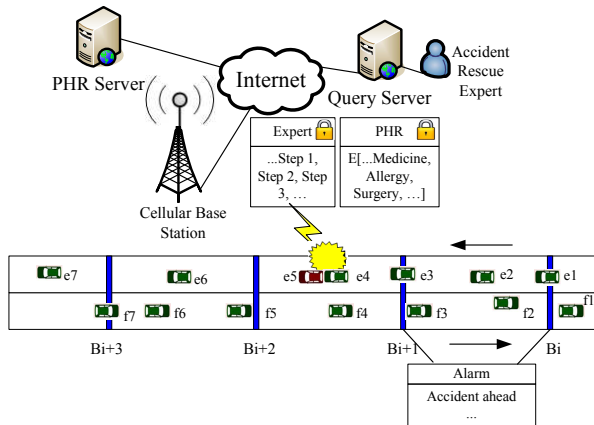


Fig. 7. The medical rescue using PHR, NOTICE and the cellular network. PHR can provide the health record of the patients. NOTICE provides a platform publishing queries and alarms. The cellular system can connect to the accident rescue expert system.

there are a series of operations as shown in Figure 8. First the accident is reported to the law enforcement, nearby medical centers, expert systems, Query servers, etc. through the cellular system. These systems receive the accident report, confirm it and respond to it (e.g., by giving orders to the vehicles involved). With the permission of the patients in the accident, medical personnel can access the PHR system through the cellular system to pull medical records of the patients and start medical procedures as soon as possible. Some medical queries can be generated and published on the Internet, for example, a query/request of a special type of blood. At the same time, vehicles in both directions can report the accident to the belts. When the belts accumulate enough reports and confirm the accident, the belts will generate alarm messages and new route messages for successor vehicles to avoid the accident.

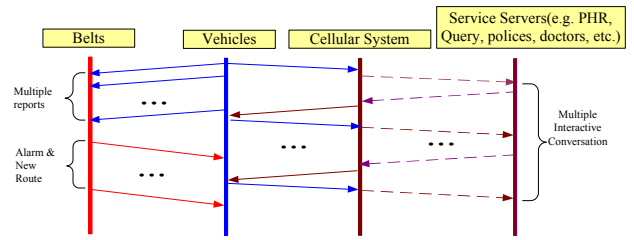


Fig. 8. Operations after an accident

Importantly, security and privacy are protected in WEHealth in the case of an accident. The belts distribute the public key to vehicles. Both vehicles and PHR server are authenticated as discussed in Section V. The sensitive medical records are encrypted. The other messages like accident rescue suggestions from expert system are encrypted as well. Pseudonyms are used instead of real identities. Attackers can not trace a particular identity.

X. CONCLUSIONS

This paper has proposed a WEHealth care system which could be a part of comprehensive effort, such as eHealth. This work opens the door for future research on nation wide healthcare, especially on vehicular wireless networks. By using the concept and architecture of NOTICE and PHR, WEHealth is a healthcare service application in traffic as well as a novel security/privacy aware platform. Users on the road can submit queries which can be answered by other users on roads, users on the Internet and online medical experts. Users on roads can access their the online Personal Health Record (PHR) as well. In an accident situation, users can seek medical help on site by querying volunteer doctors and by consulting the online accident rescue experts. At the same time the infrastructure can alarm other vehicles to prevent more severe accidents. The contribution of this study includes enhancing the feasibility of creating a national healthcare information infrastructure and developing medical help framework on accident rescue. An important contribution is that security and privacy are preserved under our proposed infrastructure.

ACKNOWLEDGMENT

The authors would like to thank support from the NSF grant CNS 0721586 and the PHR team in the Lister Hill Center (LHC) and National Library of Medicine (NLM) of NIH for the support of PHR, especially Clement J. McDonald, Lawrence C. Kingsland III, Paul Lynch, Lee Mericle, and Sumeet Muju, etc.

REFERENCES

- [ABD⁺06] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller. Attacks on inter-vehicle communication systems - an analysis. In *Proceedings of Workshop on Intelligent Transportation (WIT 2006)*, 2006.
- [AJ07] R. Agrawal and C. Johnson. Securing electronic health records without impeding the flow of information. *International Journal of Medical Informatics*, 76(5-6):471 – 479, 2007.

- [AOW08] M. Abuelela, S. Olariu, and M. C. Weigle. NOTICE: An architecture for notification of traffic incidents. In *Proceedings of the IEEE Vehicular Technology Conference - Spring*, pages 3001–3005, Singapore, May 2008.
- [BPS⁺06] R. Bader, M. Pinto, F. Spenrath, P. Wollmann, and F. Kargl. Bignurse: A wireless ad hoc network for patient monitoring. *Pervasive Health Conference and Workshops, 2006*, pages 1–4, 29 2006–Dec. 1 2006.
- [BS03] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *Pervasive Computing, IEEE*, 2(1):46–55, 2003.
- [Dou02] J. R. Douceur. The sybil attack. In *IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems*, pages 251–260, London, UK, 2002. Springer-Verlag.
- [DvHW03] N. Dokovsky, A. van Halteren, and I. Widya. Banip: Enabling remote healthcare monitoring with body area networks. In *FIDJI*, pages 62–72, 2003.
- [EWR⁺08] K. Elmufli, D. Weerasinghe, M. Rajarajan, V. Rakocevic, and S.H. Khan. Timestamp authentication protocol for remote monitoring in ehealth. In *Proceedings of Workshop on Connectivity, Mobility and Patients Comfort (CMPC) in Pervasive Healthcare Conference*, pages 73–76, Tampere Finland, Jan 29 C 31st 2008.
- [HvL04] J. P. Hubaux, S. Čapkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security and Privacy*, 2(3):49–55, 2004.
- [JKC⁺03] H. J. Jan, J. Kim, S. Choi, K. Kim, and C. Boyd. Anonymous authentication protocol for dynamic groups with power-limited devices. In *In Symposium on Cryptography and Information Security (SCIS03)*, pages 405–410, Hamamatsu, Japan, 2003.
- [KG06] G. Kaur and N. Gupta. E-health: A new perspective on global health. *Journal of Evolution and Technology*, 15(1):23–35, 2006.
- [KLFL08] F. Kargl, E. Lawrence, M. Fischer, and Y. Y. Lim. Security, privacy and legal issues in pervasive ehealth monitoring systems. In *Proceedings of 7th International Conference on Mobile Business (ICMB 2008)*, pages 296–304, Barcelona Spain, July 7th -8th 2008.
- [LLN06] E. Lubrin, E. Lawrence, and K.F. Navarro. An architecture for wearable, wireless, smart biosensors: The motecare prototype. *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on*, pages 202–202, April 2006.
- [LMFJ⁺04] K. Lorincz, D.J. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton. Sensor networks for emergency response: challenges and opportunities. *Pervasive Computing, IEEE*, 3(4):16–23, Oct.-Dec. 2004.
- [MLLM08] M. Messina, Y. Lim, E. Lawrence, and D. Martin. Implementing and validating an environmental and health monitoring system. In *Proc. 5th International Conference on Information Technology: New Generations (ITNG 2008)*, pages 994–999, Sydney, April 7-9 2008.
- [PCB00] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location-support system. In *Proc. 6th Intl Conf. Mobile Computing and Networking (Mobicom 2000)*, pages 32–43, New York, United States, 2000.
- [SS98] P. Samarati and L. Sweeney. Generalizing data to provide anonymity when disclosing information. In *Proc. of the 7th ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, page 188, Seattle, Washington, United States, Mar 1998.
- [SS08] D. Slamanig and C. Stingsl. Privacy aspects of ehealth. *ares*, 0:1226–1233, 2008.
- [Tze06] W. G. Tzeng. A secure system for data access based on anonymous authentication and time-dependent hierarchical keys. In *ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, pages 223–230, New York, NY, USA, 2006. ACM.
- [WERR07] D. Weerasinghe, K. Elmufli, M. Rajarajan, and V. Rakocevic. Securing electronic health records with novel mobile encryption schemes. *IJEH*, 3(4):395–416, 2007.
- [WO07] M. C. Weigle and S. Olariu. Intelligent highway infrastructure for planned evacuations. In *Proceedings of the First International Workshop on Research Challenges in Next Generation Networks for First Responders and Critical Infrastructures (NetCri)*, pages 594–599, New Orleans, LA, Apr 2007.
- [WWD98] K. Wong, M. Wark, and E. Dawson. A single-chip fpga implementation of the data encryption standard (des) algorithm. *Global Telecommunications Conference, 1998. GLOBECOM 98. The Bridge to Global Integration. IEEE*, 2:827–832 vol.2, 1998.
- [YOW08] G. Yan, S. Olariu, and M.C. Weigle. Providing vanet security through active position detection. *Computer Communications: Special Issue on Mobility Protocols for ITS/VANET*, article in press, 31(12):2883–2897, 2008.
- [ZFD⁺04] X. Zhao, D. Fei, C. R. Doarn, B. Harnett, and R. Merrell. A telemedicine system for wireless home healthcare based on bluetooth and the internet. *Telemedicine Journal and e-Health*, 10(supplement 2):110–116, 2004.