Privacy-preserving Scheme using Secure Group Communication for M-healthcare Information Systems

Babak Daghighi (✉ daghighi@gmail.com)

University of Malaya Faculty of Computer Science and Information Technology <https://orcid.org/0000-0001-8746-9714>

Vahid Maleki Raei

Concordia University

Miss Laiha Mat Kiah

University of Malaya: Universiti Malaya

Hamid Tahaei

University of Malaya: Universiti Malaya

Research Article

Keywords: M-healthcare information system, Secure e-health system, secure group communication, security and privacy, patient mobility

Posted Date: March 24th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-339182/v1>

License: This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Privacy-preserving scheme using secure group communication for m-healthcare information systems

Babak Daghighi^{1,*}, Vahid Maleki Raee², Miss Laiha Mat Kiah³, Hamid Tahaei⁴

¹ Faculty of Computer Engineering, Azad University Science & Research branch, Tehran, Iran

² Concordia Institute for Information System Engineering, University of Concordia, Québec, Canada

^{3,4} Faculty of Computer Science & Information Technology, University Malaya, Kuala Lumpur, Malaysia

* Corresponding Author: daghighi@gmail.com

Abstract— The expeditious growth of the wearable and implantable body sensors and wireless communication technologies have provided both inspiration and motivation for increasingly development of m-healthcare information systems as a promising next generation e-health system. In m-healthcare systems, the authorized mobile patients with the same disease symptoms can constitute a social group to share their health condition and medical experience. The privacy of social communication transferred over open wireless channels is an essential system requirement. Furthermore, the m-healthcare system on contrary to the traditional e-Health system allows mobile patients to move across distinguished location domains during different time periods. The mobility of patients considerably increases the cost of key management in terms of communication overhead if it is addressed with a naïve solution such as treating as a leave in the old location and a new join in the visited location. This paper proposes a privacy-preserving scheme, which maintains the secrecy of patients' personal health information using secure group communication in m-healthcare information systems while supporting mobility of patients. The scheme is highly scalable, and treats patients' mobility with the minimum rekeying cost, as such efficiently preserve secrecy of communication between patients associated with a social group. The security properties of the proposed scheme as well as its performance based on simulation experiments are evaluated. The experimental results demonstrate that the proposed scheme outperforms the existing solution in terms of communication overhead.

Keywords- *M-healthcare information system, Secure e-health system, secure group communication, security and privacy, patient mobility*

1 Introduction

The definition of e-health system is loose; the term refers to electronic health records (EHR) and tele-consultation [1], but has recently expanded to include the various mobile apps used to aid diagnosis and monitor patients' conditions [2] [3] [4]. The e-healthcare industry has changed the way of patient's healthcare and contributes in improving the quality of patient care by reducing the cost [5]. There are several categories of healthcare applications such as prevention, healthcare maintenance and check-ups; home healthcare monitoring; personalized healthcare monitoring; and incidence detection and management [6] [7] [8].

The healthcare system consists of several electronic tools including software systems and hardware devices [9]. These systems are increasingly becoming a distributed service involving stakeholders and resources who may be physically far from each other [10] [11] [12]. Multiple healthcare entities need to interact but do not necessarily have complete knowledge of each other. Collaboration mechanisms is required in order to permit (a) on demand formation of collaboration groups, (b) the ability for qualified strangers to join a collaboration group, (c) the ability to operate in a totally distributed setting without a central administration, and (d) guarantees of privacy and security control by the users of the collaboration system [13].

The ubiquity of mobile devices and considerable development of the wearable and implementable body sensors are undeniable because they have brought new possibilities to everyday life [14,15] [16]. A research conducted by Cisco systems forecasted the global mobile data traffic rate will tremendously grow in future due to a rapid proliferation of wireless communications and emergence of computationally fast portable devices [17]. These advances increasingly envision m-healthcare systems as a potential application of pervasive computing to improve healthcare quality and efficiency [18]. The m-healthcare systems extend the traditional centralized healthcare information system where the patient are generally assumed to stay in hospital and receive precise medical treatment from professional physicians into decentralized, and self-sponsored way. The health sensors are planted in, on or around the patient body to collect patient's personal health information (PHI) such as blood pressure, blood glucose level, and temperature level and forward them to

a PDA device. Then the PDA device serving as a gateway report these patients' personal health information (PHI) to the remote m-healthcare center.

In m-healthcare information systems, the mobile patients who have the same symptoms and diseases are allowed to search, recognize and socially interact with each other in the range of their communication without the intervention of a trusted third body for mutual support and relief. However, it brings about a series of challenges, especially how to preserve privacy of the patient's personal health information from various attack such as eavesdropping and tampering [19] [20] [21]. The main issue is that only the eligible patients of the social group and the related medical professionals must have access the patient's personal healthcare information during the data sharing in the distributed m-healthcare computing system [22] [23] [24]. It is due to the fact that most patients are concerned about each kind of unauthorized disclosure of their personal health information, which put them in trouble [25] [26] [27]. In order to deliver securely the content of the social group only to the eligible recipients, a privacy preserving key management scheme must be implemented in mobile body area networks (BAN). This key management scheme generates a common traffic key (TEK) and shares it between all participants in a social group for encrypting and decrypting PHI. The *TEK* must be updated whenever any changes occur in the social group membership in order to restricts access to the old group content by a new joining patient (i.e. to satisfy backward secrecy) as well as future group content by a leaving existing patient (i.e. to satisfy forward secrecy) [28].

Patients can exploit the possible benefit of wearing wireless body sensor and moving across distinguished location domains during different time periods. The m-healthcare information system needs to ensure the mobile patient receives the information regardless of its mobility. Patients' mobility poses a new challenge for securing m-healthcare system which is how to deliver the keying materials to moving patient while changing his location and still remaining in the social group session [29]. Patient mobility may result in extra generation of keying materials since the member is not recognized as an eligible member of the social group in the new area. As the body area networks suffer from the resources scarcity such as bandwidth limitation [30] [31], multiple rekeying messages in m-healthcare systems causes service latency. Therefore, the key management scheme must deal not only with the dynamic membership (join or leave) in a healthcare social group, but also with the dynamic patient location (mobility). While several attempts have been carried out to address the patient privacy issues lying in m-healthcare system such as [21] [32] [33] [34] [35] [36] [37], [38], most do not address patient mobility issues.

To address patient privacy issues lying in m-healthcare systems, this paper proposes a privacy-preserving scheme using secure group communication for m-healthcare information systems, called SEGUE. In the proposed model, a more practical situation of wireless mobile networks is considered in social networks where patients traverse among areas outdoors taking consideration body area networks scarcity particularly in terms of bandwidth limitation. The system handles the mobility of the patients and seamless transfer of medical information about their patients to the healthcare center (hospitals, clinics, general practitioners). In this way the patients can interact with their healthcare providers remotely and access to medical services through this distributed and multi-server based application environment.

2 Related work

One of the theoretically distinctive elements of the healthcare information system context is privacy of patients' information and their credential during the authentication process and information transfer [39]. There exist a series of attempts for authorized access control of patients' personal health information [33] [34] [35] [40] [36] [41] [37], [38]. They mainly studied the data secrecy in different modules of eHealth systems using either secure peer to peer communication or rarely secure group communication. However, the challenging problem of privacy preserving in respect to patients' mobility in m-healthcare social networks has not receive enough attention.

Lin et. al. proposed SAGE achieving not only the content oriented privacy but also the contextual privacy against a strong global adversary [33]. PEACE scheme proposed by Barua et. al. designed a secure and efficient patient-centric access control using attribute based ciphertext policy for provision of an authorized access control to patient's personal health information, and identity based encryption for protection of communication between patients and healthcare system [34]. The scheme proposed by [35] tried to preserve forward secrecy in a secure telemedicine system, which authenticates telemedicine caregiver by a session key generated with a hash function, and utilizes biometrics information for key agreement.

Authorized access control and secrecy of patient information communicated on telemedicine system was identified as one of the quality attributes in [42]. Several attempts have been carried out to preserve secrecy in telemedicine communication as one of m-Healthcare modules. Weiner et al. employed the Internet Protocol Security (IPSec) in tunnel mode with 168-bit encryption key size to protect the content transferred between recipients [40]. TeleOph provides a secure shared electronic whiteboard and multi-screen real-time ophthalmology using the secure socket layer (SSL) channel to protect data transmission between the hospital and the clinic [43]. In [36], a secure agent-based telemedicine based on P2P network architecture was constructed using two-layer safety mechanism including time-limited black boxes and RSA undetachable signature technologies for mobile agents (MA).

Poon et al. used a biometrics method to preserve secrecy of wireless body area networks used in m-Healthcare network and telemedicine system [41]. Carmen et al. proposed a method to secure body sensor communication using an intrinsic characteristics of the human body as the authentication identity or the means of securing the distribution of a cipher to secure inter BAN communications.

The most aforementioned research work used secure point to point communication to maintain the privacy of PHI. However, this mechanism cannot be efficient for a social group as a patient needs to establish a set of secure point to point communication with the other patients for preserving secrecy of information. To reduce the cost of session establishment and key distribution, secure group communication provides a scalable and efficient mechanism to preserve secrecy between group of patients [44] [45]. A key management server is responsible to generate, distribute, and update a traffic key TEK between members of a group [46] [47] [48] [49], [50] [51] [52].

Secure group communication was used in [37] and [38] to develop a secure communication respectively in telemedicine system and body area networks. Mat Kiah et al. used RSA and AES cryptography algorithms to preserve backward and forward secrecy between participants of a telemedicine system. [37]. SG-BAN proposed by Cai and Tan used secure group communication for managing and updating keying materials whenever a member joins or leaves the body area networks [38].

3 m-Health System and Security requirements

3.1 Architecture of m-Healthcare social network

M-healthcare information system generally consists of three components: the body area networks (BANs), the wireless transmission networks (WTNs), and the healthcare provider. The network is thus heterogeneous as it is a combination of various nodes with different capabilities both in terms of computing power and energy resources. Figure 1 depicts the architecture of m-healthcare information system.

Figure 1. Communication model of m-healthcare system.

Once a patient register at its local healthcare provider, a set of sensors associated to diseases he is suffering from is planted in, on or around the body to monitor and collect personal health information such as blood pressure, blood glucose level, temperature level. The patient's sensors communicate with devices such as smartphone or PDA which consists of application that allows performing the m-healthcare system functionalities, and then send this information to base stations. It is conventionally assumed that BANs are established at home or hospital and protected with by some studied security mechanism for sensor networks such as [53] [54]. The sensors forward the collected data to the health provider gateway that acts as an information aggregator. Then, the aggregator forwards the data to the health provider server via communication networks.

The m-healthcare system receives the gathered information. It analyses the collected information and sends warnings and appropriate medical records to the medical staffs. In emergency cases, the m-healthcare system can directly provide the medical status of a patient and route to the hospital, allowing physicians to prepare for treatment in advance of the

arrival of the patient. The real-time communication cannot tolerate any kind of delay or loss. The infrastructure should be reliable to provide guarantee services whether the centralized management is available or not.

In m-healthcare social group, the mobile patients suffering from the same diseases and living in the neighborhood are allowed to constitute a social group and obtain mutual support physiologically and psychologically from each other in. This is due to that they usually visit the same health provider and physician for treating their diseases located in the same vicinity.

3.2 Security and performance requirements

It is essential to understand the security requirements in an eHealth system before integrating appropriate security mechanisms. By knowing the nature of the applications, we can develop a comprehensive and strong security technique to protect the system from possible security threats. Several security services which are required to secure the eHealth systems are explained as follows:

Confidentiality: This service protects information so that only authorized patient can access the content. Confidentiality can be achieved using cryptography algorithms to encrypt data. In eHealth systems, sensitive information about the status of patient's health is transferred or stored in the system. The eavesdropping attack can be carried out with an adversary in order to abuse information for malicious activity. The use of a cryptography key can encrypt the patient information and physicians' advice. Thus, confidentiality is the essential security service in any secure eHealth system.

Authentication: This service verifies the authenticity of each entity communicating in the eHealth system in order to ensure the entity is that as it claims to be. In secure systems, a registration process verifies patient identities before providing system access. After registration, users can use passwords or keys to prove their identities. Many users are usually involved in an m-healthcare system may need to join and leave a social group. Thus, an authentication security service is necessary to prevent ineligible users from having access to the system.

Integrity: This security service ensures that group communication between patients, third parties, and physicians are not altered by an adversary when transmit over insecure networks. Lack of data integrity allows an adversary to modify the patient's information before it reach to the destination, which can be harmful in case of life-critical events.

In contrast to peer to peer communication, group communication requires to meet miscellaneous criteria to achieve security, efficiency, and scalability. The following criterion must be considered during design of a m-healthcare social networks in order to preserve the secrecy of patients' health information, and to provide system efficiency and scalability.

Backward secrecy: A patient who wishes to join a social group must be prevented from having access to the previous information and keying materials.

Forward secrecy: A patient who leaves a social group must not have access to any future information and keying materials.

Communication overhead: updating keying materials regarding any changes in group membership should not induce a high number of messages, especially for dynamic groups.

1-affects-n phenomenon: a single membership change in m-healthcare social network must not result in a rekeying process that affects the entire group members to update the traffic encryption key (TEK).

Scalability: the solution should be capable to scale the scope of key management to the large and widely distributed groups.

4 Secure m-healthcare social network implementation

A security domain is a logical or physical environment with common security and privacy protection regulations, principles and rules [55]. A security domain in m-healthcare social networks can be a group of mobile patients possessing the same diseases symptom associated with a primary physician and alternative physicians located in different health providers within the same area or vicinity and obey the same privacy mechanism.

This scheme divides the whole focused m-healthcare system domain (i.e. within a city) into the various areas. Each area contains various groups of patients. Each group involves a primary doctor and alternative doctors who can remotely handle his/her case and intervene in case of emergency, nurses and medical students. System administrator whose role is to assign doctors and medical students to patients. The assignment can be changed over time. The purpose of this division is to enable the patient to move from one area to another which are under regular medical monitoring.

Figure 3 illustrates the whole domain which is divided into the six areas. Each area is managed by an area manager deployed into the center of the area (sub group manager), which is responsible for collecting the personal health information from local patients' devices, and transmitting into the healthcare providers. The responsibility of area manager is to upload and distribute the traffic key between its local patients. In this distributed healthcare social networks, private personal health information and key updating materials are transmitted by the area managers and the traffic key (TEK) is updated by domain key manager. An example of patients' mobility is illustrated in Figure 3, where the moving patient *Patient1* is moved between area 1, 2, and 3. The patients which have the same color belong to the same medical treatment and suffering from

the same disease. The device attached with them is under the same work mode i.e. monitoring the same set of physiological characteristics.

Figure 2. Patients mobility management.

For more simplicity, the notations used throughout this paper are described in Table 1.

Table 1. Notation used in group key management scheme

Symbol	Significance	Function
P_i	Patient i	Existing moving patient in area i .
a_i	Area i	A set of patients using the same AEK and under control of AKM_i .
DKM	Domain Key Manager	The main security point, governing $AKMs$, generating and updating TEK during rekeying process.
AKM_i	Area Key Manager of area i	Granting access to P_i , PEK_i derivation, verifying the moving patients, and maintenance of the $PMOL$ and $MemL$.
TEK	Traffic Encryption Key	Specific symmetric key for encrypting and decrypting group traffic. The new_TEK and old_TEK are respectively referred to as newly generated TEK , and the currently used TEK .
PEK	Patient Key	A symmetric key that is used to encrypt messages between an AKM and each patient.
AEK	Area Encryption Key	A symmetric key used for encrypting messages sent to all members residing in an area.
DEK	Domain Encryption Key	A symmetric key shared between DKM and all $AKMs$.
$PMOL$	List of mobile patients moving an area out	This contains the list of moving members which previously left the area i and moved to other areas.
ID_{M_i}	Identity of Member i	It is used by AKM_i to generate PEK_i .
ID_G	Identity of the group communication G	It is used by AKM_i and DKM to identify particular services a patient is subscribed to.
$\{m\}K$	Message m is encrypted with symmetric key K	Message (or data) m which is encrypted with the symmetric key K .

4.1 Secure m-healthcare social network architecture

Our scheme ensures the privacy property in m-healthcare information system, which considers the mobility of patients and physicians in and outside of the hospital or between some particular health unit centers (area). The proposed scheme not only considers the hospital space but also the extension to remote patients. The proposed scheme is based on an efficient key management scheme, which can reduce the number of secured connections which is established among the nodes composing the network.

Figure 3. Secure m-healthcare social network architecture.

This scheme adopts a two tier hierarchical approach with a common traffic key shared between all entities of a m-healthcare social network similar to [48,57]. The first level is the domain level, which consists of the main key manager of the m-healthcare system referred to as domain key manager (*DKM*) for initial authentication procedure and managing the traffic encryption key. The second level is comprised of a number of manageable health provider centers (or areas) where each one is managed by an area key manager (*AKM*) independently. The areas are indeed made by dividing the domain into a number of administratively scoped regions, which can be defined logically or physically. The responsibility of *AKM* is to distribute the *TEK* between its local patients. In this distributed healthcare social networks, patients' personal health information and keying materials are transmitted automatically by the area key managers.

In this architecture, a domain can be viewed as a city, or vicinity which consists of a group of health providers. Areas can be viewed as eHealth subsystem which operate under the governance of bigger eHealth administrator systems and follow the goals and objective of the bigger. The aim of placing members in areas is to achieve scalable and efficient management, particularly when there are changes in the group membership due to join, leave or move event. Since the rekeying process is localized within the area, the *1-affects-n* phenomenon is alleviated. Figure 4 shows the main components involved in this scheme architecture.

The role of *DKM* is to ensure the management of the *TEK* triggered due to join or leave a patient to or form m-healthcare social networks. The *DKM* is responsible to manage the domain, and closely operates with *AKMs* in regards to key management. The *AKM* is responsible for key management within its area and operates under control of the *DKM*. When an *AKM* receives a message from the *DKM*, it plays a role of a proxy and sends the message to the patients residing in the area under its control. Furthermore, the management of patients' mobility are delegated to *AKMs* to omit the burden of authentication phase at the *DKM*. The *AKMs* are allowed to verify moving members, update and deliver the keying materials. Each *AKM* maintains a patient encryption key mobile owner list (*PMOL*) to keep track of moving members and reduce the need for rekeying when a moving patient return back the area where has previously been visited.

The following assumption are considered during the design of the proposed scheme.

- All cryptography keys specified in Section 4.2 are already established at initial group setup.
- All key managers (i.e. *DKM* and *AKM*) are trustworthy and reliable and all members trust them.
- The *AKM* has capability of deriving PEK_i without involving the *DKM*.
- Implicit use of member authentication mechanism such as RSA or message authentication codes (MACs) to verify the authenticity of each patient who joins the social network.
- Availability of secure storage of cryptographic keys for all group communication entities.
- Availability of secure mechanism for managing the *PMOL*.
- Sensor nodes are able to perform symmetric encryption.
- Each sensor node is able to keep a list of remote third parties, which is pre-established during the initialization phase.

4.2 Key establishment and distribution

A variety of keys are used by entities to establish a secure m-healthcare information system. Because of body area networks restrictions in terms of computation, power and bandwidth limitation [28] [31], the symmetric key cryptography algorithm is used in the design of this scheme as they are faster and less complex technique in contrast to the asymmetric key cryptography algorithm [58]. The details of all types of keys in this proposed scheme are described as follows:

Domain Encryption Key (DEK): is a symmetric key generated by the *DKM* and shared between all *AKMs* within the domain. This key is used to protect controlling messages and other keys between the *DKM* and all *AKMs*.

Area Encryption Key (AEK): is generated by each *AKM* and distributed between patients of a social group residing in its corresponding area. This key assists *AKM* in disseminating traffic key to all patients using a secure multicast communication.

Patient Encryption Key (PEK): is a unique key shared between the *AKM* of area *i* and the group member *M* residing in that particular area. The Area-Member key is generated by the *AKM* of member's area, and used only for secure unicast communication between member and its *AKM*.

Traffic Keys (TEK): is a unique key shared between all members of a social group in a domain for protecting the patients' personal health information.

Due to the symmetric structure the body sensors for medical care's such as ECG are generally deployed on patients to monitor the vital signs. The patients suffering from the same disease are connected within a same social group, and they have not permission to enter or see the communication of other social groups. In this way each social group is secured with its own *TEK*. In order to preserve backward and forward secrecy, the *TEK* must be updated whenever a patient joins the social group or leave it. Three cases of rekeying are distinguished as follows:

- Join rekeying: when a new patient joins a healthcare function, a new *AEK_i* and *TEK* must be generated and distributed to the group members. The scenario is shown in action (1) in Figure 4.
- Move rekeying: when a mobile patient changes its location from one area to another, the *TEK* is not changed but the *AEK_j* in the new area may be changed. This scenario is depicted as action (2) in Figure 4.
- Leave rekeying: when a patient leaves the healthcare function, the *TEK* is generated and delivered to the remaining social group members. The *AEK* is also updated in area which their *AEKs* are still valid and carried by the leaving mobile patient. This scenario is illustrated by action (3) in Figure 4.

4.3 Mobility key management

The *AKM* uses a key derivation function like PRF-HMAC-SHA-256 [59] to generate *PEK_i* of a new patient joining the healthcare social group. While PRF-HMAC-SHA-256 provides secure pseudo random functions suitable for generating keying materials, its goal is to ensure the packets are authentic and not modified in transit. All *AKMs* require to use the same PRF-HMAC-SHA-256 in order to achieve a coordination throughout the domain for deriving the same *PEK* in all areas. Using the same PRF enables the *AKMs* to generate a unique *PEK_i* specific for patient *P_i*. To generate the *PEK_i*, each *AKM* uses the Formula 1 as follows:

$$PEK_i = PRF-HMAC-SHA-256(DEK \parallel ID_{P_i} \parallel ID_G \parallel text) \quad (1)$$

In Formula 1, *DEK* is generated with the *DKM* and shared between all *AKMs*, *ID_{P_i}* is the identity of patient, *ID_G* is the identity of the social group that the patient interested in joining, and *Text* contains other security parameters corresponding to the member. This authentication mechanism enables all the *AKMs* to verify the *PEK* presented by a moving patient independent from the *DKM*. Figure 2 depicts the verification a moving patient in area *j* by derivation and comparison of its *PEK_i*.

Figure 4. Mobility key management process.

The advantages of using this mechanism are as follows:

- (1) the bottleneck on the *DKM* is mitigated for managing mobility of dynamic members as the *DKM* is not swarmed with the multitude singling messages for authentication of moving members.
- (2) the resource constraint mobile devices do not undergo heavy computing process during authentication phase in the visited area, and
- (3) the management of moving members are distributed between all *AKMs*, which result in saving enormous bandwidth utilization during rekeying process.

4.4 List management

An important concept used as part of the mobility protocol design is a managing list(s) referred as *PEK* Mobile Owner List (*PMOL*). This list enables each *AKM* to keep track of mobile patient who may accumulate the keying materials in the visited areas. The advantage of use of this list is to avoid frequent rekeying in visited areas that may cause disruption in social group communication. Each *AKM* in a domain securely maintains its own *PMOL* and stores the information of patients who move out its managing area. The *AKM* logs identity of the moving member ID_{M_i} , identity of group communication ID_G joined by the member, identity of the area the that a member is moving to in *PMOL*.

Another list called *MemL* maintained with *AKMs* contains the information of current patients residing in the area. The information in *MemL* is used by key managers in a domain in order to locally handle the update of keying materials within the area upon any membership changes occur in the m-healthcare social group.

4.5 Patient joining protocol to existing social group

A patient P_i located in area i sends a join request message signed with its private key to AKM_i through a secure channel such as SSL[60] [61] or TLS[62]. On receipt of join request, AKM_i verifies the member's request. If the member is authorized to join the healthcare session, AKM_i informs the *DKM* and concurrently generates a new AEK_i and PEK_i and then send to the patient P_i protected under public key of the patient.

Upon receiving the message, the *DKM* generates a new *TEK* to guarantee backward secrecy throughout the domain. The *DKM* sends the new *TEK* to AKM_i manager of area i where the new member has joined the healthcare session as well as other *AKMs* in the domain. The AKM_i sends the new *TEK* to the members residing in area i encrypted with the old AEK_i in order to preserve backward secrecy. The other *AKMs* distribute the new *TEK* to the patient inside their area by a secure multicast communication.

Figure 5. Join protocol messages flow

4.6 Patient mobility protocol

This protocol describes the mobility of a patient P_i from area i to area j with provision of backward secrecy in the visited area. Figure 6 outlines the flow of the mobility protocol in algorithmic form. The following operations are executed upon a patient mobility.

Figure 6. Mobility protocol when a member M moves from area i to area j .

- Mobile patient P_i informs simultaneously both its current AKM_i and the target AKM_j by sending a *Move Notify* message protected under PEK_i .
- On receiving the move notify message, AKM_i verifies the message and informs the DKM about the P_i mobility. AKM_i does not require to carry out rekeying process for AEK_i since the patient P_i still remains in the session.
- As the request of P_i reaches the target AKM_j , the patient P_i undergoes authentication process. The AKM_j derives the PEK_i (as stated in Section 4.3). If the patient verification is successful, AKM_j does the following:
 - It looks for P_i 's identity in its $PMOL_j$. If P_i is not in the list, AKM_j must check the join time $t_{P_i}^{join}$ of P_i . If the join time $t_{P_i}^{join}$ is after the last AEK_j update time key $t_{AEK_j}^{update}$ (i.e $t_{P_i}^{join} > t_{AEK_j}^{update}$), AKM_j needs to perform key update process to refresh the AEK_j for achieving backward secrecy. It sends the new_AEK_j to P_i and all patient in area j . Meanwhile, information of the arrival is added to the $MemL_j$.
 - In case that the M_i appear in the $PMOL$, there is no need to rekey the area encryption key AEK_i . AKM_j only sends the current area key AEK_j to P_i .
- AKM_j notifies the previous AKM_i and the DKM about moving M_i from area i to area j . PKM_i subsequently removes member information from $MemL_i$ and puts it into $PMOL_i$.

Figure 7. Patient mobility protocol when moving from area i to area j .

4.7 Existing patient leaving protocol from the social group

When a patient P_i leaves the social group treatment, it informs its AKM_i . Upon receiving the message, AKM_i decrypts and checks the message, and subsequently encrypts and sends it to the DKM . In order to achieve forward secrecy at area i , AKM_i updates the AEK_i . The DKM removes the information of departure P_i from the social group session. The new TEK is generated and distributed along with departing P_i information throughout the domain.

Upon receiving the new TEK , AKM_i sends the new_TEK and new_AEK to residue patients in area i encrypted with each patient PEK_i excluding the leaving patient P_i . AKM_i removes P_i from $MemL_i$. The leaving patient might have visited other areas inside the domain and accumulated information of each visited area. Therefore, the P_i knows all the $AEKs$ used in previously visited areas. Thereby, the $AEKs$ of these areas must be refreshed. In other areas a_t ($t \neq i$) where the patient P_i has previously visited them or is in the $PMOL_t$, AKM_t ($t \neq i$) must update the AEK_t and send it along with the new TEK to its members in its area a_t encrypted with the PEK_t of each patient P_i . Moreover, AKM_t removes information of the leaving patient P_i from its $PMOL_t$. Other AKM_q sends a multicast message containing the new TEK protected under AEK_q to all patients residing in area q . Figure 8 depicts an example of a patient leaving.

Figure 8. An existing patient leaving protocol message flows.

5 Result and analysis

The proposed scheme is compared with a secure eHealth system described in literature namely, Mat Kiah et al. [37] (for simplicity called herein TSGC). The TSGC proposed a secure telemedicine system using decentralized group key management with a common TEK for the whole collaborated members. However, it did not consider the mobility of patients which may occur between different clinical units while remaining in the social group session. Thus, the mobility of a patient is treated as a leave in the old area and a join in the new area.

5.1 General comparison

The generic comparison of the proposed scheme SEGUE and the TSGC scheme are summarized in Table 2 in terms of number of rekeying messages when any membership changes occur in the m-healthcare social network. In Table 2, the number of patients residing in area i , and the number of areas in the domain are respectively denoted by n_i , and $|A_p|$. From Table 2, both schemes require two messages to update the keying materials when a patient joins a social group. The TSGC shows considerable overhead when patients move between areas in a m-healthcare domain due to the lack of mechanism for managing mobility. Thus, the rekeying load at the core network significantly increases especially in dynamic mobile environments where the patients change their location frequently, which leads to the lack of scalability.

Moreover, the TSGC requires to manage mobility events in synchronization with the *DKM*. Thus, the centralized *DKM* must be involved in the generation of *TEK* and auxiliary keys, which makes the TSGC slower than the proposed scheme. This is due to the fact that the signaling messages should traverse a long path to the *DKM* that may be far from the *AKMs*. In the proposed scheme, The *AKM_j* can derive *PEK_i* of each mobile patient independent of the *DKM* and the old *AKM_i*. Thus, patient mobility is managed with minimal services latency.

The SEGUE shows more overhead when a patient leaves the social group. Because when a patient leaves the social group, not only the *AEK_i* of the area where he leaves the group must be updated by using unicast messages, but also the *AEK_i* of the areas where the patient has previously visited and is still valid must be refreshed. But, the TSGC just needs to update the *AEK* of the area where the leave event occurs.

Table 2. HISCOM comparison with other schemes.

Scheme	Join	Move	Leave
SEGUE	2	< 2	$n_i + n_r + A_p + 1$
TSGC	2	$(n_i - 1) + 3$	$n_i + A_p + 1$

5.2 Simulation model

The implementation of the proposed scheme has been carried out in the network simulator NS3 [63]. The NS3 is a discrete event network simulator which provides an environment to develop and implement network scenario. This section presents the simulation model and some results obtained through several simulation experiments. A two tiers distribution hierarchy with distinct five clinical units was designed for the proposed scheme. One *DKM* within the first tier is responsible for governing all *AKMs* as well as managing the common *TEK* for the whole group. Each area in the second tier is managed by an *AKM*.

The patients join to the healthcare social group according to Poisson process with inter arrival rate λ , and each patient's membership duration follows an exponential distribution with a mean duration $\frac{1}{\mu}$ time units [64], [65]. All inter arrivals are independent and identically distributed. The average number of concurrent members in the group is defined as ρ given by λ/μ .

The session time was assumed for 30 minutes. All patients enter the healthcare social group through any of the areas with an inter-arrival average λ equal to 10 seconds. Once a patient joins the group, its membership duration follows an exponential distribution with a mean duration $1/\mu$ time unit equal 15 minutes. In order to study the impact of group size variation as one of the scalability requirements on the scheme performance, both parameters the inter arrival rate and membership duration respectively vary [5sec : 75sec] and [10 min : 25 min] in separate experiments. The patient remains in each area for a determined time, and then moves to the other areas with the same probability of selection. The velocity of members is set constant for all experiments equal to 5 m/s.

5.2.1 Communication overhead

This requirement satisfies the bandwidth consumption of the wireless networks and devices. The high number of messages transmitted either by unicast or multicast during performing rekeying process consume enormous network bandwidth, which result in delays in distributing the keying materials and disruption in the m-healthcare social networks services.

It can clearly be observed from Figure 9, and Figure 10 that the TSGC induces high number of rekeying messages than the SEGUE due to the lack of a protocol intended for managing mobile patients. Lack of strategy for handling the mobility event significantly increases the rekeying messages overheads particularly in the group with big size. Both Figures 9 and 10 obviously depict that the ratio of rekeying messages has increased when the group population rise up due to either the increase of inter arrival rate or increase of membership duration.

Figure 9. Impact of inter arrival variation on rekeying message overhead.

The proposed scheme SEGUE has introduced the use of mobility list as to record the track of moving members such that the old area induces null communication overhead in mobility event and the visited area retains the communication overhead at minimum level. As a result, this mechanism improves bandwidth efficiency of the system while satisfying backward secrecy.

Figure 10. Impact of membership duration variation on rekeying message overhead.

5.2.2 *1-affects-n* phenomenon

The *1-affects-n* phenomenon refers to the number of patients affected by a rekeying process due to single changes in healthcare social group membership. This requirement satisfies the scalability of the healthcare system for the large group size, which is more critical for wireless mobile environments. The high number of patients in the social group involved in rekeying process on each event is a hurdle for the scheme to scale the scope of key management to very large m-healthcare social networks. Due to the intuitive characteristics of body area networks in terms of wireless bandwidth limitation, high affected members consume enormous wireless resources which results in failure in receiving the keying materials updates by some members on each event while contributing to delays in distributing the social group content.

It can easily be seen from Figure 11, and Figure 12, the TSGC shows the high number of affected patients who need to receive the new keying materials during an event. The reason is that the TSGC does not provide any protocol for mobility event and treats such an event as a leave in the old area and a join in the visited area. Thus, the entire group members are influenced twice. The average number of member affected by rekeying processes increases in this scheme significantly when the group size grows up.

Figure 11. Impact of inter arrival variation on $1\text{-affects-}n$ behavior overhead.

The average of affected member in the SEGUE is less than the TSGC due to the use of mobility list for keeping track of moving members, which eliminates the needs of performing rekeying process in the old area. Thus, the patients residing in the old area are not affected by the mobility event. Moreover, the rekeying process is performed in the visited area as long as either the mobile patient is not on the mobility list of the *AKM* of the visited area or its join time is after the last update time of the *AEK* of visited area.

Figure 12. Impact of membership duration variation on the average number of affected patient.

6 Conclusion

The m-healthcare information system can greatly improve the benefit of patients and hospitals, not only providing better quality of patient care, but also providing a decentralized, and organized way that the authorized patients to socially interact with each other in order to share their health conditions and medical experience for mutual support and comfort. However, it brings about series of security challenges, especially how to preserve the secrecy of patients' personal health information from various attacks in the wireless mobile network where the mobile patients can change their locations during different time periods while remaining in the session. In this paper, a new privacy-preserving scheme has been proposed using secure group communication to maintain secrecy of patients' personal health information transferred over m-healthcare systems. Meanwhile, the mobility of patients between different areas of a healthcare domain has been taken into consideration and treated with the minimum rekeying messages. The proposed scheme used a managing list called *PMOL* for effectively performing key management and authentication phase, as well as avoiding renewing the *TEK* during move events. By delegating the authentication phase of mobile patients to the intermediate *AKMs*, the domain key manager of a m-healthcare system is given scalability and preserved from bottleneck because of reducing the signaling loads at the core domain. Simulation results depicted the SEGUE far outperforms pervious schemes in terms of rekeying overhead and number of affected patients by rekeying process.

Acknowledgement

The authors would like to acknowledge the financial support of eScience fund 01-01-03-SF0786.

Compliance with Ethical Standards

Disclosure of potential conflicts of interest: We declare that we have no financial and personal relationships with other people or organizations that can inappropriately influence our work, there is no professional or other personal interest of any nature or kind in any product, service and/or company that could be construed as influencing the position presented in, or the review of, the manuscript.

Research involving Human Participants and/or Animals: This article does not contain any studies with human participants performed by any of the authors.

Informed consent: Informed consent was obtained from all individual participants included in the study.

REFERENCES

1. Oh H, Rizo C, Enkin M, Jadad A (2005) What is eHealth (3): a systematic review of published definitions. *Journal of medical Internet research* 7 (1):e1
2. Sharp M, O'Sullivan D (2017) Mobile medical apps and mHealth devices: a framework to build medical apps and mHealth devices in an ethical manner to promote safer use-a literature review. *Stud Health Technol Inform* 235:363-367
3. Shuren J, Patel B, Gottlieb S (2018) FDA regulation of mobile medical apps. *Jama* 320 (4):337-338
4. Baxter C, Carroll J-A, Keogh B, Vandelanotte C (2020) Assessment of Mobile Health Apps Using Built-In Smartphone Sensors for Diagnosis and Treatment: Systematic Survey of Apps Listed in International Curated Health App Libraries. *JMIR Mhealth Uhealth* 8 (2):e16741. doi:10.2196/16741
5. Elbert NJ, van Os-Medendorp H, van Renselaar W, Ekeland AG, Hakkaart-van Roijen L, Raat H, Nijsten TE, Pasmans SG (2014) Effectiveness and Cost-Effectiveness of eHealth Interventions in Somatic Diseases: A Systematic Review of Systematic Reviews and Meta-Analyses. *J Med Internet Res* 16 (4):e110. doi:10.2196/jmir.2790
6. Dorsey ER, Topol EJ (2016) State of Telehealth. *New England Journal of Medicine* 375 (2):154-161. doi:10.1056/NEJMra1601705
7. Cornet VP, Holden RJ (2018) Systematic review of smartphone-based passive sensing for health and wellbeing. *Journal of biomedical informatics* 77:120-132
8. Ali EE, Chew L, Yap KY-L (2016) Evolution and current status of mhealth research: a systematic review. *BMJ Innovations* 2 (1):33-40. doi:10.1136/bmjinnov-2015-000096
9. Chen M, Gonzalez S, Leung V, Zhang Q, Li M (2010) A 2G-RFID-based e-healthcare system. *IEEE Wireless Communications* 17 (1):37-43. doi:10.1109/MWC.2010.5416348
10. Campion Jr TR, Edwards AM, Johnson SB, Kaushal R (2013) Health information exchange system usage patterns in three communities: Practice sites, users, patients, and data. *International Journal of Medical Informatics* 82 (9):810-820. doi:<http://dx.doi.org/10.1016/j.ijmedinf.2013.05.001>
11. Feng W, Zhang LN, Li JY, Wei T, Peng TT, Zhang DX, Guo ZX, Wang WS (2020) [Analysis of special ehealth service for corona virus disease 2019 (COVID-19) pneumonia]. *Beijing Da Xue Xue Bao Yi Xue Ban* 52 (2):302-307
12. Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K (2018) Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems* 78:659-676. doi:<https://doi.org/10.1016/j.future.2017.04.036>
13. Ahmed SM, Rajput A (2020) Chapter 16 - Threats to patients' privacy in smart healthcare environment. In: Lytras MD, Sarirete A (eds) *Innovation in Health Informatics*. Academic Press, pp 375-393. doi:<https://doi.org/10.1016/B978-0-12-819043-2.00016-2>
14. Industry ARC (2020) *Wireless Sensor Network Market - Forecast(2020 - 2025)*. Industry Analytics Research Consulting.
15. Mordor Intelligence (2019) *Wireless Sensors Network Market - Growth, Trends, and Forecast (2020 - 2025)*. <https://www.mordorintelligence.com/industry-reports/wireless-sensor-networks-market>. Accessed 22/06/2020 2020
16. Kumari P, Mathew L, Syal P (2017) Increasing trend of wearables and multimodal interface for human activity monitoring: A review. *Biosensors and Bioelectronics* 90:298-307. doi:<https://doi.org/10.1016/j.bios.2016.12.001>
17. Cisco Co. (2020) *Cisco Annual Internet Report (2018–2023) White Paper*. <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>. Accessed 22/06/2020 2020
18. Hilty DM, Chan S, Torous J, Luo J, Boland RJ (2019) Mobile Health, Smartphone/Device, and Apps for Psychiatry and Medicine: Competencies, Training, and Faculty Development Issues. *Psychiatric Clinics* 42 (3):513-534. doi:10.1016/j.psc.2019.05.007
19. Sun W, Cai Z, Li Y, Liu F, Fang S, Wang G (2018) Security and Privacy in the Medical Internet of Things: A Review. *Security and Communication Networks* 2018:5978636. doi:10.1155/2018/5978636
20. Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S (2017) Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal* 18 (2):113-122. doi:<https://doi.org/10.1016/j.eij.2016.11.001>
21. Tang W, Ren J, Zhang Y (2019) Enabling Trusted and Privacy-Preserving Healthcare Services in Social Media Health Networks. *IEEE Transactions on Multimedia* 21 (3):579-590. doi:10.1109/TMM.2018.2889934
22. Househ M, Borycki E, Kushniruk A (2014) Empowering patients through social media: The benefits and challenges. *Health Informatics Journal* 20 (1):50-58. doi:10.1177/1460458213476969
23. Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS (2016) Cyber threats to health information systems: A systematic review. *Technology and Health Care* 24:1-9. doi:10.3233/THC-151102
24. Yüksel B, Küpçü A, Özkasap Ö (2017) Research issues for privacy and security of electronic health services. *Future Generation Computer Systems* 68:1-13. doi:<https://doi.org/10.1016/j.future.2016.08.011>
25. Blobel B, Lopez DM, Gonzalez C (2016) Patient privacy and security concerns on big data for personalized medicine. *Health and Technology* 6 (1):75-81. doi:10.1007/s12553-016-0127-5
26. Masood I, Wang Y, Daud A, Aljohani NR, Dawood H (2018) Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure. *Wireless Communications and Mobile Computing* 2018:2143897. doi:10.1155/2018/2143897
27. Gardiyawasam Pussewalage HS, Oleshchuk VA (2016) Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management* 36 (6, Part B):1161-1173. doi:<https://doi.org/10.1016/j.ijinfomgt.2016.07.006>
28. Daghighi B, Kiah MLM, Shamshirband S, Iqbal S, Asghari P (2015) Key management paradigm for mobile secure group communications: Issues, solutions, and challenges. *Computer Communications* 72:1-16
29. Daghighi B, Mat Kiah ML, Shamshirband S, Rehman MHU (2015) Toward secure group communication in wireless mobile environments: Issues, solutions, and challenges. *Journal of Network and Computer Applications* 50 (0):1-14. doi:<http://dx.doi.org/10.1016/j.jnca.2014.11.001>
30. Daghighi B, Kiah MLM, Iqbal S, Rehman MHU, Martin KM (2018) Host mobility key management in dynamic secure group communication. *Wirel Networks* 24 (8):3009-3027. doi:10.1007/s11276-017-1511-4

31. Habib ur Rahman M, Liew CS, Wah TY, Shuja J, Daghighi B (2015) Mining personal data using smartphones and wearable devices: A survey. *Sensors* 15 (2):4430-4469
32. Shrestha NM, Alsadoon A, Prasad PWC, Hourany L, Elchouemi A Enhanced e-health framework for security and privacy in healthcare system. In: 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC), 21-23 April 2016 2016. pp 75-79
33. Lin X, Lu R, Shen X, Nemoto Y, Kato N (2009) SAGE: a strong privacy-preserving scheme against global eavesdropping for ehealth systems. *IEEE Journal on Selected Areas in Communications* 27 (4):365-378
34. Barua M, Liang X, Lu R, Shen X PEACE: An efficient and secure patient-centric access control scheme for eHealth care system. In: Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, 2011. IEEE, pp 970-975
35. Mir O, Nikooghadam M (2015) A Secure Biometrics Based Authentication with Key Agreement Scheme in Telemedicine Networks for E-Health Services. *Wireless Personal Communications* 83 (4):2439-2461. doi:10.1007/s11277-015-2538-4
36. Hsu W-S, Pan J-I (2013) Secure Mobile Agent for Telemedicine Based on P2P Networks. *Journal of Medical Systems* 37 (3):1-6. doi:10.1007/s10916-013-9947-2
37. Kiah MM, Al-Bakri S, Zaidan A, Zaidan B, Hussain M (2014) Design and develop a video conferencing framework for real-time telemedicine applications using secure group-based communication architecture. *Journal of medical systems* 38 (10):1-11
38. Cai Y, Tan J Secure group communication in body area networks. In: Information and Automation, 2008. ICIA 2008. International Conference on, 2008. IEEE, pp 555-559
39. Fichman RG, Kohli R, Krishnan R (2011) Editorial overview-the role of information systems in healthcare: Current research and future trends. *Information Systems Research* 22 (3):419-428
40. Weiner M, Schadow G, Lindbergh D, Warvel J, Abernathy G, Dexter P, McDonald CJ Secure Internet video conferencing for assessing acute medical problems in a nursing facility. In: Proceedings of the AMIA Symposium, 2001. American Medical Informatics Association, p 751
41. Poon CC, Zhang Y-T, Bao S-D (2006) A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine* 44 (4):73-81
42. LeRouge C, Garfield MJ, Hevner AR Quality attributes in telemedicine video conferencing. In: System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on, 2002. IEEE, pp 2050-2059
43. Yu S, Wei Z, Deng RH, Yao H, Zhao Z, Ngoh LH, Wu Y A tele-ophthalmology system based on secure video-conferencing and white-board. In: e-health Networking, Applications and Services, 2008. HealthCom 2008. 10th International Conference on, 2008. IEEE, pp 51-52
44. Rafaei S, Hutchison D (2003) A survey of key management for secure group communication. *ACM Comput Surv* 35 (3):309-329
45. Challal Y, Seba H (2005) Group key management protocols: A novel taxonomy. *International Journal of Information Technology* 2 (1):105-118
46. Chung Kei W, Gouda M, Lam SS (2000) Secure group communications using key graphs. *Networking, IEEE/ACM Transactions on* 8 (1):16-30. doi:10.1109/90.836475
47. Wallner D, Harder E, Agee R (1999) Key Management for Multicast: Issues and Architectures. RFC 2627. Internet Engineering Task Force,
48. Hardjono T, Cain B, Monga I (2000) Intra-Domain Group Key Management Protocol. Internet Engineering Task Force. <http://tools.ietf.org/html/draft-irtf-smug-intragkm-00>.
49. Kim Y, Perrig A, Tsudik G (2004) Group Key Agreement Efficient in Communication. *IEEE Trans Comput* 53 (7):905-921
50. Amir Y, Nita-Rotaru C, Stanton S, Tsudik G (2005) Secure spread: An integrated architecture for secure group communication. *Dependable and Secure Computing, IEEE Transactions on* 2 (3):248-261
51. Mittra S (1997) Iolus: a framework for scalable secure multicasting. *SIGCOMM Comput Commun Rev* 27 (4):277-288
52. Mehdizadeh A, Hashim F, Othman M (2014) Lightweight decentralized multicast-unicast key management method in wireless IPv6 networks. *Journal of Network and Computer Applications* 42 (0):59-69. doi:<http://dx.doi.org/10.1016/j.jnca.2014.03.013>
53. Yun Z, Yuguang F, Yanchao Z (2008) Securing wireless sensor networks: a survey. *Communications Surveys & Tutorials, IEEE* 10 (3):6-28. doi:10.1109/COMST.2008.4625802
54. Zhang J, Varadharajan V (2010) Wireless sensor network key management survey and taxonomy. *Journal of Network and Computer Applications* 33 (2):63-75
55. Ruotsalainen P (2010) Privacy and security in teleradiology. *European Journal of Radiology* 73 (1):31-35. doi:<http://dx.doi.org/10.1016/j.ejrad.2009.10.018>
56. IEEE Standard Glossary of Computer Networking Terminology (1995). IEEE Std 6107-1995:0_1. doi:10.1109/IEEESTD.1995.122636
57. Kiah MLM, Daghighi B (2012) An Implementation of Secure Group Communication in a Wireless Environment. *International Journal of Computer and Electrical Engineering* 4 (6):850
58. Lenstra AK, Verheul ER (2001) Selecting cryptographic key sizes. *Journal of cryptology* 14 (4):255-293
59. Frankel S, Kelly SG (2007) Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. Internet Engineering Task Force,
60. Freier A, Karlton P, Kocher PC (1996) The SSL Protocol: Version 3. Internet Engineering Task Force,
61. Young E, Hudson T (2015) OpenSSL cryptography and SSL/TLS toolkit.
62. Dierks T, Rescorla E (2008) The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246. Internet Engineering Task Force,
63. Henderson T, Riley G, Floyd S, Roy S (2016) Network Simulator NS-3.
64. Almeroth KC, Ammar MH Collecting and modeling the join/leave behavior of multicast group members in the mbone. In, 1996. IEEE, pp 209-216
65. Almeroth KC, Ammar MH (1997) Multicast group behavior in the Internet's multicast backbone (MBone). *Communications Magazine, IEEE* 35 (6):124-129

Figures

Figure 1

Communication model of m-healthcare system.

Figure 2

Patients mobility management.

Figure 3

Secure m-healthcare social network architecture.

Figure 4

Mobility key management process

Figure 5

Join protocol messages flow

Mobility protocol when a member M moves from area i to area j.

Figure 7

Patient mobility protocol when moving from area i to area j.

Figure 8

An existing patient leaving protocol message flows

Figure 9

Impact of inter arrival variation on rekeying message overhead.

Figure 10

Impact of membership duration variation on rekeying message overhead

Figure 11

Impact of inter arrival variation on 1-affects-n behavior overhead.

Figure 12

Impact of membership duration variation on the average number of affected patient