Addressing a Secure Session-Key Scheme for Mobility Supported e-Healthcare Systems

Pardeep Kumar[1], Pawani Porambage[1], Mika Ylianttila[1]
Centre for Wireless Communication,
University of Oulu, Finland
pradeepkhl@gmail.com, pporamba@ee.oulu.fi,
mika.ylianttila@ee.oulu.fi

Andrei Gurtov[2], Hoon-Jae Lee[3], Mangal Sain[3]
[2]Aalto University, Finland
[3]Dongseo University, Busan, South Korea
gurtov@hiit.fi, hjlee@dongseo.ac.kr,
mangalsain1@gmail.com

***Abstract*—Wireless medical sensor networks, also called e-Healthcare systems, provide mobility to the patients for making life easier and comfortable. However, a secure mobility support is highly desirable to a patient while he/she is moving. In this paper, we discuss security issues facing mobility supported e-Healthcare applications, and propose a secure session-key scheme for addressing security issues. The proposed scheme is suitable for the e-Healthcare systems where a patient is allowed to move and stay connected, securely. The proposed scheme not only establishes a session-key but according to HIPAA acts it also performs robust authenticity for the (mobile) medical sensor, the fixed access point, and the base-station. Our preliminary evaluation shows that the proposed scheme is feasible in-hospital, in-clinic, and homecare environments.**

***Keywords*—Authentication, session-key, security, medical sensor network, e-healthcare, mobility, hospital.**

I. Introduction

During the past years wireless medical sensor network (WMSN) is turning into a promising and intelligent solution for e-healthcare systems. WMSN is a network of low-cost medical sensor devices worn in, on, or planted strategically around the body. The medical sensor devices are resource constraint in nature (i.e., less memory, low computational power, less bandwidth and low battery-powered) and communicate each via wireless links and forward individual physiological vitals to the doctor, remote server or health information systems. The medical sensors include pulse oxy-meter, temperature, respiration, blood pressure and etc [1][2].

Globally a tremendous number of existing research projects or groups are exploring intelligent ways for integrating wireless medical sensor technologies to deliver efficient and affordable healthcare services, such as long-term constant monitoring of patient vital and activity monitoring, etc [3][4]. Indeed, these wireless technologies have introduced several advantages (flexibility, effectiveness, and etc) in traditional healthcare environments, e.g., in-hospital, in-clinic and homecare [5]. However, deploying such wireless technologies in e-Healthcare system comes with newly emerged issues. One of the main issues is how to guarantee the security and privacy of the patients' physiological vitals while a patient is on move within a large medical environment [6]-[8]. In other words, when patients' moves their topology and path changes, regularly. Moreover, health insurance portability and accountability act (HIPAA) provide rules for an individual healthcare record [9]. Thus, in order to (a patient) stay connected securely, a secure session-key scheme is highly required in mobility supported WMSN healthcare applications. A simple mobility scenario in the hospital environments is depicted in fig.1, here a WMSN-enabled patient is allowed to move (e.g., for medical tests in the laboratories or in garden).

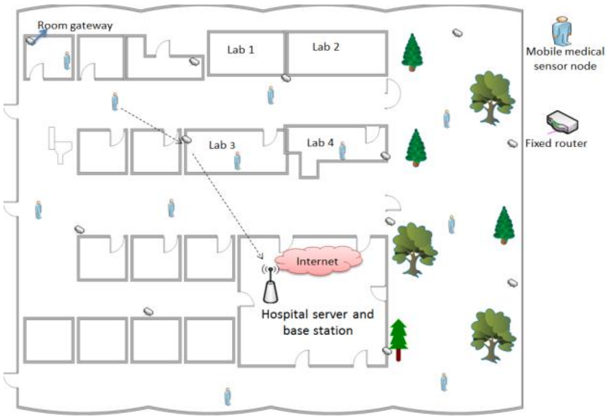

Fig. 1. A WMSN mobility scenario for the hospital environments

In order to provide security in mobility scenario, *Qiu et al* [6] pointed out main issues : (i) a medical sensor is resource constraint device; (ii) a patient needs to leave local room gateway while on move; (iii) a new router/cluster-head needs to ensure that a joining node (i.e., patient) is from its own hospital or at-least not a malicious node/user (i.e., it required strong authentication); (iv) a joining node and a new router needs to establish a secure session key for securing the subsequent communication; (v) the computation cost should be reasonable at mobile node side; and in addition, (vi) the security of e-Healthcare application should be robust against threats/attacks [9]. Moreover, in order to address the secure mobility issues in hospital (or e-healthcare) systems, *Qiu et al* proposed an authentication and key establishment in dynamic wireless sensor networks [6]. In [7], 6LoWPAN-based secure mobility issues have been discussed for hospital applications. The communication cost in [7] is high. However, each protocol has own merits and demerits.

The aim of this research is to address a secure session-key scheme that can provide robust security at reasonable costs and easy to implement in real e-Healthcare systems. The proposed scheme not only establishes a secure session-key between two end parties but it also performs the strong authentication between all the communicating entities. Moreover, it provides desirable and robust security services to the patient (i.e., a mobile node), as per the HIPAA rules [9].

II. Proposed Scheme

In this paper, a hospital scenario is considered where a patient equipped with wireless medical sensor is allowed to move freely within the hospital boundaries. *Note*, now onwards a patient and a mobile node are used interchangeably. In the proposed scheme mainly three entities are involved, i.e., the mobile node (MN), the router (RT), and the base-station (BS). We have made the following assumptions: (i) all the entities have identical cryptosystems (an encryption *(E)*/decryption *(D)*, e.g., AES and a hash function *(h)*, e.g., SHA-1); (ii) each MN shares a unique key (K_{BM}) with BS and each RT shares a common key (K_{BR}) with BS; (iii) RT is a high resources device and it can directly communicate to BS and vice-versa; and (iv) RT and BS are trusted entities.

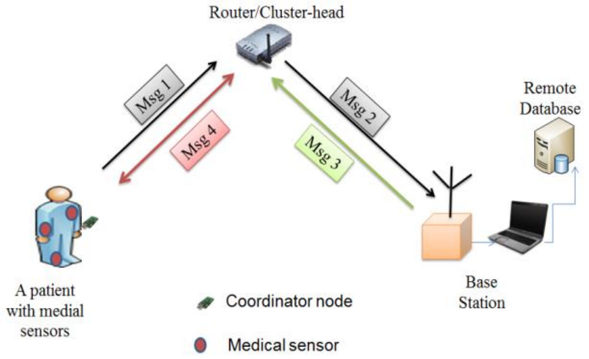

Fig. 2. Architecture and flow of control.

It is also assumed that a mobile node has a secured and trusted connection with the local gateway (i.e., patient's room). However, when a mobile sensor moves from home network (local ward) to the hospital other networks, it needs to be authenticated to the new neighbors (i.e., routers) and establish a secure session key for secure communication. Fig. 2 depicts a simple architecture and flow of the proposed scheme. To stay securely connected, a mobile node first sends a request message to a new router to whom it wants to be connected, as:

$$MN \rightarrow RT: Msg1=\{ID_{MN},C\}; \qquad (1)$$

Here, $C=E_{KBM}[ID_{MN}\,||R0]$, ID_{MN} is the identity of a mobile node and *R0* is a random number which is generated by MN. *E* indicates the symmetric encryption and K_{BM} is a shared key between MN and BS.

Upon receiving the message from MN, RT wants to make sure that the mobile node is from the hospital, it (RT) generates a message, *Msg2*, and sends to the base-station for verifying the authenticity of MN, i.e.

$$RT \rightarrow BS: Msg2=\{ID_{RT},R1,C, H(K_{BR},ID_{RT}||R1||C)\} \qquad (2)$$

Where ID_{RT} is the identity of RT and *R1* is a random number that generated by the router. *H* indicates a keyed-hash function, which is computed over the shared secret (K_{BR}).

After receiving *Msg2*, the base-station performs as:

- Verifies the received keyed-hash *(i.e.,* $H(K_{BR}, ID_{RT}||R1|| C))$. If it is true, RT is a legal router; otherwise it terminates the system.
- In order to perform the authentication of MN, it decrypts the sub-message <*C*>, and obtains $ID_{MN}*$ and *R0**. Now it checks own list and verifies whether $ID_{MN}*$ is a legal node or a revoked node. Generates a session-key *(*i.e., $S_{Key}= h(ID_{MN}||ID_{RT}\,||R0||\,R2))$ and sends a message *(Msg3)* to the router, i.e.

$$BS \rightarrow RT: Msg3=\{ID_{BS}, E_{KBR}\,[ID_{BS},ID_{MN},R0,R1,R2, S_{Key}]\} \; (3)$$

Here, ID_{BS} is identity of BS, *R2* is a BS generated random number, *E* is a symmetric encryption cryptosystem and K_{BR} is a shared key between the base-station and the router.

Upon receiving *Msg3*, RT decrypts the message using K_{BR} key and obtains $ID_{BS}*$, $ID_{MN}*$, *R0**, *R1**, *R2**, $S_{Key}*$; and it performs the following:

- Verifies *R1*=R1* and $ID_{BS}* = ID_{BS}$, if yes, BS is legal.
- Computes: $P\ =h(ID_{MN}||R0)$ sends a message *(Msg4)* to MN, i.e.

$$RT \rightarrow MN: Msg4= \{ID_{RT}, E_P[ID_{RT,}\, R0,R2, S_{Key}]\} \qquad (4)$$

Here, due to the stringent security reasons, *R0, R2* and session-key (S_{Key}) are encrypted using $P\ (=h(ID_{MN}||R0))$and it ensures that the session-key is for a dedicated node and it is confidential.

After getting the message, MN computes: $P' = h(ID_{MN}||R0)$ and decrypts the message using own *P′* and obtains $\{ID_{RT}*, R0*,R2*, S_{Key}*\}$, and performs as:

- Verifies: *R0*=R0* and ID_{RT}*= ID_{RT}, if not then aborts; otherwise, it computes: $S_{Key}=h(ID_{MN}||\,ID_{RT}\,||R0||\,R2))$ and checks: $S_{Key}* = S_{Key}$, if yes, then a secure session-key has been established between the mobile node and the router.

III. Evaluation

A. Security Analysis

We have provided a brief security analysis that can safeguard against popular security threats, as in [4] [5].

Mutual authentication: In the proposed scheme, BS authenticates the identities of MN and RT through *Msg2 (i.e.,* $\{ID_{RT},R1,C,\ H(K_{BR},ID_{RT}||R1||C)\})$. RT authenticates to BS through *Msg3 (i.e.,* $\{ID_{BS}, E_{KBR}\,[ID_{BS},ID_{MN},R0,R1,R2, S_{Key}]\})$. The end user (i.e., mobile node) authenticates a neighboring router through *Msg4 (i.e.,* $\{ID_{RT}, E_P[ID_{RT,}\, R0,R2, S_{Key}]\})$. Hence mutual authentication is performing between all the legal entities. Moreover, due to the fact of no prior trusted connection between the router and the mobile node, our scheme employs on a session-key $(S_{Key}=\ h(ID_{MN}||ID_{RT}\,||R0|| R2))$, which is generated by the base-station. In order to make trust on the session-key, the mobile node needs to recalculate the session-key first based on ID_{MN}, ID_{RT}, *R0,* and *R2*. Then using the recalculated session-key, it verifies the received session-key *(i.e.,* $S_{Key}* = S_{Key}$*)*, if true, then the mobile will only ensure that the router is authorized by the base-station.

Replay attack: Assumed that if an adversary repeats a valid transmission again and again (maliciously), however he cannot succeed in replaying old messages since all the messages *(Msg1, Msg2, Msg3* and *Msg4)* contain fresh one time random numbers *(i.e., R0, R1, and R2)*. Thus, with the (security) property of random numbers, adversary cannot replay previous messages.

Man-In-The-Middle attack (MITM): Generally, wireless communications are easily vulnerable to the MITM attack, where an intruder can setup an independent communication between the communicating entities. if an intruder wants to attempt MITM attacks, he needs to capture the messages and modify the message flow either between the mobile node and the router or between the router and the base-station. However, the proposed scheme can cope with MITM since an intruder doesn't have possession of the secret keys *(K_{BM} and K_{BR})*, he cannot modify the messages *(Msg1, Msg2, Msg3* and *Msg4)*.

Impersonation attack: The proposed scheme is secure against mobile node impersonation attack. For instance, if an attacker attempts to impersonate a legal mobile node, he needs to know the secret key, which is shared between the legal mobile node and the base-station.

B. *Performance Analysis*

Communication Cost: One of the prime concerns in wireless networks is communication cost since it consumes more power than computation cost. However, it is easy to notice from the proposed scheme that it requires only four message exchanges to establish a secure session-key, which are practical in-hospital, in-clinic and homecare scenarios. Whereas the scheme proposed in [6] requires three message exchanges and does not provide robust security. Moreover, the scheme demonstrated in [7] requires twenty-four message exchanges to execute the whole protocol, which is expensive.

Computation Cost: We have compared the computation cost (in bytes) of proposed scheme with [6]. For the message size, we use the 32-bit patient identity *(ID_{MN})*, router ID *(ID_{RT})*, and the base-station ID *(ID_{BS})*. Each 128-bit shared key *(i.e., K_{BM} and K_{BR})*, each 32-bit random numbers *(R0, R1, and R2)* and 128-bit transient session-key (*S_{Key}*). The resulting *Msg1, Msg2, Msg3* and *Msg4* messages are 12, 32, 40, and 16 bytes long. Whereas, the computation cost (in bytes) of [6] using the same parameter as in our proposed scheme, the *request (req), approve (appv)* and *notice* messages are 28, 20, 32 bytes long.

Table 1 shows the computation cost comparisons between our proposed scheme and Qiu et al [6]. This is due to fact that in order to consider the real-deployment in e-Healthcare scenarios and the robust security services requirements as per the HIPAA rules and regulations [9], the proposed scheme incurred more computational and communication cost. In addition, in a close analysis of [6], we have found that Qiu et al scheme would have many security threats, such as, mobile node impersonation attack, router masquerade attack, and message- replay attack. Whereas the proposed scheme provides more robust security against message-replay attack, impersonation attack, MITM attack, and performs strong mutual authentication between all the entities before establishing a session-key.

TABLE I. COMPUTATION COST COMPARISION WITH [6]

	Messages	**Length (Bytes)**
Our proposed scheme	Msg1	12
	Msg2	32
	Msg3	40
	Msg4	16
Qiu et al[6]	Notice	28
	Appv	20
	Notice	32

IV. CONCLUSION

In this work we addressed a secure session-key for e-Healthcare scenario where a patient/mobile needs to be authenticated with new neighboring router. It has been shown that the proposed scheme incurred more computation and communication overhead while it provides more robust security services for such a critical (healthcare) applications where individual life is at high risk. However, an experimental result would have been a better picture to demonstrate the computation and communication cost of the proposed scheme. We will show our test-bed results in longer version of this paper along with more security countermeasures (denial-of-services and node compromised attacks, etc.)

Acknowledgement

The work has been funded by Tekes under project MAMMotH and Academy of Finland project SEMOHealth. Fifth and Sixth authors was funded by national research foundation of Korea (NRF) (no.: 2013-071188) and BB21 project of Busan metropolitan city.

REFERENCES

[1] M. R. Yuce, "Implementation of Wireless Body Area Networks for Healthcare Systems," Sensors and Actuators A: Physical, 162 (2010).

[2] Caldeira et al., "Toward Ubiquitous Mobility Solutions for Body Sensor Networks on HealthCare," IEEE Communications Magazine, 2012.

[3] H. Alemdar and C. Ersoy, "Wireless Sensor Networks for Healthcare: A Survey, " Computer Networks, pp. 2688-2710, 2010.

[4] A. Pantelopoulos, and N. G. Bourbakis, "A Survey on Weareable Sensor-based Systems for Health Monitoring and Prognosis," IEEE Trans. on Systems, Man, and Cybernetics, vol. 40, no. 1, January 2010.

[5] Lin et al, "SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth Systems," IEEE Journal on Selected Area in Communications, vol. 27, No.4, May 2009.

[6] Qiu et al., "Authentication and key establishment in dynamic wireless sensor networks," Sensors 2010, 10, pp. 3718-3731.

[7] Jara et al, "HWSN6 Hosptial wireless sensor networks based on 6LoWPAN technology: mobility and fault tolerance management," in the Proceeding of International Conference on Computational Science and Engineering, 2009, pp. 879-884.

[8] Jara et al., "Intra-mobity for Hospital wireless sensor networks based on 6LoWPAN," in the prodeeding of 6th International conference on wireless and mobile communication (ICWMC'10), 2010, pp. 389- 394.

[9] -- "An introductory resource guide for implementing the Health Insurance Prortability and Accountability Act (HIPAA) Security Rules," National Institute of Stantdard and Technology, U.S. Department of Commerce, October 2008.