Cryptanalysis of an 'Efficient-Strong Authentiction Protocol (E-SAP) for Healthcare Applications Using Wireless Medical Sensor Networks'

Muhammad Khurram Khan[1], Saru Kumari [2], Pitam Singh[3]
[1]Center of Excellence in Information Assurance (CoEIA)
King Saud University, Riyadh, Saudi Arabia
[e-mail- *mkhurram@ksu.edu.sa*]
[2]Department of Mathematics, Agra College, Agra
Uttar Pradesh, India
[e-mail- *saryusiirohi@gmail.com*]
[3]Department of Mathematics, Motilal Nehru National Institute of Technology (MNNIT)
Allahabad, Uttar Pradesh, India
[e-mail- pitams@mmnnit.ac.in]

Received November 20, 2012; revised January 12, 2013; accepted January 16, 2013; published May 31, 2013

Abstract

Now a day, Wireless Sensor Networks (WSNs) are being widely used in different areas one of which is healthcare services. A wireless medical sensor network senses patient's vital physiological signs through medical sensor-nodes deployed on patient's body area; and transmits these signals to devices of registered medical professionals. These sensor-nodes have low computational power and limited storage capacity. Moreover, the wireless nature of technology attracts malicious minds. Thus, proper user authentication is a prime concern before granting access to patient's sensitive and private data. Recently, P. Kumar et al. claimed to propose a strong authentication protocol for healthcare using Wireless Medical Sensor Networks (WMSN). However, we find that P. Kumar et al.'s scheme is flawed with a number of security pitfalls. Information stored inside smart card, if extracted, is enough to deceive a valid user. Adversary can not only access patient's physiological data on behalf of a valid user without knowing actual password, can also send fake/irrelevant information about patient by playing role of medical sensor-node. Besides, adversary can guess a user's password and is able to compute the session key shared between user and medical sensor-nodes. Thus, the scheme looses message confidentiality. Additionally, the scheme fails to resist insider attack and lacks user anonymity.

Keywords: Wireless medical sensor networks, medical professional authentication, medical sensor-node impersonation, insecure session key, password guessing.

http://dx.doi.org/10.3837/tiis.2013.05.002

1. Introduction

Recently, Wireless Medical Sensor Networks (WMSNs) have emerged as a tool to enhance healthcare quality in lesser expenditures than that required using human labor. WMSNs is actually a transmission technology used by health professionals (e.g. doctors, nurses etc.) to procure patient's health related information like blood pressure, body temperature, pulse, ECG etc. To achieve this, medical sensors such as pulse oxi-meter, ECG electrodes, blood pressure sensors, body temperature sensors are deployed to patient's body. These medical sensors transmit patient's physiological information to professionals in a wireless manner. Undoubtedly, this wireless technology has made work possible within instants without any man-power involved. But there is parallel call for proper authentication of professionals seeking patient's information through WMSN, in order to protect patient's private medical data from various adversaries like corrupt persons, private enemies, health insurance professionals, etc. Thus, many researchers are working in this field to fulfill security and privacy requirements of WMSN so as to establish a secure, efficient and reliable healthcare environment.

Along with authentication schemes like [1-3], a series of relevant research has been conducted in the field of wireless sensor networks (WSNs) [4-7] and then in healthcare using WSNs [8-13] and so on. In 2006, Wong et al. [14] presented a dynamic user authentication scheme for WSNs. In 2007, Tseng et al. [15] demonstrated replay attack and impersonation attack on [14]; and proposed a remedy [15] to mend these attacks. In 2009, Das [16] pointed out the drawback of maintaining a password table in [14-15] and also proposed a solution in terms of two-factor authentication scheme using a smart card protected with a password. In 2010, Khan et al. [17] found that Das's scheme [16] suffers from insider attack and does not facilitate users to change their password; and proposed a scheme to improve on these security loopholes. In 2012, P. Kumar et al. [17] asserted that most of the schemes like [16-17, 19-20] proposed for WSNs provide nominal security and involve sufficiently high computation and communication cost. Besides, P. Kumar et al. felt dearth of strong user authentication protocol in wireless healthcare applications for which they proposed their so called "E-SAP Efficient-Strong Authentication Protocol for Healthcare Applications Using WMSNs" [17]. Their scheme allows users to freely change the password and establishes session key between user and medical sensor-node. They claimed that their scheme is superior to other existing protocols regarding cost and effectiveness; and most of the prevalent attacks.

Unfortunately, this paper finds that P. Kumar et al.'s scheme suffers from smart card loss attack and its various consequences like user impersonation attack, password guessing attack, insecure session key generation between user and medical sensor-node, and attack on user's anonymity. We show that disclosure of user's identity not only give chance to many unauthorized/illegal entities to access patient's physiological information, and also creates un-necessary problems for a valid professional. While going through the scheme, we also come across the insider attack, medical sensor-node impersonation attack, and improper mutual authentication.

The remainder of this paper is organized as follows. Section-2 briefly describes WMSN architecture and its utility in healthcare services. Section-3 reviews P. Kumar et al.'s scheme. Section-4, presents cryptanalysis of P. Kumar et al.'s scheme. Finally, Section-5 concludes the paper. Throughout the paper, professional and user is used interchangeably.

2. WMSN Architecture and its Utility in Healthcare Services

The network architecture for WMSN is presented in **Fig. 1**. It consists of four parties:

- Users (medical professionals) seeking access to patients' physiological data.
- Medical sensors-nodes implemented on patients' body.
- Gateway (*GW*)-node playing key role between user and medical sensors.
- Patients being monitored by medical professionals through medical sensors.

Only first three parties are active participants in an authentication procedure. Whenever a users (professionals) needs to access patients' physiological data, he sends request to the *GW*-node. The *GW*-node forwards this request to the medical sensors-nodes. Then, the medical sensors-nodes respond to the user's request.

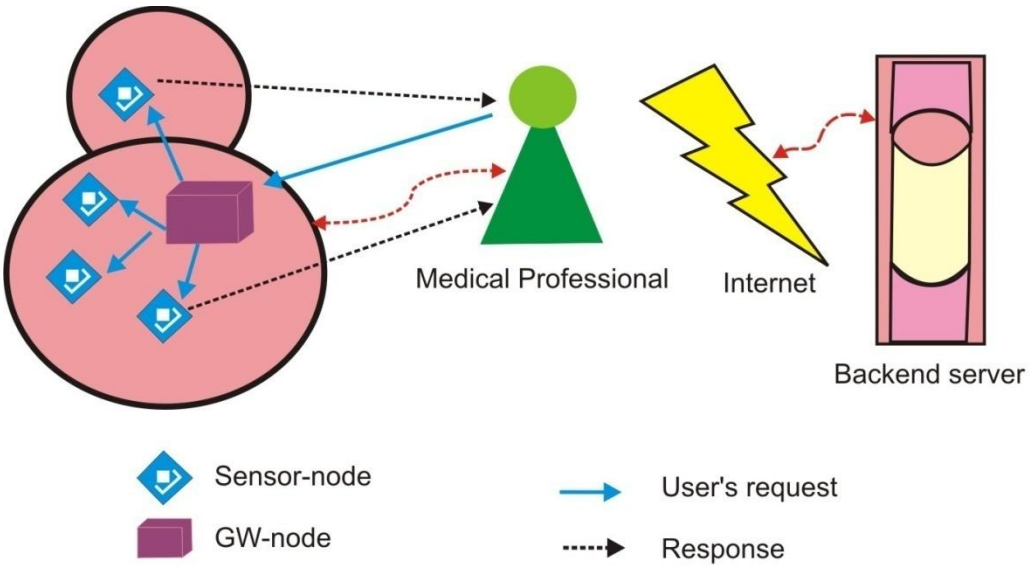

Fig. 1. WMSN Architecture

Utility of WMSN in Healthcare

- Improved healthcare services,
- Regular and un-interrupted patients' monitoring,
- Saves time and cost effective,
- Preserves private and sensitive data of patients' from adversaries, *etc*.

3. Review of P. Kumar et al.'s Scheme

The scheme consists of five phases namely, user (professional) registration phase, patient registration phase, login phase, authentication phase and password change phase. Each of these phases is described along with **Fig. 2** and **Fig. 3** briefly depicting the user registration phase and login-authentication phase respectively. Initially, the Gateway (GW)-node selects three long-term secret keys $\{J, K, Q\}$, where each one is of length 256. Besides, the GW-node shares a long-term secret key $SK_{gs} = h(Q||IDg)$ with medical sensor-node S_n using some key agreement method [21-22], where IDg is the identity of GW-node.

3.1 User (Professional) Registration Phase

In this phase, U the user (professional) registers itself to the GW-node at the hospital registration center, as described below:

1) User submits his chosen identity and password $\{ID_u , PW_u\}$ to GW-node using secure channel.
2) On receiving $\{ID_u, PW_u\}$, the GW-node computes $C_{ug} = E_J(ID_u||ID_g)$ and $N_u = h(ID_u \oplus PW_u \oplus K)$
3) GW-node stores $\{h(.), C_{ug}, N_u, K\}$ into a SC and issues $SC = \{h(.), C_{ug}, N_u, K\}$ to U, where K is a long-term GW-node secret.

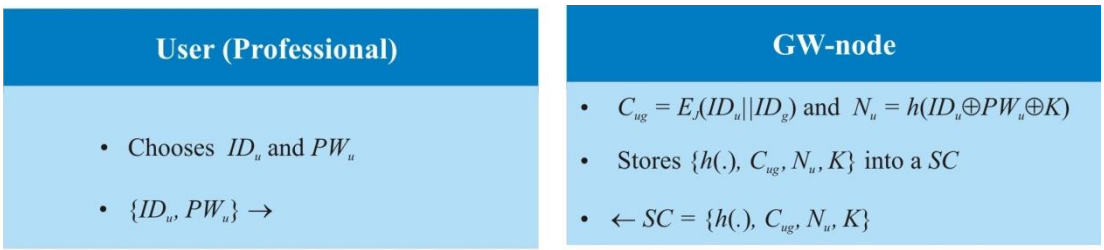

Fig. 2. User (Professional) Registration Phase of P. Kumar et al.'s Scheme

3.2 Patient Registration Phase

In this phase, a patient registers himself at the hospital registration center [23]. Patient submits his/her name to the registration center. After receiving patient's name the registration center selects a suitable sensor kit (*i.e.*, medical sensor and GW-node) and designates professionals (users). Next, registration center sends patient's identity ID_{pt} and medical sensors kit information (*i.e.*, GW-node, Sensor-node *etc.*) to the designated professionals/users. Then, the technician deploys wireless medical sensors on the patient body area.

3.3 Login Phase

With this phase, a professional roaming into the patients' ward, logins to the GW-node to access the patients' physiological information from the body network. The professional inserts his/her smart card SC into the terminal and keys in $\{ID_u, PW_u\}$. Then, SC verifies the user using stored values and computes the login request as follows:

1) Computes $N_u^* = h(ID_u \oplus PW_u \oplus K)$ to compare $N_u^* = N_u$, if so, then proceeds further; otherwise, terminates this session.
2) Computes $h(ID_u)$ and $CID_u = E_K(h(ID_u)||M||S_n||C_{ug}||T')$, where, M is a random nonce

generated by *SC*.

3) Then *SC* sends login request $\{CID_u, T'\}$ to *GW*-node, where, T' is the current time stamp.

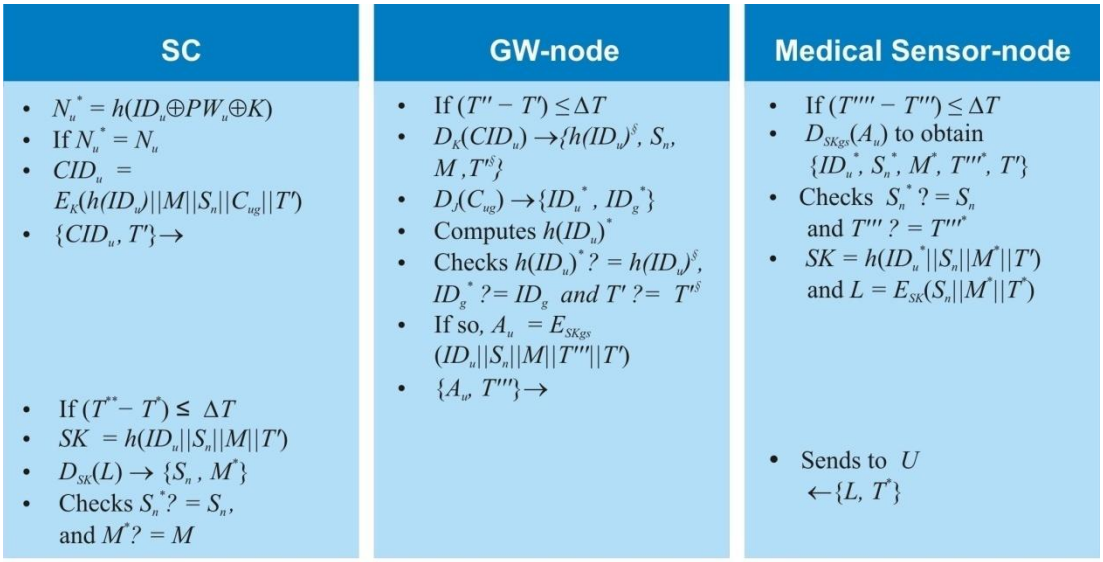

Fig. 3. Login and Authentication Phase of P. Kumar et al.'s Scheme

3.4 Authentication Phase

This phase comes into existence after the *GW*-node receives a login request from a professional. Under this phase, the *GW*-node confirms the legality of *U* and mutual authentication between *U* and sensor-node is achieved. On receiving login request, the *GW*-node performs the following operations to authenticate the user:

1) Checks if $(T'' - T') \geq \Delta T$, if so, rejects the login request; otherwise proceeds further. Here, T'' is the current time of *GW*-node and ΔT is the time interval for expected transmission delay.
2) Decrypts CID_u as $D_K(CID_u)$ to obtain $\{h(ID_u)^{\S}, S_n, M$ and $T'^{\S}\}$. Also, decrypts C_{ug} as $D_J(C_{ug})$ to obtain $\{ID_u^*, ID_g^*\}$.
3) Computes $h(ID_u)^*$ and compares $h(ID_u)^* = h(ID_u)^{\S}$, $ID_g^* = ID_g$ and $T' = T'^{\S}$, if each is correct, then accepts the login request; otherwise terminates the login session.
4) Computes $A_u = E_{SKgs}(ID_u||S_n||M||T'''||T')$, where T''' is the current timestamp of *GW*-node. Then, the *GW*-node sends $\{A_u, T'''\}$ to the medical sensor-node.

On receiving $\{A_u, T'''\}$ from the *GW*-node, the medical sensor-node performs the following operations:

5) Checks if $(T'''' - T''') \geq \Delta T$, if so, rejects the request. Otherwise proceeds further. Here, T'''' is the current time of the medical sensor-node.
6) The medical sensor-node S_n decrypts A_u as $D_{SKgs}(A_u)$ to obtain $\{ID_u^*, S_n^*, M^*, T'''^*, T'\}$ to make sure that the request has come from the legal *GW*-node.
7) Compares $S_n^* = S_n$ and $T''' = T'''^*$, if not so, aborts the login request; otherwise proceeds further.

8) Computes session key $SK = h(ID_u^* || S_n || M^* || T')$, and $L = E_{SK}(S_n || M^* || T^*)$, where, T^* is the current timestamp of the medical sensor-node. Next, the medical sensor-node sends $\{L, T^*\}$ to the user (professional).

On receiving $\{L, T^*\}$ from the medical sensor-node, the professional performs the following steps:

9) Check if $(T^{**} - T^*) \geq \Delta T$, if so, rejects the request and terminates. Otherwise, it continues with the further process. Here, T^{**} is the current timestamp.
10) SC computes $SK = h(ID_u || S_n || M || T')$ and decrypts L as $D_{SK}(L)$ to obtain $\{S_n, M^*\}$. Compares $S_n^* = S_n$, and $M^* = M$, if so, then a secure session key is established; otherwise not.

3.5 Password Change Phase

With this phase U can change or update the password in SC for which the following steps are performed:

1) First U inserts SC into the terminal and keys in (ID_u, PW_u).
2) SC computes $N_u^* = h(ID_u \oplus PW_u \oplus K)$ and checks if $N_u^* = N_u$. If so, performs the next step otherwise stops the operation.
3) U enters new password $(PW_u)new$.
4) SC computes $(N_u)_{new} = h(ID_u \oplus (PW_u)_{new} \oplus K)$ and replaces N_u with $(N_u)_{new}$.

4. Cryptanalysis of P. Kumar et al.'s Scheme

In this section, we discuss various attacks possible on P. Kumar at al.'s scheme along with **Fig. 4** depicting all vulnerabilities. Suppose an attacker U_a somehow [24-25] extracts values $\{h(.), C_{ug}, N_u, K\}$ from a lost SC. Then, U_a can decrypt CID_u as $D_K(CID_u) = (h(ID_u) || M || S_n || C_{ug} || T')$ to obtain $\{h(ID_u), M, S_n, C_{ug})\}$ from an intercepted login request $\{CID_u, T'\}$ of any user. This is due to the same master key K stored in the SC of each user (professional). Then, U_a can impersonate U at any time to obtain patient's physiological information.

4.1 User Impersonation Attack

To impersonate U, the attacker U_a only needs the current timestamp T_a and a random nonce M_a. Then U_a computes $CID_a = E_K(h(ID_u) || S_n || C_{ug} || T_a)$ and sends $\{CID_a, T_a\}$ to GW- node. Obviously this message will successfully go through GW-node authentication test as it contains valid values $\{h(ID_u), S_n, C_{ug}\}$ and fresh values $\{M_a, T_a\}$.

4.2 Password Guessing Attack

If U_a happens to guess ID_u corresponding to the SC from which he extracts the master key K, then password PW_u of U can also be guessed. For this, U_a guesses PW_a and computes $N_u^* = h(ID_u \oplus PW_a \oplus K)$ and checks if $N_u^* = N_u$. If so, then U_a successfully guesses the PW_u of U. This is considered as total breach of security as U_a possess both SC as well as user's credentials identity and password $\{ID_u, PW_u\}$.

4.3 Lacks User Anonymity

Once U_a possess $h(ID_u)$ of U, he can guess the identity ID_u of U. Therefore, the scheme does not provide user anonymity.

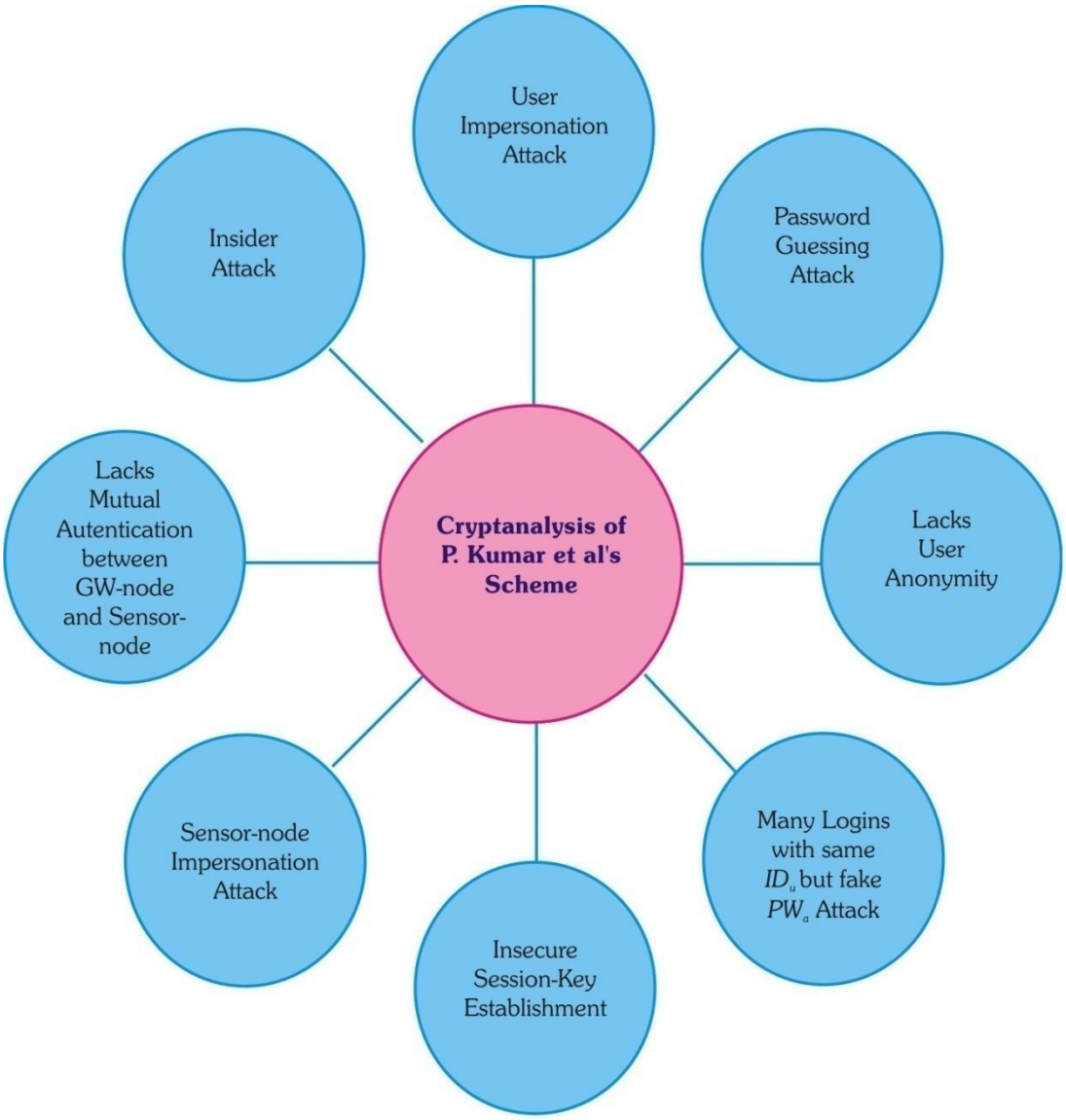

Fig. 4. Attacks on P. Kumar et al.'s Scheme

4.4 Multiple Logged-in Adversaries using *U*'s Identity ID_u but Fake Password PW_a Attack

As just described, the scheme does not support user anonymity; hence U_a can use ID_u to craft other harms to the scheme as described below along with **Fig. 5**.

1) An attacker U_a knowing ID_u of U can register himself to the GW-node by submitting $\{ID_u, PW_a\}$, where PW_a is a fake password chosen by U_a.
2) In turn GW-node will provide U_a a $SC = \{h(.), C_{ug}, N_a, K\}$. Here, $C_{ug} = E_J(ID_u||ID_g)$ and $N_a = h(ID_u \oplus PW_a \oplus K)$

In P. Kumar et al.'s scheme, the role of password lasts up to confirming the legality of user by the *SC*. Afterwards, only identity ID_u of U is used to authenticate U at the *GW*-node. Consequently, there arise two following scenarios, which are also depicted in **Fig. 5**:

- U_a can easily login to the *GW*-node on behalf of U using received $SC = \{h(.), C_{ug}, N_a, K\}$. U_a keys in ID_u and PW_a after inserting the *SC* into the smart card reader. After verifying $\{ID_u, PW_a\}$, *SC* computes and sends the login request $\{CIDa = E_K(h(ID_u)||M_a||S_n||C_{ug}||T_a), T_a\}$ to the *GW*-node. Obviously, the *GW*-node will consider it a valid login request from U as it contains valid ID_u in C_{ug}.
- U_a can distribute the identity ID_u of U among persons who wish to access patient's physiological information in an unauthorized manner for illegal purposes. These persons can re-register themselves to the *GW*-node and access data through S_n. U_a can also achieve this purpose by distributing the values $\{h(ID_u), S_n, C_{ug}\}$ instead of ID_u, among these persons. Then, they can impersonate U as describe in subsection-4.1. If such unauthorized access is detected, then it will raise a question mark on the reliability and truthfulness of the valid user (professional) whose identity ID_u is distributed by U_a.

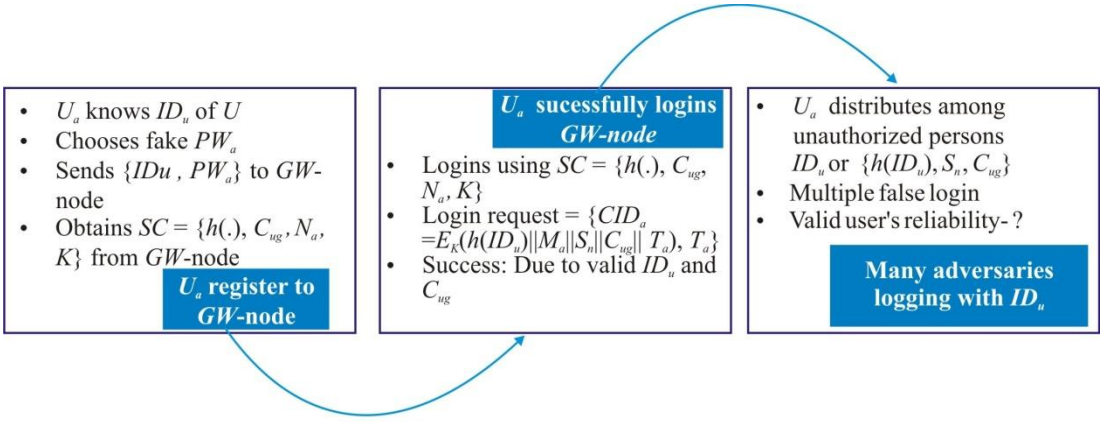

Fig. 5. Multiple Unauthorized Logins with Same Identity

4.5 Insecure Session-Key Establishment

Once U_a retrieves the values $\{h(ID_u), M, S_n\}$ from CID_u, he can compute the session key $SK = h(IDu||S_n||M||T')$ to be shared between the sensor node S_n and user U. For this, U_a can guess ID_u as explained in subsection-4.3. As timestamp T' is available in corresponding intercepted login request $\{CID_u, T'\}$, so now U_a possesses all values $\{ID_u, S_n, M, T'\}$ required to compute $SK = h(ID_u||S_n||M||T'\}$. Thus, the session key *SK* generated in the scheme is insecure. As a result, the scheme fails to provide confidentiality to the air messages between U and medical sensor-node.

4.6 Sensor-Node Impersonation Attack

A planned attacker U_a, as depicted by **Fig. 6**, knowing master key K from lost *SC* can decrypt CID_u's corresponding to as many users as he wants. Further, U_a can guess ID_u corresponding to each retrieved $h(ID_u)$, and tabulate the data $\{h(ID_u), ID_u\}$. From then on, U_a can successfully

impersonate the sensor-node S_n and make fool of a user as explained below stepwise along with **Fig. 6** and **Fig. 7**:

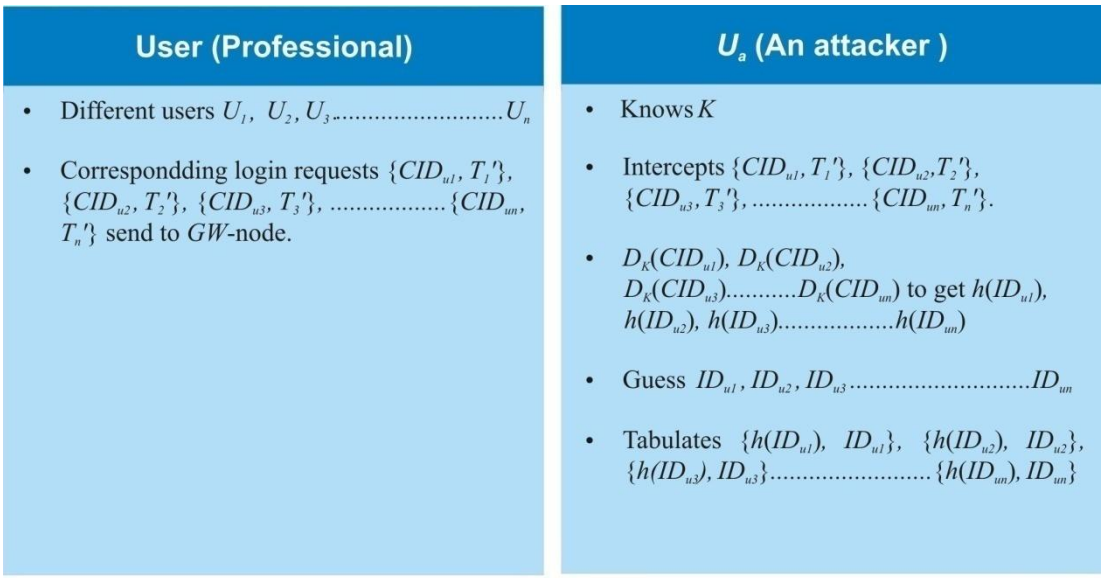

Fig. 6. U_a 's Preparation for Sensor-Node Attack

1) As U_a finds a login request $\{CID_u, T'\}$ on the network, he intercepts and blocks it, quickly decrypts CID_u to see if $h(ID_u)$ included in it is present in the table maintained or not. If not so, then relays the login request to GW-node.
2) If so keeps the login request blocked. Then using ID_u from the tabulated record , values $\{M, S_n\}$ from current decryption, and T' from login request, U_a quickly computes $SK = h(ID_u||S_n||M||T')$.
3) Computes $L = E_{SK}(S_n||M||T_a)$ and sends $\{L, T_a\}$ back to U, where T_a is the current timestamp chosen by U_a.
4) Obviously L will pass the authentication test at user side as it contains valid $\{S_n, M\}$ and fresh timestamp T_a.

Here, notice that SK is the session key established between U and U_a whereas U thinks it to be confidential between him and the sensor node S_n. At the worst, U_a can send fake information about a patient to the user (professional like doctor, nurse, etc). It may result to serious situations in a patient's treatment thereby denying the very purpose of healthcare through wireless medical sensor networks.

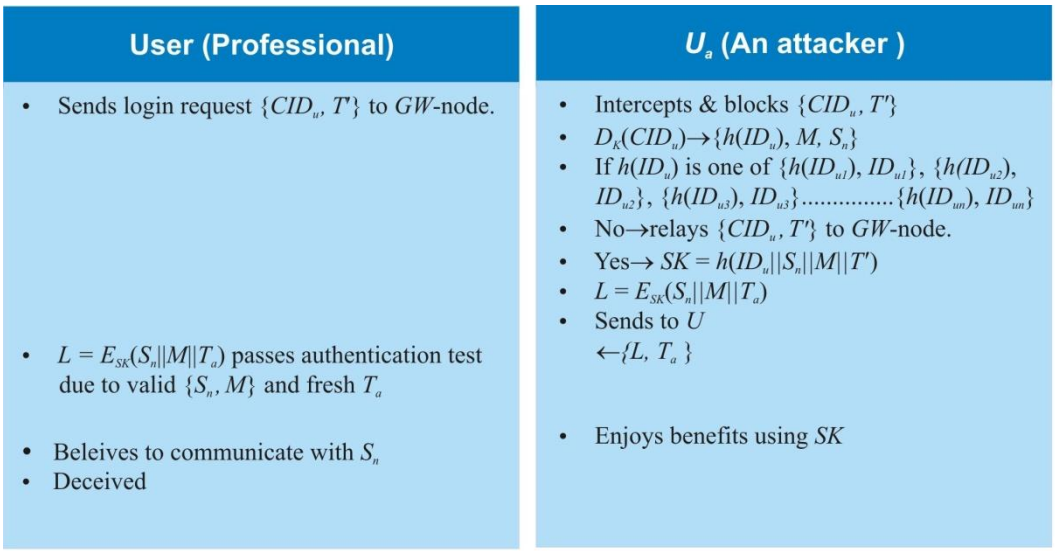

Fig. 7. Sensor-Node Impersonation Attack

4.7 Lacks Mutual Authentication between (i) *GW*-node and Sensor-node (ii) *U* and Sensor-node

In P. Kumar et al.'s scheme, after verifying the login request of U, GW-node computes and sends an ensuring message {A_u, T''} to the required medical sensor-node. Undoubtedly, the equivalence $S_n^* = S_n$ confirms the legality of GW-node to medical sensor-node but reverse is not achieved. Thus, GW-node has no way to ensure itself of connecting with real medical sensor-node. Therefore, the scheme does not provide mutual authentication between GW-node and medical sensor-node.

Besides, the authors claim to provide mutual authentication between medical sensor-node S_n and user U. Mutual authentication between U and S_n is established using the session key $SK = h(ID||S_n||M||T')$. But as shown in subsection-4.5 and subsection-4.6, U_a can compute SK and impersonate S_n respectively. Therefore, the scheme fails to provide mutual authentication between user and medical sensor-node.

4.8 Insider Attack

For convinience users are habituated of using same password for different applications. In P. Kumar et al.'s scheme, U submits his password PW_u in plaintext to GW-node, during registration phase. Thus, the administrator of GW-node has very easy access to each user's password and he can misuse it to masquerade U at terminals where U uses the same password. Though authors assume that hospital registration center is a trusted authority but we opine that it is the trustworthy that breaches the trust. So, it is very risky to submit password PW_u in plaintext, and hence should be avoided.

5. Conclusion

Due to wireless communication technology, WMSNs offer easy functionality for telemedicine. At the same time there is demand for a concrete structured user authentication scheme for WMSNs. Only then the purpose of reliable and efficient healthcare services can be achieved. In this paper, we have analyzed a recently proposed authentication protocol for healthcare services using WMSNs by P. Kumar et al. We have shown that their scheme does not facilitate essential security features like user anonymity, secure session key generation, air message confidentiality, proper mutual authentication between user and *GW*-node, and user and medical sensor-node. Furthermore, we have demonstrated that their scheme does not impart security to user's password as insider attack and offline password guessing attack are applicable on it. Future direction towards this work is to design a robust user anonymous authentication protocol for WMSNs.

References

[1] M.K. Khan, "Fingerprint biometric-based self and deniable authentication scheme for the electronic world," *IETE Technical Review*, vol. 26, no. 3, pp. 191-195, 2009. Article (CrossRef Link)

[2] S. K., M. K. Gupta and M. Kumar, "Cryptanalysis and security enhancement of Chen et al.'s remote user authentication scheme using smart card," *Central European Journal of Computer Science*, vol. 2, no.1, pp. 60–75, 2012.Article (CrossRef Link)

[3] M. K. Khan, S. K. Kim and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'," *Computer Communications*, vol. 34, no. 3, pp. 305–309, 2010.Article (CrossRef Link)

[4] L.C. Wuu, C.H. Hung and C.M. Chang, "Quorum-based Key Management Scheme in Wireless Sensor Networks," *KIIS Transactions on Internet and Information systems*, vol. 6, no. 9, pp. 2442 -2454, 2012. Article (CrossRef Link)

[5] Y. D., T.Q., H.J. and W.F. Sun. "A Pattern-based Query Strategy in Wireless Sensor Network," *KSII Transactions on Internet and Information systems*, vol. 6, no. 6, pp. 1267 – 1285, 2012. Article (CrossRef Link)

[6] M. I. Razzak, M. K. Khan, K. Alghathbar, "Contactless Biometrics in Wireless Sensor Network: A Survey," in *Proc of 3rd International Conference on Security Technologies (SecTech'10), CCIS, Springer-Verlag*, vol. 122, pp. 236-243, Dec. 2010. Article (CrossRef Link)

[7] M. K. Khan and K. Alghathbar, "Security Analysis of 'Two-Factor User Authentication in Wireless Sensor Networks," in *Proc. of 4th International Conference on Information Security and Assurance (ISA'10), Lecture Notes in Computer Science*, (Japan), vol. 6059, pp. 55-60, June 2010. Article (CrossRef Link)

[8] A. Thapa and S. Shin, "QoS Provisioning in Wireless Body Area Networks: A Review on MAC Aspects," *KSII Transactions on Internet and Information systems*, vol. 6, no. 5, pp. 1267 – 1285, 2012. Article (CrossRef Link)

[9] W.Y. Chung, "Multi-Modal Sensing M2M Healthcare Service in WSN," *KSII Transactions on Internet and Information systems*, vol. 6, no. 4, pp. 1090 – 1105, 2012. Article(CrossRef Link)

[10] S. Ullah, H. Higgins, B.B., B. L., C. B., I. M., S. Saleem, Z. Rahman and K.S .Kwak, "A Comprehensive Survey of Wireless Body Area Networks - On PHY, MAC, and Network Layers Solutions," *J. Medical Systems*, vol. 36, no. 3, pp. 1065-1094, 2012. Article (CrossRef Link)

[11] S. Ullah and K.S. Kwak, "Body Area Network for Ubiquitous Healthcare Applications: Theory and Implementation," *Journal Medical Systems*, vol. 35, no. 5, pp. 1243-1244, 2011. Article (CrossRef Link)

[12] S. Saleem, S. Ullah, H.S. Yoo, "On the Security Issues in Wireless Body Area Networks", *Journal of Digital Content Technology and its Applications (JDCTA)*, vol. 3, no. 3, pp. 178-184, 2009. Article (CrossRef Link)

[13] S. Ullah, P. Khan, N. Ullah, S. Saleem, H. Higgins, K.S Kwak, "A Review of Wireless Body Area Networks for Medical Applications", *International Journal of Communications, Network and System Sciences (IJCNS)*, vol. 2 no. 8, 2010. Article (CrossRef Link)
[14] K. H. M. Wong, Y. Zheng, J. Cao and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. of IEEE International Conference on Sensor Network Ubiquitous, and Trustworthy Computing*, vol. 1, pp. 318–327, 2006. Article (CrossRef Link)
[15] H. R. Tseng, R. H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," *IEEE on Global Telecommunications Conference*, pp. 986–990, 2007. Article (CrossRef Link)
[16] M.L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009. Article (CrossRef Link)
[17] M.K. Khan and Khaled Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010. Article (CrossRef Link)
[18] P. Kumar, S.G. Lee and H.J. Lee, "E-SAP: Efficient-Strong Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks," *Sensors*, vol. 12, pp. 1625-1647, 2012. Article (CrossRef Link)
[19] B. Vaidya, J.J.P.C. Rodrigues and J.H. Park, "User authentication schemes with pseudonymity for ubiquitous sensor network in NGN," *International Journal of Communication Systems*, vol. 23, pp. 1201–1222, 2009. Article (CrossRef Link)
[20] D. He, Y. Gao, S. Chan, C. Chen and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc Sens. Wirel. Netw.* vol. 10, pp. 1–11, 2010. Article (CrossRef Link)
[21] C. Chen, D. He, S. Chan, J. Bu, Y. Gao and R. Fan, "Lightweight and provably secure user authentication with anonymity for the global mobility network," *International Journal of Communication Systems*., 2010, doi:10.1002/dac.1158. Article (CrossRef Link)
[22] Z.L. Ping and W. Yi, "An ID-based authenticated key agreement protocol for wireless sensor networks," in *Proc. of 1st International Conference on Information Science and Engineering (ICISE)*, Nanjing, pp. 2542 - 2545, 2009. Article (CrossRef Link)
[23] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, "SAGE: A strong privacy-preserving scheme against global evesdropping for ehealth systems," *IEEE Journal of Selected Areas Communication.*, vol. 27, pp. 365–378, 2009. Article (CrossRef Link)
[24] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," in *Proc. of Advances in Cryptology*, (*CRYPTO'99*), pp. 388-397, 1999. Article (CrossRef Link)
[25] T.S. Messerges, E.A. Dabbish and R.H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541-552, 2002. Article (CrossRef Link)

Muhammad Khurram Khan is currently an Associate Professor with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. He has edited seven books and proceedings published by Springer-Verlag and IEEE. He has published more than 140 papers in international journals and conferences and he is an inventor of 7 U.S./PCT patents in the information security field. Dr. Khurram is a Founding Editor of the Bahria University Journal of Information and Communication Technology. He is on the editorial boards of several International SCI journals, including the Journal of Network and Computer Applications (Elsevier), the Journal of Security and Communication Networks (Wiley), Telecommunication Systems (Springer), Computers and Electrical Engineering (Elsevier), Electronic Commerce Research (Springer), journal of Computing & Informatics, the Journal of Information Hiding and Multimedia Signal Processing (JIHMSP), and the International Journal of Biometrics (Inderscience). Dr. Khurram is one of the organizing chairs of several top-class international conferences and he is also on the program committee of dozens of conferences. He is a recipient of several national and international awards for his research contributions. In addition, he has been granted several national and international funding projects in the field of information security. His current research interests include biometrics, multimedia security, and digital authentication.

Saru Kumari is currently an Assistant Professor with the Department of Mathematics, Agra College, Agra, Dr. B. R. A. University, Agra, India. She received her Ph.D. in Mathematics in 2012 on “Some Remote User Authentication Schemes with Smart Card: Weaknesses and Improvements” from C.C.S. University, Meerut, Uttar Pradesh, India. Her research interests include cryptography, information security, and Applied Mathematics.

Pitam Singh is currently working as an Assistant Professor with the Department of Mathematics, Motilal Nehru National Institute of Technology, Allahabad, India. His research area is Cryptography and Fuzzy logic.