Mobile Netw Appl
DOI 10.1007/s11036-013-0446-y

RCare: Extending Secure Health Care to Rural Area Using VANETs

Mrinmoy Barua · Xiaohui Liang · Rongxing Lu · Xuemin (Sheman) Shen

Abstract In this paper, we propose a delay-tolerant secure long-term health care scheme, RCare, for collecting patient's sensitive personal health information (PHI). Specifically, to minimize the overall health care cost, RCare provides network connectivity to rural areas using conventional transportation vehicles (e.g., cars, buses) as relay nodes. These vehicles are expected to store, carry, and forward the PHI to the health-service-provider located mostly at the city area following an opportunistic routing. RCare improves network performance by providing incentive to the cooperative vehicles, and encompasses identity based cryptography to ensure security and privacy of the PHI during the routing period by using short digital signature and pseudo-identity. Network fairness and resistance to different possible attacks are also ensured by RCare. Extensive security and performance analyses demonstrate that RCare is able to achieve desired security requirements with effectiveness in terms of high delivery ratio with acceptable communication delay.

Keywords Rural care · eHealth · Security and privacy · Vehicular adhoc networks · Delay tolerant networks

M. Barua (✉) · X. Liang · R. Lu · X. Shen
Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada N2L 3G1
e-mail: mbarua@uwaterloo.ca

X. Liang
e-mail: x27laing@uwaterloo.ca

R. Lu
e-mail: rxlu.cn@gmail.com

X. Shen
e-mail: xshen@bbcr.uwaterloo.ca

1 Introduction

Recent advances in wireless communications and computing technologies have lent credibility in the migration of health care systems from traditional paper based to electronic system. This electronic health (eHealth) service provisioning is an increasing important requirement as the elder population in the industrialized countries is growing rapidly and an urgent solution for minimizing the health services cost is needed. According to the U.S. Census Bureau, the world's 65-and-older population is projected to triple by 2050; it was 516 million in 2009, projected to be 761 million in 2025, and 1.53 billion in 2050 [1]. This aging population mostly suffers from chronic illness, such as heart diseases, stroke, cancer, diabetes, hypertension, and makes the task of rural health care more challenging. These chronic diseases require long-term monitoring, accurate disease-management, lifestyle changes, and medication screening. Various statistics reports indicate that 133 million people or almost half of all Americans live with a chronic condition. That number is projected to increase by more than one percent per year by 2030, resulting in an estimated chronically ill population of 171 millions [19].

Part of this elderly population or chronic patients living in urban area typically receive better health care comparing to that of rural area due to the lack of care givers and infrastructures. It is true that recent growth of urbanization has people moving from rural to urban areas, but half of the world population still lives in the rural area. Specifically, in USA and Canada, around 20 % of the total population lives in rural area, 56 % of the population in the 27 Member States of the European Union (EU) lives in rural areas, and 60 % in China [9]. Moreover, some large metropolitan areas contain small towns and these small towns are isolated from the central

Published online: 11 June 2013

cluster. Providing long-term health care to these areas is also challenging.

Chronic patients live in the rural areas need to be monitored by health professionals regularly and need to be in touched with the care-givers to have an acceptable health status. Providing health care at rural areas faces many barriers, such as lacking of communication infrastructure, travel costs, lacking of health knowledge and care givers and all these prevent deprived residence from seeking acceptable health care with ease and flexibility. Recent advances in Wireless Body Area Networks (WBANs) have made it possible to deploy bio-sensors on, in, or around the patient lives at the rural area and allow to provide long-term monitoring of physiological parameters (e.g., electrocardiogram (ECG), blood oxygen levels) with physical activities. However, technological solution is needed to transfer these aggregated sen-sed data from the patient residence to the care giver's end.

Delay Tolerant Networks (DTNs) is an emerging network paradigm, which is considered as a potential low-cost solution to the problem of connecting devices in an rural area where end-to-end network connectivity is not available. In DTNs, intermittent nodes use opportunistic connectivity (e.g., a new node moves in communication range or an existing one wakes up) to provide data communication. In this paper, we address the problem of transferring sensed data from patient end to care-giver's end by integrating WBANs with Vehicular Adhoc Networks (VNETS). Authorized Vehicles equipped with On Board Units (OBUs) cooperate as relay nodes and could be used to provide network access for long-term health care application in the rural area. However, selfish nodes in DTNs do not relay other data packets but use honest nodes to relay their own packets. It degrades the network performance, and effects network fairness, as well as security. One of the promising ways to address this issue and stimulate cooperation among selfish nodes in DTNs is the incentive scheme [13]. Although the proposed scheme does not provide the solution of emergency care at the rural area but continuous monitoring with acceptable delay is helpful to set up a proactive health care system where patient life can be saved by some precaution.

In this work, we propose an incentive based delay tolerant long-term health care scheme, RCare, which is capable of monitoring patient's health status in a rural area. It uses WBAN, WiFi, and VANETs technologies to provide secure and fair data communication with provision of incentive and good reputation to the cooperative relay nodes. Due to the disconnected nature of DTNs, traditional security schemes are not applicable to RCare. To address this problem, our solution exploits Identity Based Cryptography (IBC) [4] by using aggregate digital signature that ensures proper incentive to all cooperative nodes, as well as ensure data integrity.

The remainder of this paper is organized as follows. Section 2 contains a brief description of related works. System model and design goals with different security and privacy requirements are described in Section 3. The proposed RCare scheme is introduced in Section 4. Section 5 analyzes the different security and privacy features followed by performance evaluation in Section 6. Finally, Section 7 draws our conclusions.

2 Related work

Remote patient monitoring provides additional benefits to both patients and medical personnel. The design principle and authentication processes of a remote health care system are described in [7]. Timestamp based authentication protocol in remote monitoring system is introduced in this paper and a specific protocol for untrusted mobile devices is also proposed in their work. Remote health care architecture with patient-centric access control is proposed in [3]. In order to assure the privacy of patient's personal health information (PHI), authors first defined different access privileges to data requesters according to their roles and then assigned different attribute sets to the data requesters. By using these different sets of attribute, only the qualified access requester can get access to corresponding patient's PHI and thus ensures patient-centric access policies in a remote health care architecture. A heterogeneous wireless access-based remote patient monitoring system is presented in [16]. Lin et al. [11] proposed a privacy preserving scheme, SAGE, for health care that can effectively works against global adversary. Both the content oriented and contextual privacy can be achieved by the SAGE. Masi et al. [15], proposed a feasible and effective communication protocol for exchanging patient healthcare information among disconnected clinics and hospitals. By using Telehealth Doorenbos et al.[6] enhance access to professional health education for rural healthcare providers. It can inform and educate rural health-care providers about changes in medicine and evidence-based practices, both of which may help them provide quality care.

Secure data communication in a WBAN is discussed in [2], where public and symmetric key cryptography techniques are used for secure key management and data encryption, respectively. Prediction based secure and reliable data forwarding in WBAN is introduced in [10]. This work's major contribution is to resist data injection attack during data communication in a WBAN.

Recently, several related works on incentive mechanisms for different kinds of networks appeared in [5, 12–14, 21]. In [14], Mahmoud et al., propose a light-weight secure cooperative incentive protocol that uses combination of public-key and hashing operations. They use Merkel hash tree to bundle

the packets. In [12], a practical incentive protocol for DTNs is proposed. Here, source node attaches some incentive with a group of messages. With the fair incentive, the selfish DTNs nodes could be stimulated and it increases packet delivery ratio. In our work, we modified this incentive policy and provide security and privacy with network fairness. A simple, robust and practical incentive mechanism for DTNs is proposed in [18] using pair-wise-tit-for-tat. Extensive simulation results are given to show that the incentive mechanism can increase total delivered traffic in the whole DTNs network.

Lu et al. in [13] define the fairness principle for a reputation based ad hoc network. For the Vehicular Ad Hoc Networks (VANETs), an event-based reputation model is proposed in [5] to filter bogus warning messages. Based on the location of the vehicles, the model classifies incoming traffic into different roles. Event reputation value is calculated in considering the different roles. Considering the global security, individual privacy, and easy deployment in an VANETs environment, Lei et al. present as aggregate privacy-preserving authentication protocol (APPA) in [20]. Their work aggregates multi-signatures into a single verifiable signature. Individual privacy is ensured by using public pseudo-identity that can be only traced by trusted authority.

3 Models and design goals

In this section, we formalize the system model and identify the design goal.

3.1 System model

In our model, we consider patients or users are located in a rural area where network infrastructure is not available and they need long-term monitoring due to chorionic diseases. The model is also applicable at the urban area to minimize the overall service cost, where users are located at their own residence, old-home or care center. Data communication in our proposed work relies on heterogeneous wireless environment, where WBAN (IEEE 802.15.6) is used for the body-sensor to PDA communication, Wi-Fi/IEEE 802.11n is used for PDA to RAP communication, and IEEE 802.11p namely VANET is used for Rural Access Point (RAP) to Road Side Unit (RSU) communication. Figure 1 illustrates the architecture of the system model, which consists of four interactive components:

- Trust Authority (TA): It generates the public security parameters for RCare scheme. TA is fully trusted by the all participants in the proposed scheme and in-charge of the users and vehicles registration. It is also connected to the RSU backbone network. TA is responsible for providing proper incentive or reputation to the cooperative users or vehicles. Authorized health service providers (e.g., Hospital, urgent care) may work as TA. TA is assumed powered with sufficient computing and storage capabilities and infeasible for any adversary to compromise.
- Patients: They are the registered users and equipped with bio-sensors on, in, or around their bodies. Sensors deploy in a body form a Wireless Body Area Networks (WBANs), where PDA, or efficient-sensor works as a gateway. Patient is responsible to share a secret key among the body sensors.
- Road-Side Units (RSUs): RSUs are fixed units that can be deployed at road intersections or any area of interest (e.g., bus stations, parking lot entrances, shopping center etc.). A typical RSU also functions as a wireless access point which provides wireless access to users within its coverage. RSUs are interconnected (e.g., by a dedicated network or through the Internet via cheap ADSL connections) and form a RSU backbone network. RSUs are operated and maintained by the TA and considered as trustworthy by the network's users. Received data packets at RSUs are securely forwarded to the corresponding health-care provider by using different mature Internet security protocols (such as, IPSec). So it is sufficient to transmit the data packet from rural area to any of the RSUs. In addition, RSUs also perform message authentication and certificate validation. In this article RSUs are distributed in the city area where network infrastructure is already exist.
- On-Board Units (OBUs): OBUs are installed on vehicles. A typical OBU can equip with a GPS module and a short-range wireless communication module (e.g., DSRC IEEE 802.11p [20]). Vehicles with OBUs also have sufficient processing capability and data storage. It can communicate with an RSU or other vehicles in vicinity via wireless connections. For simplicity, we refer to a vehicle as a vehicle equipped with an OBU in the rest of this paper. A vehicle can be malicious if it is an attacker or compromised by an attacker.
- Rural Access Point (RAP): In a rural area RAP is placed at social spots, such as major road intersection, gas station, shopping store etc. It can temporarily store the patient's medical data and using short-range wireless communication forward it to be relayed.

In this paper, we divide the whole network into three phases; Phase-1) data communication in a WBAN; phase-2) data communication between users and corresponding Rural Access Point (RAP); and phase-3) communication among RAP, On Board Units (OBUs), and Road Side Units (RSUs), or destination. Vehicles are categorized into three types: a) vehicles in the city (Type-1); b) vehicles in the

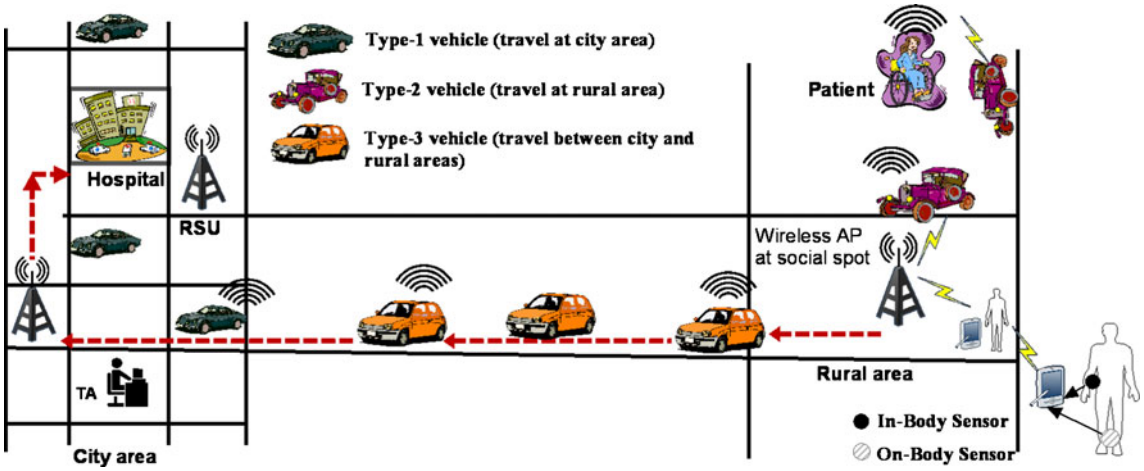

Fig. 1 System model of proposed RCare scheme

rural area (Type-2); and c) vehicles traveling between city and rural area (Type-3). Based on the different types, mobility and location of vehicles are independent. Cooperative vehicles choose shortest path to route from one place to another.

3.1.1 Wireless transmission network

We adopt Bluetooth technology in our proposed Rcare scheme as the communication standard in the WBAN environment. Different body sensors, such as accelerometer, blood pressure and oxygen saturation (SpO_2) and temperature sensors, frequently send the sensory data to the PDA using this short range, low power communication protocol. Globally used WiFi technology is used to carry the data packet at the RAP using opportunistic data forwarding. Wireless access in vehicular environment can also assist in transferring these data packets to the RAP end. However, communication between RAP and RSU is only performed by VANETs using WiFi standard (IEEE 802.11p [8]). Dashed line in the Fig. 1 shows the network connectivity in the proposed Rcare scheme.

3.2 Design goals

Our design goal is to develop a delay-tolerant long-term patient health monitoring system, where the network performance is enhanced by providing proper incentive to the cooperative relay nodes, as well as data security and patient privacy is preserved. In our privacy model, we consider how to protect a user identity privacy, where the adversary has a complete view to eavesdrop all forwarding packets but RAP and RSUs are not compromisable. RCare aims at achieving message integrity and source authentication, so that patient's sensitive PHI can deliver unaltered.

3.2.1 Security and privacy requirements

We aim at achieving the following security objectives.

1. *Message integrity and source authentication:* All accepted messages should be delivered unaltered, and the origin of the messages should be authenticated by the health-care service provider.
2. *Prevention of Packet analysis attack:* Intermediate relay nodes have sufficient time to analyze the data packet. The scheme should provide proper encryption protocol so that eavesdropper can not be able to trace-out any valid, sensitive information about patient. In addition, intermediate relay node should not be able to degrade the service quality by changing the Physical and MAC layers' packet priorities used in IEEE 802.11p standard.
3. *Prevention of Ciphertext-only attack:* The scheme should be secured enough to prevent recover of the plaintext from a set of stored ciphertexts.
4. *Provide patient privacy:* Privacy is one of the important concerns from a patient perspective. Illegal disclosure and improper use of patient's PHI can cause legal disputes and undesirable damaging in patient's personal life. In all levels of the communication, the scheme must provide patient identity privacy.
5. *Resistant to intermediate nodes adding or dropping:* Due to gain more incentive or reward, some selfish nodes may modify or add false relay information by colluding group of users. The scheme should be able to detect this type of attack.
6. *Non-repudiation:* Non-repudiation prevents either sender or receiver from denying a transmitted message. To ensure the non-repudiation, the patient can not refute the validity of a PHI afterward. As the intermediate routing nodes will get some incentive, message

non-repudiation must be ensured by the proposed scheme.

7. *Secure Routing:* In a multi-hop communication scenario, secure routing is required for the sensitive patient health information. Due to the heterogenous wireless environment, the scheme should provide secure and efficient routing of the sensitive data packets.

3.2.2 Incentive strategy

Performance of any delay-tolerant network usually depends on the cooperation of network's participants. In our proposed scheme, users and vehicles are awarded based on their participation in the network. To ensure the fairness of the incentive protocol, the intermediate forwarding nodes (either users or vehicles) can receive credit if and only if the destination node receives the data packet (Case 1). Even though the packet is not delivered to the destination, the relaying nodes still get good reputation values for their cooperation (Case 2). Reputation function takes holding-time as a parameter and encourages to forward data-packet earlier to maintain higher reputation value. To ensure more participation from the network's users, the TA defines reputation-threshold so that users crossing the threshold value will get some incentive as a bonus (Case 3). Processes of reward calculation is shown in Eq. 1.

$$Reward_i = \begin{cases} Dist_i.C_{IP} + Dist_i.R_{IP}, & \text{Case 1} \\ Dist_i.R_{IP}, & \text{Case 2} \\ Incentive_{Bonus}, & \text{Case 3.} \end{cases} \quad (1)$$

User can get a reward $Dist_i.C_{IP} + Dist_i.R_{IP}$ if the data packet P arrives at the destination. Here, $Dist$ is the distance that traveled by user/vechile, C_{IP} is unit incentive credit provided by the data packet's source, and R_{IP} is the fixed unit reputation provided by the trusted RAP/TA. Reputation value R_{IP} at any time T_n is formulated as

$$R_{IP(n)} = e^{-\lambda T_i}.R_{IP(n-1)} + CPR_i,$$

where packet holding time $T_i = T_n - T_{n-1}$. Reputation value decreasing rate is λ, and CPR_i is the cumulative participant ratio calculated by RAP/TA as $PF_j.\sum_{T=n'}^{T=n} \frac{1}{TPF_{T_j}}$. It is the ratio of the packet forwards (PF) by an individual user and total number of PF by all users at any time period $T_j = T_n - T_{n'}$. Reputation value decreasing rate,λ, can be dynamically readjusted based on network density, data type, device energy level etc.

4 The proposed RCare scheme

In this section, we present the proposed RCare, including system setting, data formation, secure patient health information transmission in different phases, incentive and reputation granting, and PHI receiving at care-giver's end. Patient's identity and location privacy, as well as secure transmission of sensitive PHI are considered to design our proposed scheme. Before delving into the details of the proposed scheme, we first review the bilinear pairing which is used as a cryptographic technique and serves the basis of the proposed RCare scheme.

4.1 Bilinear pairing and complexity assumptions

4.1.1 Notations

If x,y are two strings, then $x||y$ is the concatenation of x and y. If S is a finite set, $s \in_R S$ denotes sampling an element s uniformly at random from S. $\{0, 1\}^*$ denotes bit-string of variable length and that converts to a defined group element by the notation $\{0, 1\}^* \rightarrow \mathbb{G}$.

4.1.2 Bilinear pairing

Let $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ be two multiplicative cyclic groups of the same prime order q, and e be a computable bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathbb{T}}$ with the following properties [4]:

- Bilinearity: For all $P, Q \in \mathbb{G}$ and any $a, b \in \mathbb{G}_q^*$, we have $e(P^a, Q^b) = e(P, Q)^{ab}$.
- Non-degeneracy: There exists $P, Q \in G$ such that $e(P, Q) \neq 1_{\mathbb{G}_{\mathbb{T}}}$.
- Computability: There is an efficient algorithm to computer $e(P, Q)$ for all $P, Q \in \mathbb{G}$.

Definition 1 (Bilinear Parameters Generator ($\mathcal{G}en$)) A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter k as input and output 5 tuples $(q, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e, g)$ as the bilinear parameters, where q is a prime number with $|q| = k$. $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ are two cyclic groups of the same order q, $g \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathbb{T}}$ is a non-degenerated and efficiently computable bilinear map.

Definition 2 (Computational Diffie-Hellman (CDH) problem) The security of the proposed system depends on the hardness of computational Diffie-Hellman (CDH) problem, i.e., given $< g, g^a, g^b >$ for $g \in \mathbb{G}$ and unknown $a, b \in \mathbb{Z}_q^*$, there is no algorithm running in expected polynomial time, which can compute g^{ab} with non-negligible probability.

4.2 The RCare scheme

In this subsection, we present our proposed scheme RCare, which is designed with major four parts, namely a) system initialization and registration; b) secure data communication in a WBAN environment; c) data communication between

PDA and RAP; and d) transfer data packet to RSU using OBUs. Patient, also refer as user in RCare, uses WBAN that allows to continuous monitoring of physiological parameters (e.g., electrocardiogram (ECG), Electroencephalography(EEG), pulse rate, blood flow and oxygen levels, pressure, and temperature) with physical activities. The WBAN's gateway (e.g., PDA, SmartPhone) then forwards the sensed data to the RAP directly or uses relay nodes (other users/ vehicles) depends on the communication coverage. The forwarded data packet is then temporally stored in RAP and wait until there is an opportunity to forward the packet to RSUs at designated area using VANETs.

4.2.1 System initialization

Let all users and the TA of RCare scheme's use the same security parameters (S) and public bilinear parameters $(q, g, e, \mathbb{G}, \mathbb{G}_{\mathbb{T}})$ that generated by the function $\mathcal{G}en(S)$. The proposed scheme then generates cryptographic hash functions $H : \{0,1\}^* \rightarrow \mathbb{G}$, $H_2 : \mathbb{G} \rightarrow \{0,1\}^l$, where l is any predefined bit string length. The scheme then initializes $ENC()$ and $DEC()$ as public key cryptographic encryption and decryption protocols to be used in WBAN and $\mathcal{E}nc()$ and $\mathcal{D}ec()$ as symmetric encryption and decryption protocols, i.e., AES, or DES, to be used in phase-2 and phase-3 of data communication. TA picks up a random number $s \in \mathbb{Z}_q^*$ as a secret key, and computes the corresponding public key $P_{TA} = g^s$. Finally, TA publishes the public system parameters $(q, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e, g, P_{TA}, H)$. Both patients and cooperative vehicles that relay data packets are considered as registered users of the proposed scheme.

TA in RCare defines acceptable holding time (HT) for city and rural areas at the initialization phase. This is the maximum acceptable time an authorized cooperative relay node can store data packet before forwarding to the next available relay hope. TA chooses this time based on the number of users, incentive rate, and distance between rural area and urgency of sensed-data.

4.2.2 Registration processes

Individual user, vehicle, and body-sensor need to be registered to the system before being a part of the scheme. Registration processes have the following steps:

Step 1: Each RCare's registered user has a unique identity $U_i \in U$, $U = \{U_0 ... U_n\}$ is the set of users, and $V_i \in V$, $V = \{V_0 ... V_n\}$ is the set of registered vehicles. TA checks the individual identity and computes the pseudo-identity $PID_{U_i} = H(sU_i)$ and $PID_{V_i} = H(sV_i)$ for the user and vehicle respectively. TA stores users identities and their corresponding pseudo-identities locally. Users' add their corresponding pseudo-identities (PID) in the data packets and their identity privacy is guarantee as others can not be able to know the real identities.

Step 2: TA chooses appropriate medical body sensors based on patient's requirement. It then generates a serial number (SN) for the sensor using the patient's identity and sensor's manufacture defined unique Media Access Control (MAC) address, $SN = H(U_i || MAC_{sensor})$. Generated sensor's serial number (SN) then stores in the registered user's PDA that will be used as gateway in WBAN environment.

Step 3: RCare's registered user chooses a random number $x_i \in_R \mathbb{Z}_q^*$ as its private key. The user then computes the corresponding public key as $PK_{U_i} = g^{x_i}$.

Step 4: TA/RAP creates personal reputation account (PRA) and personal credit account (PCA) for each registered user.

4.2.3 Secure communication processes

Here, we describe different communication phases. We first describe the secure communication processes between body-sensor and PDA. Thereafter, we present steps for communication between PDA and RAP, and RAP and RSU. We use 'node' in $phase - 2$ and $phase - 3$ to refer user and vehicle, respectively.

Phase-1: Communication between body-sensors and gateway (PDA)

Here we present how a sensor securely transmits sensed data to the authenticated gateway or PDA of a registered patient. The secure communication is ensured by following a hybrid encryption policy. We use public-key cryptography to securely shared a secret key among the sensors, after that symmetric-key cryptography is used to encrypt the data. Figure 2 demonstrates basic communication steps in WBAN, where sensor processes the data and checks the freshness before sending to PDA.

The communication processes follow the following steps:

Step 1: WBAN's gateway (PDA) first chooses a random number $\beta \in_R \mathbb{Z}_q^*$, and computes session key $K = g^{\beta}$. Hashed value of this session key $H_2(K)$ is used as a shared key or symmetric key by the body sensor to encrypt the sensed data.

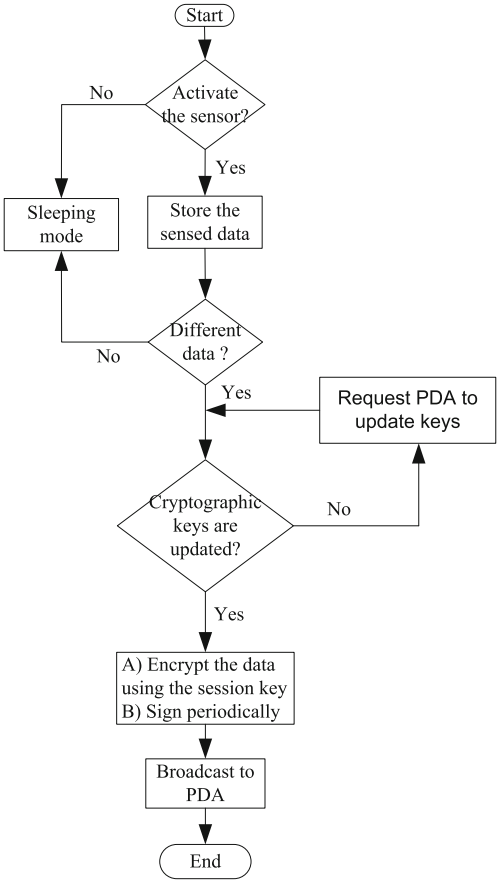

Fig. 2 Secure communication flowchart in a WBAN

Step 2: PDA then generates the session key's associate message $K' = K||CT||KVT$, where CT is the current time and KVT is the key validity time limit. If the session key's life time exceeds KVT, the corresponding body sensor then request PDA for a new key. By using K' and body-sensor's public key ($PK_{SN} = g^{\alpha}$, α is the secret key of the corresponding sensor), it then computes the encrypted message v as shown in Eq. 2.

$$\begin{aligned} v &= Enc\left(PK_{SN}, K', PK_{U_i}\right) \\ &= K' \oplus H_2\left(M_U^{x_i}\right) \end{aligned} \tag{2}$$

Here $M_U = e(Q, PK_{SN})$, $Q = SN = H(U_i||MAC_{sensor})$.

Step 3: To prove the validity of the session key, PDA signs the message K' as

$$\begin{aligned} S &= Sig(v, U_i, MAC_{sensor}, \beta) \\ &= g^{\frac{1}{H(v||U_i||MAC_{sensor}+\beta+x_i)}} \end{aligned}$$

Step 4: The encrypted message is decrypted using the $Dec(PK_{U_i}, v, d)$ function, here $d = H(SN)^{\alpha}$.

$$Dec(PK_U, v, d) = K' \tag{3}$$

$$\begin{aligned} Dec(PK_U, v, d) &= v \oplus H_2(e(d, PK_U) \\ &= v \oplus H_2(e(SN, g)^{\alpha x_i} \\ &= v \oplus H_2(e(SN, PK_{SN})^{x_i} \\ &= K' \oplus H_2\left(M_U^{x_i}\right) \\ &\quad \oplus H_2\left(M_U^{x_i}\right) = K' \end{aligned}$$

Step 5: Specific sensor then verify the signature S as

$$\begin{aligned} & e\left(g^{H(v||SN)}.K.PK_U, S\right) = e(g, g). \\ & e\left(g^{H(v||SN)}.K.PK_U, S\right) \\ & = e\left(g^{H(V||SN)}.g^{\beta}.g^{x_i}, S\right) \\ & = e(g, g)^{(H(v||SN+\beta+x_i))^{-1}.(H(v||SN+\beta+x_i))} \\ & = e(g, g) \end{aligned}$$

Phase-2: Communication between Users and RAP

After receiving the data packet at the PDA using phase-1, the user needs to transmit the sensed data to the local wireless access point, RAP. Steps toward secure data communication between the user and RAP using cooperative vehicles or other users (equipped with mobile wireless devices) as relay nodes are described as below:

Step 1: User U_0 with private-public key pair (x_0, $PK_{U_0} = g^{x_0}$) computes first the shared key $K_{ud} = PK_d^{u_0} = g^{x_0 x_d}$, where ($x_d$, $PK_d = g^{x_d}$) is the private-public key pair of the destination RAP. User 'U_0' equipped with body sensors, aggregates the sensed data ('m') and encrypts as $E = \mathcal{E}nc_{k_{sd}}(m)$.

Step 2: Determine a proper incentive policy (IP). Based on the significance of the sensed data, user chooses a packet-valid-time (PVT) and generates the data packet $M_u = PID_{U_i}||L_{U_0}||D||IP||Session_{ID}||Packet_{ID}||PVT||TS$. Here, L_{U_0} is the location information, D is the corresponding access point/destination identity, and TS is the time-stamp that indicates packet generating time.

Step 3: User then generates verifiable encrypted signatures Sig_s and Sig_0 as shown in Eqs. 4 and 5. Later on, Sig_0 is replaced by the aggregated signature Sig_{agg} that generates by multiplying secure key of the

intermediate nodes.

$$Sig_s = PK_d^{H(M_u||E)+u_0)} \quad (4)$$

$$Sig_0 = u_0 H(E||L_{U_0}||TS) \quad (5)$$

Step 4: Intermediate relay node, U_1, first checks the IP and take the routing decision based on the proposed incentive policy. If U_1 feels interested in routing the data packet, it then verifies the validity of Sig_0 with the equation $e(Sig_0, g) \stackrel{?}{=} e(PK_{U_0}, H(E||L_{U_0}||TS))$ and calculates the difference between current time and received packet's TS. If the difference is less than PVT, U_1 sends acknowledgement (ACK) to the sender U_0.

Step 5: Let $U_0 \rightarrow U_1 ... U_i \rightarrow U_d$ be the current packet forwarding path. In each routing step, intermediate node calculates short signature, $Sig_j = u_j.H(PID_{U_j}||L_{U_j}||TS)$ and computes aggregate signature as

$$Sig_{agg} \leftarrow Sig_j . \prod_{i=0}^{j-1} Sig_i.$$

Intermediate node U_j verifies the aggregate signature as

$$e(Sig_{agg}, g) \stackrel{?}{=} e(PK_{U_0}, H(E||L_{U_0}||TS)) \times \prod_{i=1}^{j-1} e(PK_{U_i}, H(M_i))$$

Here $M_i = PID_{PID_i}||L_{U_i}||TS_i$. Cooperative intermediate nodes are also attached nodes' pseudo-identities, location information, and time-stamp (TS), as shown in Fig. 3. Cooperative intermediate nodes also store hashed value of the received data packet with their current location information as a receipt. In a non-cooperative environment, these receipts will be submitted to the TA to collect their individual rewards.

Step 6: Steps 4 and 5 will be repeated until the packet reached at RAP. It then obtains the aggregate signature as $Sig_{agg} \leftarrow Sig_0 \prod_{i=1}^{d-1} Sig_i$ and verifies the validity of Sig_s and Sig_{agg} as $e(Sig_s, g^{H(M_u||E)}.PK_{U_o}) \stackrel{?}{=} e(PK_D, g)$, and $e(Sig_{agg}, g) \stackrel{?}{=} e(PK_{U_0}, H(E||L_{U_0}||TS)) \prod_{i=1}^{d-1} e(PK_{U_i}, H(M_i))$, here $M_i = (PID_{U_i}||L_{U_i}||TS_i)$.

Step 7: RAP now removes the details of next hop forwarding node set and provides incentive, or updates reputation of the participated users in our proposed RCare scheme.

Phase-3: Communication between RAP and RSUs

In our system model, all RSUs are securely connected to the TA and located at the city area, so it is sufficient to deliver the packet to any RSUs using VANETs. Steps in phase-3 are same as Phase-2, except some identities are changed. Vehicles (type-2) in the rural area are cooperate as packet carrier and search for any vehicle going towards the city, and vehicles (type-3) going towards city are treated as packet forwarder. The RAP follows packet forwarding $step - 4$ and $step - 5$ of the $phase - 2$. Intermediate cooperative vehicles,$(V_{1...d-1})$, calculate short signature as

$$Sig_i = v_i.H(PID_i||L_{V_i}||TS_i); i := 1..d-1.$$

Intermediate nodes verify the aggregate signature before forwarding it to the next cooperative node. When the packet reaches to any RSU, indicated as destination 'D', the RSU verifies the validity of the message as shown in $step - 6$. It then decrypts the message 'm' as $m = \mathcal{D}ec_{k_{sd}}(E)$, and provides the incentive and rewards to the participated vehicles $(V_1 ... V_{d-1})$.

4.3 Signature correctness

The correctness of Sig_s and Sig_{agg} are given as follows:

$$e\left(Sig_s, g^{H(M_u||E)}.PK_{U_o}\right) = e\left(PK_d^{\frac{1}{H(M_u||E)+u_0}}, g^{H(M_u||E)}.g^{u_o}\right) = e(PK_d, g) \quad (6)$$

$$\begin{aligned} e(Sig_{agg}, g) &= e\left(Sig_0 \prod_{i=1}^{d-1} Sig_i, g\right) \\ &= e\left(u_0 H(E||L_{U_0}||TS).\prod_{i=1}^{d-1} Sig_i, g\right) \\ &= e(PK_{U_0}, H(E||L_{U_0}||TS)) \\ &\quad \times \prod_{i=1}^{d-1} e(PK_{U_i}, H(M_i)) \end{aligned}$$

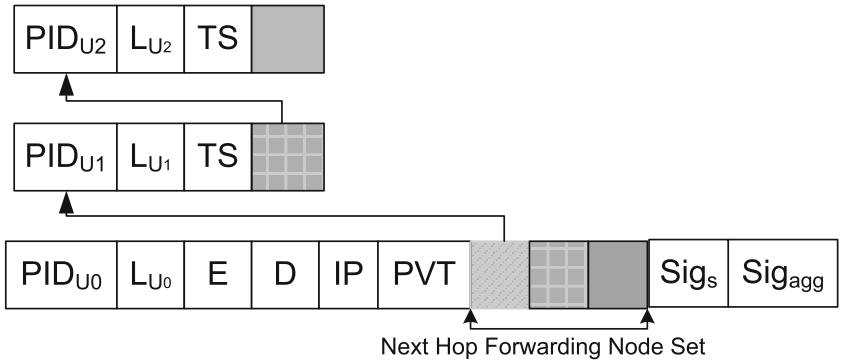

Fig. 3 Data Packet architecture of RCare scheme

4.4 Incentive and reputation granting

The TA/RAP provides incentive or reputation to the cooperative nodes as demonstrated in Algorithm 1.

Algorithm 1 Incentive and Reputation Confirmation

Require: The RAP and TA obtain aggregate signature and verify the validity of the message.

1: Get the location information, $L_{V_0}, L_{V_1}, ...L_{V_{d-1}}$, measure each intermediate node relay distance $Dis_i = |L_{U_i} - L_{U_{i-1}}|$ and their routing direction with types.
2: **for** i=1 to $d-1$ **do**
3: **if** Data packet reaches destination and the total routing time $\leq$ PVT **then**
4: Provide incentive $C_i = Dis_i \times C_{IP}$, as described in the incentive-strategy subsection.
5: **else**
6: Provide reward $R_i = Dis_i \times R_{IP}$ and incentive if accumulated rewards exceed some predefined reputation-threshold.
7: **end if**
8: Store the C_i and R_i in the individual PCA and PRA account respectively.
9: **end for**

5 Security analysis

In this section, we analyses different security and privacy issues of the proposed RCare scheme. Notice that 'node' and 'user or vehicle' are used interchangeably.

Resilience to packet analysis attack In the proposed scheme, a source node U_s encrypts the sensitive message m as $E = \mathcal{E}nc_{k_{sd}}(m)$. Here the encryption key K_{sd} is the combination of source and destination's secret keys ($K_{sd} = g^{sk_s.sk_d}$). To compute K_{sd}, the adversary has to know either the source or destination secret key. In our proposed scheme, the destination of all data packets are assigned to the trusted authority that is not compromisable and the sender will not get any benefit by disclosing his secret key. In addition, Computational Diffie-Hellman (CDH) hardness described in Section 4, ensures that even the adversary knows the public keys, he can not generate the shared key in an expected polynomial time. The adversary can get only the location (L_{U_0}) information, but this information does not contains any link to the user's original identity. In addition, eavesdropper may change priorities of physical and MAC layers' sub-channels used in IEEE 802.11p to degrade the service quality. But intermediate relay nodes in our scheme are not allowed to hold relaying packets for an undefined time due to the packet validity time period (PVT). It makes our proposed scheme adaptable to any sub-carrier channel used in IEEE 802.11p, thus ensures acceptable service quality. This parameter also reduces the probability of eavesdropping attack because the computation time needed to break the CDH hardness is far more than the chosen PVT.

RCare ensures message integrity and source authentication RCare ensures end-to-end message integrity. Users register their body-sensors at the initialization phase and the TA generates public-private key pair and pseudo-identities for these devices. Sensor's pseudo-identity is a hashed value of respective user identity and sensor's Media Access Control (MAC) address. This pseudo-identity (PID_{SN}) is used for message encryption and signature during the communication between body-sensors and PDA. It ensures message integrity at the user's end. On the other hand, RCare uses sender's secret key to generate the signature Sig_s, and the receiver can verify the signature by using the public parameters of the sender, seen in Equ. 4. This verification ensures corresponding source authentication. Hashed value of the encrypted message along with others system parameters are integrated with Sig_s and Sig_{agg}, which ensures contents of sensitive message have not been tempered with and altered thus it confirms message integrity with non-repudiation.

Resistent to intermediate-node removing or adding RCare scheme uses aggregate group signature, where secret key of each intermediate relay nodes is multiplied with the original signature. If any selfish node removes previous relaying nodes' identities, the validity of the signature will be failed

and encrypted message will be treated as invalid. Honest cooperative nodes in that case submit their received packet to the TA, and the TA can easily catch out the misbehaving nodes by checking the validity of submitted users aggregate signatures. The TA will then remove or mark that node as snooper and thus resist intermediate-node removing or adding. Moreover, this resistent helps to grow up cooperative attitude among all authorized users of the proposed RCare scheme.

RCare provides user's identity privacy We use users' pseudo-identities instated of their real identities to provide user's identity privay, and these pseudo-identities are periodically updated and maintained by the TA. Publicly available pseudo-identities are generated by using one way cryptographic hash function and computing real-identity from these pseudo-identities is impossible since keyed hash is one-way and it is impossible to reverse. To make these pseudo-identities more indistinguishable, the TA periodically update user's pseudo-identities.

RCare provides fairness RCare user's only pays credits to the cooperative intermediate users/vehiles based on distance that they travel to relay the data packet. However, if the data packet will not reach at the destination, the user won't pay any credits and it is fair to the user's perspective. The intermediate users/vehiles who are not responsible for the non-cooperative packet drooping, will gain reputation values from the TA. The RSUs and RAP always give priority to the highly reputed users. Even, if their aggregated reputation values cross the pre-defined threshold, they will get some incentive from the TA for their cooperative behavior. Thus, intermediate users or vehicles feel fair to forward RCare's data packet and improve the network performance.

Resistent to the eavesdropping attacks An eavesdropping attacker aims at accessing the private and sensitive patient's medical data. The CDH hardness (details in Basic of Bilinear Pairing subsection) ensures that the proposed scheme is resistant to this eavesdropping attack. Moreover, any intermediate node is not allowed to hold relaying packet for a undefined time due to the packet validity time period (PVT). This parameter also reduce the probability of active eavesdropping or man-in-the-middle attack because of computation time needed to break the CDH hardness is far more than the PVT.

6 Performance evaluation

In this section, we evaluate the performance of RCare in terms of probabilistic model, cryptographic overhead, average delivery ratio, and delay.

6.1 Probabilistic model

We conduct a probabilistic model to analyze the relation among the total number of users (n) in a given region, probability of having acceptable incentive rate (p_i) agreed by intermediate relay nodes, and the successful packet forward probability (P_f).

Let $E(A_i)$ be the event that there are i cooperative nodes, and $n-i$ be the number of non-cooperative nodes in a specific area. Let $E(P_f)$ be the event that there is at least a node that agree with the incentive policy and will verify the message to relay to the next-hop node. Using the equation of total probability, the relation among $Pr(P_f)$, n, and $Pr(P_i)$ can be represented as:

$$\begin{aligned} Pr(P_f) &= \sum_{i=0}^{n} Pr(E(P_f)|E(A_i)).Pr(E(A_i)) \\ &= 1 + (1-p_i)^n - 2\left(1 - \frac{p_i}{2}\right)^n. \end{aligned}$$

Here, $(1-p_i)^i$ is the probability that none of the i users agrees the incentive policy, $(1-(1-p_i)^i)$ is the probability that there is at least one cooperative node that accept the incentive policy, and $(1-(1-p_i)^{n-i})$ is the probability that there will be at least one non-cooperative node which may feel interest to relay the message to the next-hop and accept the incentive policy. Hence, $Pr(E(A_i)) = \binom{n}{i}(1/2)^i\left(1-\frac{1}{2}\right)^{n-i}$ and $Pr(E(P_f)|E(A_i)) = (1-(1-p_i)^i)(1-(1-p_i)^{n-i})$; each user position is independent and follows binomial distribution. Figure 4 shows the relation among $Pr(P_f)$, $Pr(P_i)$, and n. It can be seen that $Pr(P_f)$ increases as either $Pr(P_i)$ or n increases. Fixing the packet forwarding probability, $Pr(P_f)$, to be more than 90 %, we have to ensure either large number of users or higher incentive policy. For example, when $Pr(P_i)$ is 15 %, we have to ensure the number of user is greater than or equal to 40 to have 91 % of $Pr(P_f)$. But for a low number of users

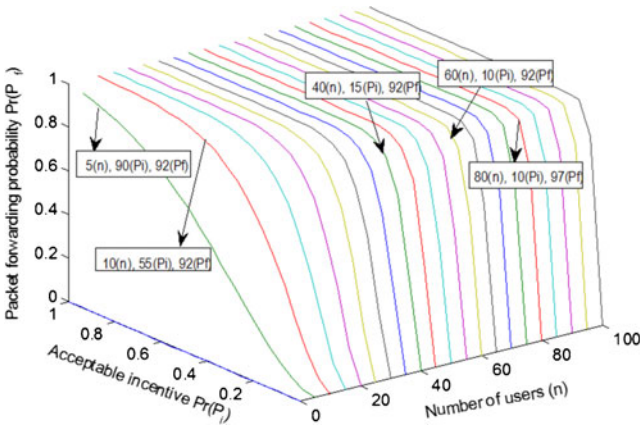

Fig. 4 Relation among P_f, p_i, and n

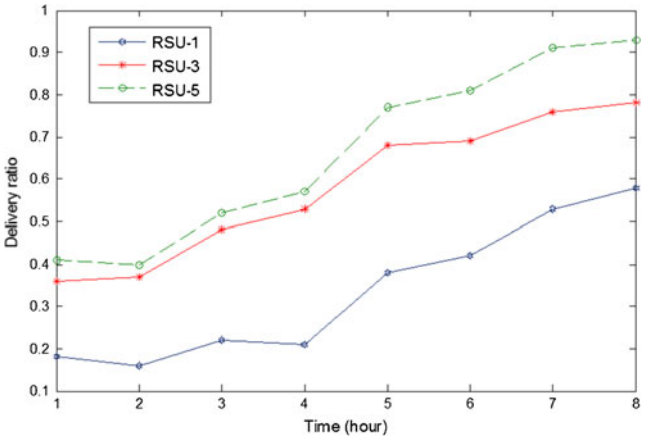

Fig. 5 Packet delivery ratio with HT=45 min

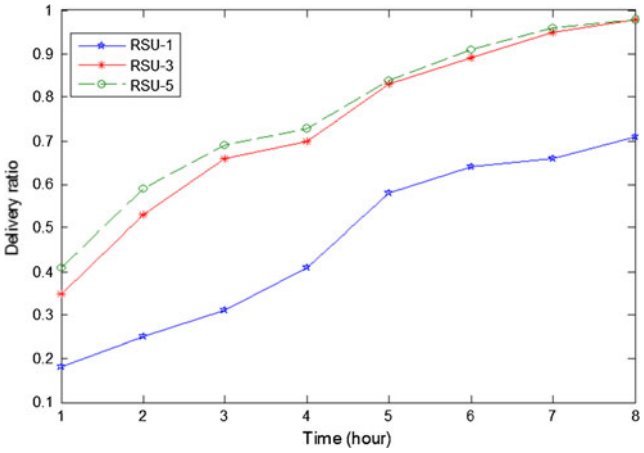

Fig. 6 Packet delivery ratio with HT=2h

$n = 10$, we have to confirm $Pr(P_i) \geq 55\ \%$ to have more than 90 % of $Pr(P_f)$.

6.2 Cryptographic overhead

In our layered packet architecture, the elements in $\mathbb{G}$ could be up to 160 bits [21]. We assume the Sig is 20 bytes, E is 120 bytes, and all other fields are 4 bytes. If there are n-intermediate nodes in the network, the communication overhead is around $140+24.n+20+|Sig_{agg}|$ bytes, $|Sig_{agg}|$ denotes the length of aggregate signature that minimize the packet length in a layered architecture [21].

Time cost We consider 20 ms and 550 ms as the computation time for the pairing using personal computer and personal digital assistant (PDA) that used as gateway in WBAN [17]. Computing cost of pairing at OBUs is expected to be same as personal computer. In [22], it is shown that a single pairing T_{pair} needs about 10 times more to compute than a multiplication T_{mul}. Proposed RCare's signature and verification processes need $T_{pair} + T_{mul}$ and $2.T_{pair} + T_{mul}$ operations, respectively. Based on the time analysis, we use 600 ms and 20 ms as the signing time for user and vehicle, respectively.

6.3 Simulation

We implement RCare scheme using a custom event-driven simulator built in Java, and consider three types of vehicles in the simulation scenario: type-1: only driving in the city area, type-2: driving in rural area, and type-3: driving between city and rural areas.

At first, we evaluate the performance by changing number of deployed RSUs and acceptable packet-holding time (HT) at the city area. Here, HT is the valid time duration by which the data packet has to be forwarded to the next cooperative relay node. Considering the city area as 5 km × 6 km, we deploy RSU in every 30 km^2 refer as RSU-1, every 10 km^2 refer as RSU-3, and every 6 km^2 refer as RSU-5. Packet-holding time HT chooses as 45 min and 120 min. Simulation results demonstrate that deploying more RSUs have a good impact on the delivery ratio (Figs. 5 and 6) and by increasing the packet-holding time, intermediate relay nodes have got more chance to deliver data packets at the destination. But compare to RSU-1, RSU-3 and 5 have almost identical performance using long holding time (2 h). Based on this observation, we deploy RSUs in every 10 km^2 (RSU-3) and prefer to use long packet-valid-time (PVT) for the rest of simulations.

We run the rest of simulations in an area of 15000 × 6000 m for 12 h (assumed $PVT = 12$ h), where road intersections are located at every 1 km and 5 km in the city and rural area, respectively. Other simulation parameters are summarized in Table 1.

In our simulation, we deploy 60 % of nodes in the city area (type-1), 20 % in the rural area (type-2), and the rest are

Table 1 Simulation parameters

Parameter	Value range
City area	5000 m × 6000 m
Rural area	10000 m × 6000 m
DTN nodes	N=60, 100
Velocity	50 km/h, 80 km/h
Packet interval	Every 20 min
Communication range	
PDA	200 m
RAP	350 m
OBUs	250 m
RSUs	350 m
Simulation time	12-hrs
Incentive Rate (IR)	50,70,90

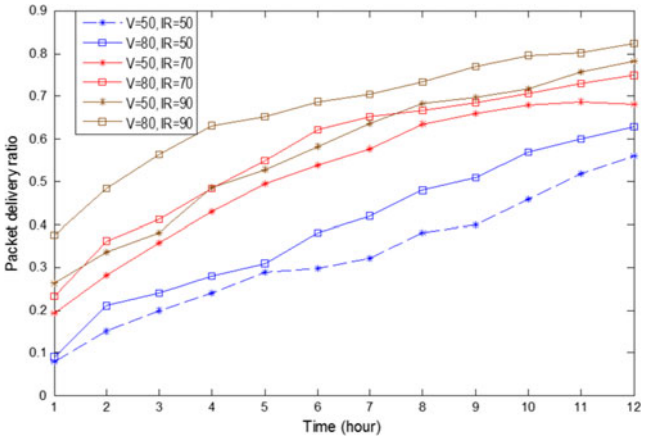

Fig. 7 Delivery ratio with N=60

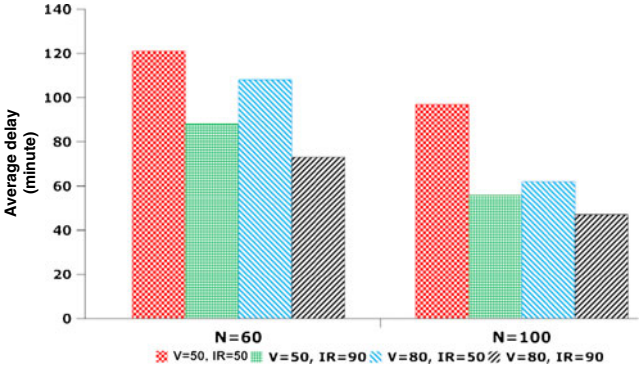

Fig. 9 Average delay within 12 h simulation with number of vehicles N=60 and 100

traveling forward and backward between the city and rural areas (type-3).

Figures 7 and 8 show the impact of vehicle's speed, incentive rate, and number of vehicles on the packet delivery ratio over a period of time. By increasing the vehicle's speed, we can achieve better packet delivery ratio compare to lower speed having the same incentive rate. For example, around 20 % more packet delivery ratio can be achieved by increasing vehicle's speed from 50 km/h to 80 km/h at the fourth hour of simulation with N=60 (Fig. 7). Increasing incentive rate motivates participating vehicles to relay other's data packets and it assists to increase the packet delivery ratio too. Simulation results demonstrate that we can achieve around 80 % of packet delivery ratio having V=80,IR=90 and N=60 at the 9th hour. It is around 30 % more compare to that of IR=50.

Figure 8 shows that higher packet delivery ratio can be achieved by increasing the number of participating users, N. For example, at the 4th hour, we can get around 30 % packet delivery ratio having N=100, V=50, and IR=50, but with N=60 we can achieve only 20 %. To ensure higher packet delivery ratio, we need to confirm either higher incentive rate or large number of participant users.

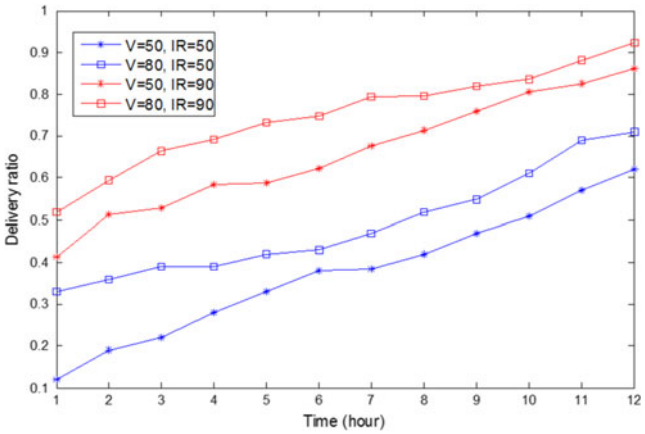

Fig. 8 Delivery ratio with N=100

Figure 9 depicts the average end-to-end delay with 12 h of simulation having variation in number of nodes (N) and incentive-rates (IR). We can see that increasing number of nodes and incentive-rate reduce the average delay and the average delay varies between 50-minutes and 120-minutes. For example, when the number of nodes $N = 60$, we can reduce the average delay to 20 min by increasing the IR from 50 to 90. This average delay can be reduced to 40 min when we use $N = 100$ and also increase the IR from 50 to 90. Simulation results demonstrate that vehicle with higher speed needs less average delay compare to slow moving vehicle.

7 Conclusion

In this paper, we have proposed a delay-tolerant secure long-term health care system, RCare, for monitoring patients located at rural area. RCare ensures secure and privacy preserving data aggregation using body sensors in WBAN environment. It describes data forwarding steps from the patient end to the care-giver's end that also achieves different security and privacy requirements. The fairness among all cooperative participants in RCare is guaranteed by adopting proper incentive and reputation policies. These policies also improve the network performance in terms of high delivery ratio and low average delay. Through extensive security and performance analyses, it has been demonstrated that RCare is highly effective to resist possible security attacks and efficient to provide emerging health care to patient resides at the rural area.

Acknowledgment Part of this work is sponsored by NSERC-CIM CRD.

References

1. U.S. census bureau. State and national population projections. http://www.census.gov/population/www/projections/popproj.html
2. Barua M, Alam MS, Liang X, Shen X (2011) Secure and quality of service assurance scheduling scheme for wban with application to ehealth. Wireless communications and networking conference (WCNC), 2011 IEEE, pp 1–5. Cancun, Quintana-Roo, Mexico
3. Barua M, Liang X, Lu R, Shen X (2011) ESPAC: enabling security and patient-centric access control for ehealth in cloud computing. Int J Secur Netw 6(2/3):67–76
4. Boneh D, Franklin MK (2001) Identity-based encryption from the weil pairing. In: CRYPTO '01: proceedings of the 21st annual international cryptology conference on advances in cryptology. Springer-Verlag, London, pp 213–229
5. Ding Q, Li X, Jiang M, Zhou X (2010) Reputation-based trust model in vehicular ad hoc networks. In: International conference on wireless communications and signal processing (WCSP), pp 1–6
6. Doorenbos A, Kundu A, Eaton L, Demiris G, Haozous E, Towle C, Buchwald D (2011) Enhancing access to cancer education for rural healthcare providers via telehealth. J Cancer Educ 26:682–686
7. Elmufti K, Weerasinghe D, Rajarajan M, Rakocevic V, Khan S (2008) Timestamp authentication protocol for remote monitoring in ehealth. In: International conference on pervasive computing technologies for healthcare (PervasiveHealth), pp 73–76
8. Jiang D, Delgrossi L (2008) IEEE 802.11p: towards an international standard for wireless access in vehicular environments. In: IEEE vehicular technology conference, pp 2036–2040
9. Kinsella K, He W (2008) An aging world: 2008. U.S. census bureau. http://www.census.gov/prod/www/abs/p95.html
10. Liang X, Li X, Shen Q, Lu R, Lin X, Shen X, Zhuang W (2012) Exploiting prediction to enable secure and reliable routing in wireless body area networks. In: INFOCOM, 2012 proceedings IEEE, pp 388–396
11. Lin X, Lu R, Shen X, Nemoto Y, Kato N (2009) Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems. IEEE J Sel Areas Commun 27(4):365–378
12. Lu R, Lin X, Zhu H, Shen X, Preiss B (2010) Pi: a practical incentive protocol for delay tolerant networks. IEEE Trans Wireless Commun 9(4):1483–1493
13. Lu R, Lin X, Zhu H, Zhang C, Ho PH, Shen X (2008) A novel fair incentive protocol for mobile ad hoc networks. In: IEEE wireless communications and networking conference (WCNC), pp 3237–3242
14. Mahmoud ME, Shen X (2011) Esip: secure incentive protocol with limited use of public-key cryptography for multihop wireless networks. IEEE Trans Mobile Comput 10(7):997–1010
15. Masi M, Pugliese R, Tiezzi F (2011) A standard-driven communication protocol for disconnected clinics in rural areas. In: IEEE international conference on e-Health networking applications and services (Healthcom), pp 304–311
16. Niyato D, Hossain E, Camorlinga S (2009) Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization. IEEE J Sel Areas Commun 27(4):412–423
17. Ramachandran A, Zhou Z, Huang D (2007) Computing cryptographic algorithms in portable and embedded devices. In: IEEE international conference on portable information devices, PORTABLE07, pp 1–7
18. Shevade U, Song HH, Qiu L, Zhang Y (2008) Incentive-aware routing in dtns. In: IEEE international conference on network protocols (ICNP), pp 238–247
19. Partners for Solutions, J.H.U., the Robert Wood Johnson Foundation (2004) Chronic conditions:making the case for ongoing care. http://www.partnershipforsolutions.org/DMS/files/chronicbook2004.pdf
20. Zhang L, Wu Q, Qin B, Domingo-Ferrer J (2011) Appa: aggregate privacy-preserving authentication in vehicular ad hoc networks. In: Lai X, Zhou J, Li H (eds) Information security, lecture notes in computer science, vol 7001. Springer, Berlin/Heidelberg, pp 293–308
21. Zhu H, Lin X, Lu R, Fan Y, Shen X (2009) Smart: a secure multilayer credit-based incentive scheme for delay-tolerant networks. IEEE Trans Vehic Technol 58(8):4628–4639
22. Zhu R, Yang G, Wong D (2005) An efficient identity-based key exchange protocol with kgs forward secrecy for low-power devices. Internet Netw Econ 3828:500–509