A Hybrid and Fast Authentication Protocol for Handoff Support in e-Healthcare Systems among WSNs

Ndibanje Bruce[1]
[1]Department of Ubiquitous IT
Graduate School of Dongseo University,
Sasang-Gu, Busan 617-716, Korea
bruce.dongseo.korea@gmail.com

Gi-Hyun Hwang[2], Hoon Jae Lee[2]
[2]Division of Computer and Engineering
Dongseo University
Sasang-Gu, Busan 617-716, Korea
hwanggh@gdsu.donseo.ac.ke,hjlee@dongseo.ac.kr

***Abstract*—Ubiquitous Technologies in eHealthcare systems are playing a vital role to perform a non-stop monitoring of patients' health in hospitals or outpatient. The application of eHealthcare System towards wireless sensor networks such as ECG, voice over IP and audio/video conferencing, location-aware and ambient intelligence require the support of mobile nodes or node groups. Furthermore, medical staff moves close to patients and collects their monitoring body parameters through their wireless devices. Thus, in such situation, the lack of network connectivity is not admissible or should at least be time bounded, e.g. mobile nodes cannot be disconnected from the rest of the WSN for an undefined period of time. In this paper, we propose a hybrid and fast authentication protocols that support fast hand-off for real-time applications aforementioned. The proposed protocol is based on RSS measurement and on public key cryptography with Diffie-Hellman algorithm which provides security against both leakage-resilience of private keys on untrustworthy. The performance analysis shows that our proposed authentication protocols are efficient and resilient to various kinds of attacks.**

***Keywords*—eHealthcare; handover; handoff; authentication protocol; attacks; hybrid**

I. Introduction

With the rapid growth of Ubiquitous Technologies, huge applications have been proposed and others are still going on under academic or industrial researches. The eHealthcare system is one of the topics supported by different ubiquitous technologies. Via a network it is wirelessly possible to reach each one of the patients' nodes ubiquitously (anytime anywhere) as long as a network terminal is accessible. Sensitive data of patients such as physiological or physical health parameters are sensed, collected and processed by small sensor nodes that are placed on patients [1-2].

However, supporting reliable and real-time communications for eHealthcare Wireless Sensor Networks under nodes' mobility is not practical using contemporary WSN protocols; since they don't permit to fulfill reliability and real-time requirements under physical mobility.

Hence, in this paper, we have been addressing the design of an optimal handoff procedure, building upon a hybrid and fast authentication protocol to support the handoff process in WSNs for eHealthcare applications. This protocol is firstly based on RSS measurement where the handoff is triggered when the RSS level of the current AP (Access Point) drops below the minimum value required for successful communication between a client (Mobile Node) and the current AP. Secondly, it is based on public key cryptography with Diffie-Hellman algorithm which provides security against both leakage-resilience of private keys on untrustworthy. We endeavor a reliable continuous monitoring solution of hospitalized patients based on an eHealthcare Systems with mobility support. This work has been compared with existing or similar works and our performance analysis results show that our proposed hybrid and fast authentication protocols is efficient and resilient to various kinds of attacks.

The reminder of this paper is organized as follows. Section II discuss about literature review on authentication protocol for handover support of nodes in WSNs. The proposed work is detailed in Section III. Section IV presents a performance analysis to evaluate our proposed work. Finally, Section V concludes the paper and suggests further research directions.

II. Literature Review

The use of Ubiquitous Technologies with nodes mobility support in eHealthcare environments towards WSNs, allows medical staff and patients to be constantly connected through wireless devices; therefore patients are remaining always under medical control.

Fundamentally, there are two major families of handoff decision. The most common models and heuristic models .The standard techniques are used in cellular, wireless mesh, WLAN, and 6LoWPAN networks [3-7]. These protocols build upon the mobile IPv6 mobility management mechanism. The handoff procedure in mobile IPv6 is initiated by predicting node mobility according to RSS information.

The WSN nodes capability of measurement of received signal strength (RSS) is already covered in the new standard 802.15.4 (Zigbee) [8] defining the physical and medium access control layer of low-cost, low-power devices in unlicensed ISM (Industrial Scientific Medical) band. Among others, the standard defines RSS indicator called RSSI that is used as a metric for radio status in WSN. The 805.15.4 standard allows inexpensive distance estimation without any new special hardware only with simple RSSI circuit. This fact makes the RSSI measurement very attractive for WSN users [9].

978-1-4799-0698-7/13/$31.00 ©2013 IEEE

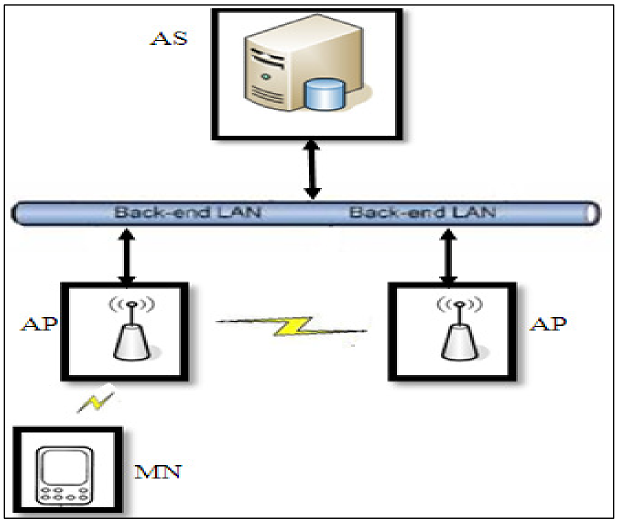

Fig.1. Basic Design of the System Architecture

To all the aforementioned proposed schemes, a handover decision is based on the link quality between the client (Mobile Node) and the current AP is getting signal from. If this value goes below a predefined threshold it is time to trigger the handover procedure before being in an uncovered area. This paper considers this feature to start the handover protocol.

TABLE I. SYMBOL AND DEFINITION USED IN THIS PAPER

Symbol	Definition
ID_{MN}	Mobile Node ID
$ID_{AP}curr$	Current Access Point ID
$ID_{AP}new$	New Access Point ID
ID_{AS}	Authentication Server ID
ID_{U}	Doctor/Nurse (User) ID
PW	Password
CurrT	Current Time
NewT	New Time
ID_{SAS}	Session ID generated by AS
N_{MN}	Random Number of MN
N_{AP}	Random Number of AP
N_{AS}	Random Number of AS
H (.)	Cryptographic hash function e.g SHA1 SHA2
$\oplus$	Bitwise XOR operation
g	Primitive element in the Galois field *GF(p)*
||	Denotes concatenation operation
P	A large prime number
MAC	Media Access Control address

III. A HYBRID AND FAST AUTHENTICATION PROTOCOL FOR HANDOVER SUPPORT IN EHEALTHCARE SYSTEMS AMONG WSNS

This section discusses our solution in the eHealthcare environment. Being in hospitals or homecare, it is nowadays possible to monitor continuously the health status of the patients.

A. *Design of Basic System Architecture*

As illustrated in Figure 1, the design system architecture of our proposed protocol consists of three basic groups: Mobile Nodes, Access Point and Authentication Server (AS).

The procedure of the initial authentication is triggered when the nurse/doctor wants to access the patient's data via a given access point using his wireless mobile device. Before detailed discussion of the proposed scheme, some assumptions are made and are not supposed to be violated while executing the scheme.

The assumptions are mentioned below:

- The medical staffs are registered in the Authentication Server by the Administration of the Healthcare Wireless Sensor Network and each staff member has to keep in secrecy his authentication parameters such as ID and pass word for subsequent utilizations.
- All allowed wireless devices (PDA, Laptops, smart phones, tablets, AP...) are required to be authenticated for the first stage by the current AP. To do so, the Network Administrator configure MAC Address Authentication page. Wireless devices with MAC addresses not on the list are not allowed to authenticate.
- The Network Administrator is to be honest and server is supported not to be compromised otherwise the security of the network and data is in critical state.
- AS is in charge of storage of all authentications information or parameters such as IDs, Nonce, MAC address, and keys.
- The AS and the APs use a secure communication channel to secure their exchanges messages. Such as deployment of his ID to all APs during the registration phase.
- The login phase of the user to the device must be done using his ID and PW provided by the Network Administrator.

B. *Initial Authentical Protocol*

This subsection gives the details of the proposed protocol. As already mentioned in our assumption list, this paper does not deal with the registrations phases of all components to the healthcare wireless network. We assumed that the phase is already done by the Administrator of the Network. Below are the steps of the initial authentication protocol issued when the MN wants to access the network (for his first time).

Step-1: MN sends to the nearest current AP an authentication message MAC based. We assumed all MAC addresses of all allowed devices are pre-configured into all APs. The MN entities compute the following:

MN compute $MN_{Auth}=h\ (ID_{MN}||MAC_{MN})$ and $D_{Auth}=\ (N_{MN}||T_{MN})$ and sends $ReqAuthMssg=E_{KMN}\ (MN_{Auth}\oplus D_{Auth})$ to current AP. Here, T_{MN} is the current time of the MN.

MN sends to AP_{curr}*: {ReqAuthMssg}* (M1)

Ste-2: The current AP decrypts the message and check if the received MAC address of this MN is in the allowed list, then the current AP accepts the authentication request. Otherwise reject the request.

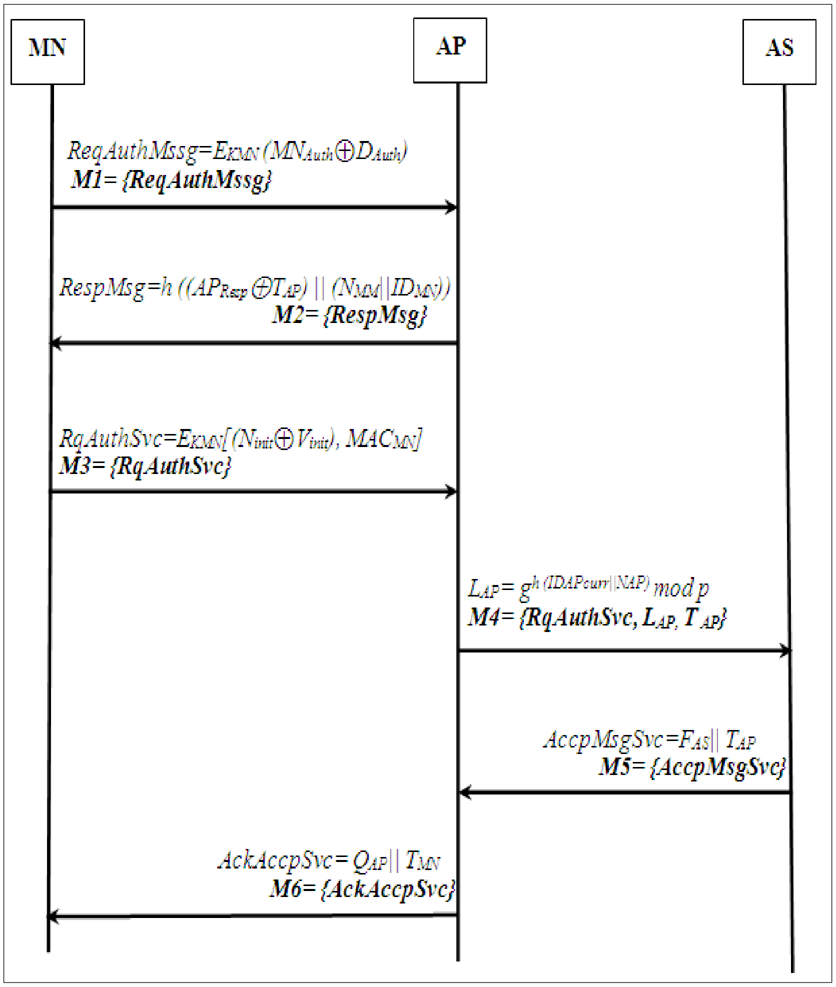
MN
AP
AS
ReqAuthMssg=EKMN (MNAuth⊕DAuth)
M1= {ReqAuthMssg}
RespMsg=h ((APResp ⊕TAP) || (NMM||IDMN))
M2= {RespMsg}
RqAuthSvc=EKMN[(Ninit⊕Vinit), MACMN]
M3= {RqAuthSvc}
LAP= gh (IDAPcurr||NAP) mod p
M4= {RqAuthSvc, LAP, TAP}
AccpMsgSvc=FAS|| TAP
M5= {AccpMsgSvc}
AckAccpSvc= QAP|| TMN
M6= {AckAccpSvc}

Fig.2. Initial Authentication Protocol Flow

Then the current AP prepares the acceptance message and computes the following: $AP_{Resp}=h\ (ID_{APcurr}||N_{AP})$ and send $RespMsg\ =h\ ((AP_{Resp}\oplus T_{AP})\ ||\ N_{MM}||ID_{MN}))$ to MN.

AP_{curr} *sends to MN: {RespMsg}* (M2)

Step-3: This step require the data protection and to detect who is accessing the network by the device MN. Then, Doctor/nurse with his MN sends an authentication request service (*RqAuthSvc*) to the current AP (AP_{Curr}). The MN computes N_{init} and $V_{init,}$ encrypt the message and send to the current AP as follows:

$N_{init}=h\ (IDU||PW)$ and $V_{init}=g^{h\ (ID_{MN}||N_{MN})}\ mod\ p$

$RqAuthSvc=E_{KMN}[(N_{init}\oplus V_{init}),\ MAC_{MN}]$

$MN \longrightarrow APcurr$*: {RqAuthSvc}* (M3)

Step-4: The current AP transmits the request message to the AS to ask if the MN and the user are registered to the networks also, he send his ID and others parameters to be identified to by the AS. The current AP computes L_{AP} and send it together with MN message to AS.

$L_{AP}=g^{h\ (IDAPcurr||NAP)}\ mod\ p$

APcurr forwards to AS: $\{RqAuthSvc, L_{AP,} T_{AP}\}$*(M4)*

T_{AP} is the current time of the AP

Step-5: When the AS receives the message from AP, he validates the time T_{AS} and check if $(T_{AS}-T_{AP})\leq \Delta T$ if yes, then continues to the verification of authentications' parameters of AP and MN otherwise reject. The AS generates his secret key K_{AS} and decrypts the received message in order to check if all entities are registered if yes go to the next step or reject the message performs $D_{KAS}(RqMAuth,\ L_{AP})$, and check the following:

$ID_{MN}=ID_{MN}^{*},\quad MAC_{MN}=\quad MAC_{MN}*,\quad ID_{APcurr}=ID_{APcurr}^{*},$

$ID_{U=}\ ID_{U}^{*}, PW=PW^{*}$

After verification and validation process finished, the AS inform the current AP that the MN and User are legitimate ones. AS prepare an acceptance message service to the AP and also send a session key and session id for this session. AS compute F_{AS} encrypt it and send back to the AP.

$K_{SES}=h\ (ID_{MN}||ID_{APcurr}||N_{MN}||T_{AS}||ID_{SAS}||MAC_{MN})$, T_{AS} is the current timestamp of AS

$F_{AS}=EK_{SES}\ (ID_{AS}||N_{AS})$

$AccpMsgSvc=h\ (F_{AS}//T_{AP})$

AS replies to AP_{curr}*: {AccpMsgSvc}* (M5)

Step-6: Upon receiving the acceptance response message from the AS, the current AP decrypt it and verifies if the AS is the legitimate one, validate the time if not abort the process. Check if $(T_{AP}-T_{AS})\leq \Delta T$ if yes, then continues to the next step otherwise stop the process. $D_{KSES}\ (AccpMsgSvc)$ and mutual authentication: $ID_{AS}=ID_{AS}^{*,}\ ID_{AP}curr=\ ID_{AP}curr^{**},\ T_{AP}=T_{AP}^{*}$ after mutual authentication is done, the current AP then send an acknowledgment message to the MN. First, AP computes the Session Key sharing with MN, and then computes Q_{AP}.

$K_{SES}=h\ (ID_{MN}\ ||N_{MN}||ID_{APcurr}||\ N_{AP}\ ||ID_{SAS}||MAC_{MN})$

$Q_{AP}=EK_{SES}\ (N_{AP}||T_{AP})$

$AckAccpSvc=(Q_{AP}//\ T_{MN})$

AP_{curr} *replies to MN: {AckAccpSvc}* (M6)

Step-7: While receiving the acknowledge message from current AP, the MN performs the mutual authentication by verifying some secret parameters. After the decryption of the arrived message, D_{KSES} *(AckAccpSvc)*, the MN store the ID_{AS} and verify the following:

$ID_{MN}=ID_{MN}^{**},\ T_{MN\,=}\ T_{MN}^{**},\ MAC_{MN}=MAC_{MN}^{**},$

$ID_{APcurr}=ID_{APcurr**}$

If yes, then the MN believes that the current AP is a real one otherwise not.

Now the MN has the right to join the Network and the medical staff can access data using their mobile devices. Moreover, the user ID_U and current AP share the symmetric session key $K_{SES}=h(ID_{MN}||N_{MN}||ID_{APcurr}||N_{AP}||ID_{SAS}||MAC_{MN})$ for performing further subsequent operation during a session.

As a result, a legitimate user can communicate with real access point and access the data through the eHealthcare network. As described in above sections, we aim to perform a handover process while the medical staff is moving into the cover area of the eHealthcare wireless sensor network. The next subsection describes the handover process of the MN to the new AP.

C. *The Handover Processs*

The handover protocol is invoked when the user want to switch to the new AP from the old one(current AP).

Step-1: The MN first computes the received signal strength of the current AP. Let's set *SSth* the signal strength level of required value of RSS to initiate the handover. Thus, when the value of RSS (let set that value below *SSth,* $\underline{RSS}$) of the current AP drops below *SSth,* the handoff is triggered, before the MN moves beyond the coverage area of the current AP. This value can also estimate the distance between those devices. If the mean received signal strength has dropped below *SSth* then the handoff should be performed. The calculation of the *RSS* value is given by the equation 1 as described in [9] where N is the RSS measurement values and *RSSi* represents each single measurement.

$$\overline{RSS}=\frac{1}{N}\sum_{1=1}^{N}RSSi \tag{1}$$

Step-2: After triggering the handover process, the authentication protocol now takes place from the current AP with $\underline{RSS}<SSth$ to new AP with strong signal of RSS. The MN then sends the request handover message to new AP with the following:

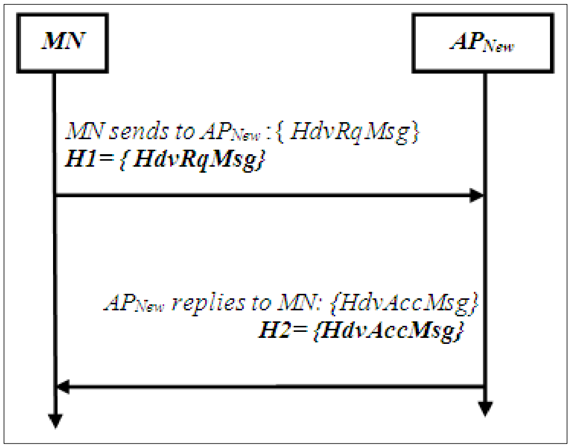
MN
APNew
MN sends to APNew :{ HdvRqMsg}
H1= { HdvRqMsg}
APNew replies to MN: {HdvAccMsg}
H2= {HdvAccMsg}

Fig.3. Handover Protocol Flow

MN computes $MN_{Hdv}=h(ID_{MN}\oplus MAC_{MN})$ *and* $K_{SESS}=g^{h(NMN||IDSAS||IDAPnew||)}$ *mod p,* the MN send the *HdvRqMsg* to $\text{AP}_{\text{New.}}$

$HdvRqMsg=EK_{SESS}\ \{MNHdv,\ TNewMN\}$

MN sends to AP_{New} :{ *HdvRqMsg* } (H1)

Step-3: The New AP decrypts the message and validate the time, check the following: $MAC_{MN}=MAC_{MN}*$ and then $AP_{New}=AP_{New}*$ if yes go to next step otherwise abort. The new AP compute $N=h\ (IDAP_{New}\oplus V_{APnew})$ and send the handover access message to the MN. $HdvAccMsg=EK_{SESS}\ (N,\ T_{APNew})$

AP_{New} *replies to MN: {HdvAccMsg}* (H2)

Step-4: While receiving the access handover message, the MN decrypts the message and validates the time, check if the secrets parameters much or not: $IDAP_{New=}\ IDAP_{New**,}\ ID_{MN}=ID_{MN}^{**},\ T_{MN\,=}\ T_{MN}^{**},\ MAC_{MN}=MAC_{MN}^{**}$, if yes continue to enjoy the network service otherwise abort.

IV. Performance Analysis

We compare the proposed protocol with existing ones [10-12]. The performance of the proposed protocols is based on communication and computation cost using the security parameters involved into the systems. We also perform the security analysis in view of known attacks on protocols.

A. *Efficient Analysis*

Different existing schemes have been analyzed in their communication protocols for the whole communication and confirmation of all entities (*i.e., mobile node, access point and authentication server*). The communication costs give the total number of exchanged messages between all entities from the session initiation until end session. In the proposed protocol, we worked on the speedy feature when the handover process is called then we suggested that the MN communicate directly with the new AP to reduce the exchange messages. This feature makes our protocol more rapid comparing with [10]. Those cases have been carefully taken in consideration by focusing on the behavior of each protocol so that we can see how our protocol is efficient or not. Let's set $E_K (M)$ as encryption of message with the key k, *DK (M)* as decryption of message with the key k, *Chk (P)* checking operations of parameters p, *H (M)* as cryptographic function with hash function of the message m, *HMAC* as computation of message authentication code and hashing, *XOR* as bitwise *XOR* operation. The comparison result is given in the Table II.

TABLE II. INITIAL AUTHENTICATION PROTOCOL : COMPUTATION AND COMMUCATION COST

Operations	Celia et al.[12]	Yang et al.[11]	Proposed
$E_K (M)$	1	2	4
$D_K (M)$	1	2	4
Chk (P)	3	3	4
HMAC or HMIC	1	8	N/A
XOR	N/A	N/A	3
H (M)	1	4	9
COM COST	5	14	6

N/A: No-Applicable

The initial authentication protocol requires some operations to establish the communication among entities. The result from the Table II shows that apart from *chk (P)* which needs 3 times, others operations needs 1time to accomplish their jobs [12]. The protocol in [11] requires 2 times for $E_K (M)$ and $D_K (M)$, 8 times to perform *HMAC* operation, 3 times for *chk (P)* and 4 times to perform *H (M)*. The proposed protocol required 3 times for *XOR* , 9 times for *H(M)* and 4 times to perform other operations. In term of computation cost our proposed protocol requires 6 messages to fulfill the initial authentication protocol while others need 5 and 14 messages. From this comparison, we can see that the proposed protocol require much time than others to perform the operations which makes strong and resilient to attacks.

TABLE III. HANDOVER PROTOCOL : COMPUTATION AND COMMUCATION COST

Operations	Celia et al.[12]	Yang et al.[11]	Proposed
$E_K (M)$	0	1	2
DK (M)	0	1	2
Chk (P)	0	2	2
HMAC or HMIC	6	2	N/A
XOR	N/A	N/A	2
H (M)	0	N/A	3
COM COST	3	5	2
COM with AS	YES	YES	No

N/A: No-Applicable

The result of the performance analysis of the handover protocol in the Table III indicated that only HMAC needs 6 times in [12] but other operations don't need to be computed. In [11], the operations $E_K (M)$ and $D_K (M)$ need 1 times, 2 times for *chk (P)* and *HMIC* while in the proposed protocol we need 3 times for *H (M)* and 2 times to perform others. The total exchanges messages to complete the whole handover process are 2 while other protocols use 3 and 5 messages. The analysis of the comparison handover protocol in the last line of Table III shows that during the process, our protocol does not deal with AS while others require to communicate with AS, thus the more AS is requested the more the handover protocol is slow. Regarding this, our protocol is faster than the compared ones.

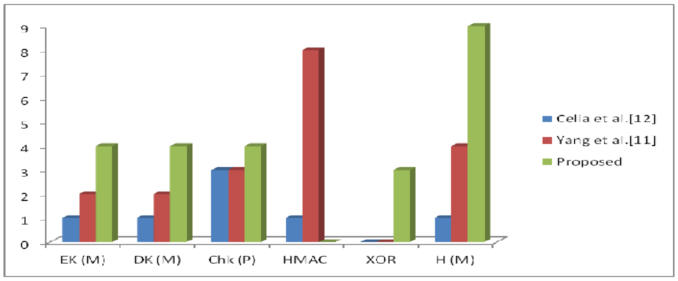

Fig.4. Total Computation Cost (Initial Authentication Protocol)

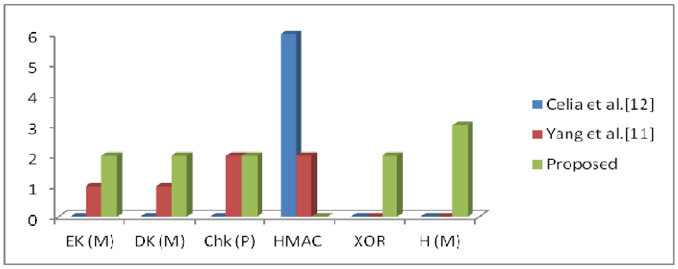

Fig.5. Total Computation Cost (Handover Protocol)

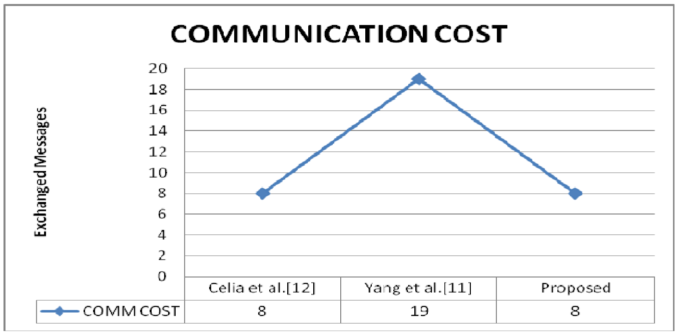

Fig.6. Total Communication Cost (Exchanged Messages)

Figures 4 and 5 show the total time needed to perform all the operations during initial authentication protocol and handover protocol respectively, while Figure 6 describes the total messages exchanged for the whole communication and confirmation of all entities used in the protocols aforementioned. In Figure 4 we can see the pick of *HMAC* for the proposed protocol in [11] and pick of *H(M)* for our proposed protocol both picks during initial authentication protocol. Figure 5 gives a pick at *HMAC* durring handover protocol in [12]. Finally, the communication cost in Figure 6 gives a pick in [11] because their protocol required more exchangeed messages than others.

B. Security Analysis

Masquerade Mobile Node Attack : The protocol is against this attack in its concept. We assume that an attack wants to access the network using his mobile device. In this case, he will attempt to connect his device by sending the *{ReqAuthMssg}.*Without any problem the current *AP* will reject the request because ok unknown device (*ID* and *MAC*'s device are unregistered).

Source Substitution Attack: This attack is defined by Diffie *et al.* [13] where the attack can use another entity's public key and play with it to obtain a certificate in the name of the attacker for that public key value. Thus, it permits the attacker to impersonate the system to be the signer of data. Similar to this concept, an attack can intercept *{ReqAuthMssg}* and then re-use it claiming to be the legitimate owner. In this scenario, the system will compute all parameters and check if the device is registered which is true then continuing to check, the system will see that $D_{Auth}= (N_{MN}||T_{MN})$ contains the nonce (N_{MN}) already used at time (T_{MN}) finally void this process.

Mutual authentication Protocol: The proposed protocol provides the mutual authentication protocol for the whole communication process between all entities (*mobile node, access point and authentication server).* This security feature is against known attack like compromised devices or replay attack. In Step-1, the AP checks if the device is registered in his data base, Step-5, The AS verify the authentication parameters of the AP and MN, Step-6 and Step-7, the AP and MN processes to the mutual authentication respectively to check if the entity is the legitimate one.

Session key establishment: A session key, K_{SES} is established between the communicating entities after authentication process. This key is different in each session and cannot be replayed after the session expires.

V. Conclusion

This paper proposed a hybrid and fast authentication protocol to support handover process applied to e-Healthcare system using wireless devices. The main concept of hybrid function is based on the mixture of the two main functions detailed in this paper. A part the cryptographic function, we have described another vital function (signal strength) to trigger the handover process. In addition it is called fast protocol because the AS is not involved into the handover process, and also the access point and AS are connected via back-end LAN, which is a wired network with very high speed. Furthermore, the results of the efficiency and security analysis demonstrate that the proposed protocols are efficient and resilient to various attacks. For the future work, there is a need of implementation experiment of the protocols in order to evaluate their feasibility for the purpose of eHealthcare applications.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. And it also supported by the BB21 project of Busan Metropolitan City.

References

[1] H. Ghasemzadeh, R. Jafari, and B. Prabhakaran, "A Body Sensor Network With Electromyogram and Inertial Sensors: Multimodal Interpretation of Muscular Activities," in IEEE Transactions on Information Technology in Biomedicine, vol. 14, Issue: 2, 2010, pp. 198 - 206, doi: 10.1109/TITB.2009.2035050.

[2] L. Shu, J. Niu, T. Hara, M. Hauswirth, and S. Nishio, "Integrating Weather Information with Body Sensor Networks for Health Monitoring," in In the 6th International Conference on Body Area Networks (BodyNets 2011), Beijing, China, November 7-8, 2011.

[3] R. Ramjee, K. Varadhan, L. Salgarelli, S. R. Thuel, S. Y. Wang, and T. L. Porta, "HAWAII: a Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks," *IEEE/ACM Trans. on Networking*, vol. 10, No. 3, pp. 396-410, June 2002

[4] S. Pack*, et al.*, "Fast Handoff Support in IEEE 802.11 Wireless Networks," *Communications Surveys & Tutorials, IEEE,* vol. 9, pp. 2-12, 2007.

[5] L. Bo*, et al.*, "A Survey on Mobile WiMAX Wireless Broadband Access]," *Communications Magazine, IEEE,* vol. 45, pp. 70-75, 2007.

[6] Kim JH, Hong CS, Shon T. A Lightweight NEMO protocol to support 6LoWPAN. *ETRI Journal* 2008; 30(5): 685–695

[7] Wong, K. D. and D. C. Cox, "A Pattern Recognition System for Handoff Algorithms", *IEEE Journal on Selected Areas in Communication*, Vol. 18, No. 7, July 2000.

[8] IEEE Standard for Information Technology Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std 802.15.4-2003.

[9] H. Fotouhi, M. Alves, A. Koubaa, and N. Baccou, "On a Reliable Handoff Procedure for Supporting Mobility in Wireless Sensor Networks," in The 9th International Workshop on Real-Time Networks (RTN 2010) in conjunction with the 22nd Euromicro International Conference on Real-Time Systems (ECRTS 2010), Brussels, Belgium, July 6-9, 2010.

[10] P.Morávek, D. Girbau, A.Lazaro, D. Komosný, "Received Signal Strength Uncertainty in Energy-Aware Localization in Wireless Sensor Networks", *9th International Conference on Environment and Electrical Engineering EEEIC in Prague*, May 2010, ISBN:978-1-4244-5371-9

[11] Y.W.Dong L.J.Zhao , W.Ke S.L.Ming "Authentication Protocols to Support Fast Handoff for 802.11s Mesh Networks"**.** *International Conference on Multimedia Information Networking and Security.* IEEE 978-0-7695-4258-4/10 DOI 10.1109/MINES.2010.140, 2010.

[12] C. Li, U.T. Nguyen,"Fast Authentication for Mobility Support in Wireless Mesh Networks" Department of Computer Science and Engineering York University, Toronto, Ontario M3J 1P3, Canada.

[13] W. Diffie, P. C. van Oorschot, and M. J.Wiener, "Authentication and authenticated key exchanges," *Designs, Codes Crypt.*, vol. 2, pp. 107–125, 1992.