Journal of Universal Computer Science, vol. 24, no. 9 (2018), 1258-1270
submitted: 30/12/17, accepted: 30/6/18, appeared: 28/9/18 © J.UCS

Verifying Secure Authentication Protocol for Communication between IoT-based Medical Devices

Nipon Theera-Umpon
(Biomedical Engineering Institute, Chiang Mai University, Chiang Mai 50200 Thailand
Department of Electrical Engineering, Faculty of Engineering, Chiang Mai University
Chiang Mai 50200 Thailand
nipon.t@cmu.ac.th)

Kun-Hee Han
(Department of Information Communication Engineering, Baekseok University
Cheonan, Korea
hankh@bu.ac.kr)

Woo-Sik Bae
(Department of AIS Center, Ajou Motor College, Boryeong, Chungnam, Korea
drbws@daum.net)

Sanghyuk Lee
(Department of Electrical and Electronic Engineering and AI University Research Centre
(AI-URC) Xi'an Jiaotong-Liverpool University, China
Biomedical Engineering Institute, Chiang Mai University, Chiang Mai 50200 Thailand
Information Technology Faculty, Ton Duc Thang University, Ho Chi Minh, Vietnam
Sanghyuk.Lee@xjtlu.edu.cn)

Van Huy Pham
(Corresponding author, Faculty of Information Technology, Ton Duc Thang University
Ho Chi Minh City, Vietnam
phamvanhuy@tdt.edu.vn)

Abstract: The evolving Internet of Things (IoT) technology has driven the advancement of communication technology for implantable devices and relevant services. Still, concerns are raised over implantable medical devices (IMDs), because the wireless transmission section between patients and devices is liable to intrusions on privacy attributable to hacking attacks and resultant leakage of patients' personal information. Also, manipulating and altering patients' medical information may lead to serious leakage of personal information and thus adverse medical incidents. To address the foregoing challenges, the present paper proposes a security protocol that copes with a range of vulnerabilities in communication between IMDs and other devices. In addition, the proposed protocol encrypts the communication process and data to eliminate the likelihood of personal information being leaked. The verification highlights the safety and security of the proposed protocol in wireless communication.

Keywords: U-Healthcare Service, Authentication protocol, Casper, Integrated authentication protocol, Model Checking, Security Policy
Categories: C.2.2, E.3, L.4.0

1 Introduction

Recently, there has been a vast increase in the use of Internet of Things (IoT) devices across various fields including industrial, factory and service areas [Chiang, 16; Zanella, 14; Singh, 15; Loukas, 15; Brown, 13]. Since the Global Standards Initiative on the Internet of Things (IoT-GSI) defined IoT as “the infrastructure of the information society” in 2014, the IoT has created technology from integration of the physical world to computer-based systems. This includes interconnections between machine and machine, machine and human by way of smart devices such as electronics, sensors, actuators, and software. With developing technology and growing demand, IoT technology has extended from automation into nearly all areas of smart cities. With expanding of internet connected environments, it is also expected to process large amounts of data from many locations and more effectively. Now IoT has become one of platform for the smart city, energy internet [Zanella, 14; Singh, 15].

With IoT technology applications, many benefits are offered such as convenience, speed, and efficiency in cost. Exposure to dangerous and difficult conditions can be avoided guaranteeing physically safe working environments. Furthermore, it can save processing time due to real time data processing. As a result, it helps reduce costs in data management. However, IoT technology also has many challenging aspects in particular security. For example, unauthorized access and personal information misuse problems can occur, it also opens up systems to possible to attack [Cirani, 15]. When it comes to medical IoT devices attention must be focused on providing sufficient security, because data is related to personal information.

Communication technology enables devices with communication tools to connect intelligently to the internet for interaction with humans and animals as well as other devices. Medical IoT provides smart services based on context awareness, and it is projected to play a pivotal role in the hyper connected society in pursuit of openness and sharing [Cirani, 15]. Specifically, microminiaturized sensors and measurement units are applied in many industrial fields including medical devices [Gope, 15]. These smart medical devices make it possible for patients to check their health conditions at anytime or provides checks for those who live in remote areas where even simple healthcare services may not be available. Therefore, medical IoT helps to provide medical service for anyone at anytime and anywhere. However, as mentioned previously, the wireless transmission section of the communication between patients and devices is vulnerable to attacks by intruders. This could lead to alteration of patient information or serious issues such as swapping personal information and health conditions with others [Bae, 14; Seyed, 15; Seo, 15; Wei, 12]. With attention on the said security problem, research on security in inter-device communication has recently been enhanced via hardware and/or software [Song, 07, Ray, 14].

In this paper, a protocol which is capable of disabling various attacks with mutual authentication and encrypted communication through software is proposed. The protocol follows widely accepted verification tools, so Compile for the Analysis of Security Protocols (Casper) and Failure Divergence Refinements (FDR) [Lowe, 09; Formal Systems (Europe) Ltd., 10] tools are considered for the formal verification. Casper and FDR are implemented in this paper to verify the proposed protocol usefulness. The verification results show that the protocol is able to ensure the security of wireless communications between medical devices [Han, 16]. The paper is presented as follows: In the next chapter, a review of the relevant research on U-healthcare services and Casper and FDR protocol for application in security environment is provided. An authentication protocol with Casper and FDR are proposed and tested in Chapter 3. In Chapter 4, the security performance of the proposed protocol is discussed. Finally, conclusions are provided in Chapter 5.

2 Preliminaries

2.1 U-healthcare

Medical IoT technologies used to assist emergency patients has expedited extensive research on technology for U-healthcare services. U-healthcare systems provide healthcare services for patients anywhere and at any time. In order to complete the system, medical data collection and transmission with smart sensors and transmitters from the patient's body to the doctor are necessary, and this process makes it possible for patients to receive proper and timely treatment from their doctor. The process involves family doctors and other healthcare specialists analysing biometric information for confirmation and providing feedback to patients. During treatment, patients and doctors interact with each other by way of video consulting and imaging with wired and/or wireless communication. Due to the growing population of senior persons, IoT-based U-healthcare is expected to play a significant part in life and healthcare in the future.

Whether it is text, image or other, patients information should be handled securely. So, the security issues relevant to healthcare systems and medical devices are extremely important to patients' from both health and personal information perspectives, which warrants the verification of their security [Song, 07]. In general, security threats in IoT-based healthcare communication are comparable to the security requirements in wireless communication [Niu, 15; Lin, 15]. Now security threats in healthcare communication for U-healthcare are summarized as follows.

- Authentication and integrity: Users of communication devices are required to prove they are authorized. To this end, each device should have a unique ID.

- Confidentiality: Data transmitted and received in wireless communication should be kept confidential against unauthenticated devices.

- Anonymity and privacy: Unless anonymity is met in wireless communication, there is risk of privacy intrusion. Any exposure of personal healthcare information to intruders could result in serious issues including safety.

- Non-repudiation: Robust non-repudiation technology should be applied to devices transmitting data so that they cannot repudiate the results of data transmission and reception.

As mentioned, the security of patient information during transmission by IoT devices has been emphasized. Transmission protocols are therefore important in satisfying the security requirements. The following provides an introduction of two popular security protocols, Compile for Analysis of Security Protocols (Casper) and Failure Divergence Refinements (FDR).

2.2 Casper and FDR

Communication Sequential Process (CSP) is a compiler developed for use in diverse protocols [Hoare, 85]. Casper is a specification language which is highly complicated especially for security protocols, and it needs less skill for designers in the formal design method in the process of formal specification in CSP [Hoare, 85]. It has an advantage in processing, that is, even infinitesimal mistakes lead to hindering design and analysis. To address the challenge, Casper is developed to simplify the design process in operation of transmission in security protocols.

As for the specification, the following characteristics are specified prior to running the program. Which is considered into a CSP document.

- Defines the agents, variables, and functions in the protocol
- Represents each agent as a process
- Shows all the messages exchanged between the agents
- Specifies the security properties to be checked
- Defines the real variables, in the actual system to be checked
- Defines all the functions used in the protocol
- Lists the agents participating in the actual system with their parameters instantiated
- Specifies the intruder’s knowledge and capabilities, etc.

The converted CSP document is verified with the FDR program to determine if it meets the attributes, e.g. security and authentication. FDR verifies safety, deadlock and livelock and shows the scenarios about any potential intrusion upon discovering any security vulnerabilities to facilitate the analysis of vulnerabilities.

2.3 Conventional wireless authentication methodology

Recently, development of security technology for wireless communication has been greatly emphasised. One of the effective methodologies, K. Ramenzani proposed modified the wireless communication protocol by way of applying EAP Reauthentication Protocol (ERP), simply EAP-ERP, and verify with Casper [Ramezani, 16]. However, the protocol was considered only for mobile devices, and requires a large computational load and also requires authentication through several processes [Ramezani, 16]. Therefore, it has a limitation for using in small IoT devices. The protocol description is illustrated as follows, which was proposed by Ramenzani in 2016.

```
#Protcol description
0.->b : a
1.b -> a : ReqlD,b,c
2.a -> b : a
3.b -> c : b,{a}{kbc}
4.c -> d : {a,Frealm}{kcd}
5.d ->c{(TLSreq) % v}{kcd}
```

6.c-> b :{v % ((TLSreq) % v)}{kbc}
7.b->a: v % TLSreq
8.a->b:(CpherSuit,na) % w
9.b->c:{w% ((CipherSuit,na)%w)}{kbc}
10.c->d:{w%(CipherSuit,na)}{kcd}
11.d->c:{(nd,SessionID,TLSfinish,{c}{cpk(a)}) % z}{kcd}
12.c->b:{z % ((nd,SessionID,TLSfinish,{c}{cpk(a)})%z)}{kbc}
13.b->a:z % (nd,SessionID,TLSfinish,{c}{cpk(a)})
14a.a->b:TLSfinish,{pms}{pk(d)},h(k,CipherSuit,TLSfinish))%y
14b.a->b:{TLSfinish}{msk}%r
15a.b->c:{y%((TLSfinish,{pms}{pk(d)},h(k,CipherSuit,TLSfinish))%y)}{kbc}
15b.b->c:{r%(({TLSfinish}{msk})%r)}{kbc}
16a.c->d:{y%((TLSfinish,{pms}{pk(d)},h(k,CipherSuit,TLSfinish))){kcd}
16b.c->d:{r%({TLSfinish}{msk})}{kcd}
17.d->c:{(({TLSfinish}{msk},h(k,TLSfinish))%o}{kcd}
18.c->b:{o%(({TLSfinish}{msk},h(k,TLSfinish))%o)}{kbc}
19.b->a:o%({TLSfinish}{msk},h(k,TLSfinish))
20. c -> d : {a,Frealm}{kcd}
21. d -> c : {msk,DSRK,EAPsuccess}{kcd}
22. c -> b : {msk,EAPsuccess,Frealm}{kbc}
23. b -> a : Frealm ,EAPsuccess

3 Protocol Proposal on Medical Device

The proposed protocol is designed for the wireless communication between implantable medical devices and readers for data transmission and reception. Normally, the wireless section is exposed to diverse security threats. The proposed protocol is considered to provide a secure communication setting against threats including hacking. Secretkey, SessionKey and Hash Function are used to construct the protocol in this paper. Moreover, to prevent any time-lapse attacks in the transmission section, Time Stamp is applied as well. As transmission values always vary with sections, different data can be transmitted each time, which keeps intruders from engaging in replay attacks, location tracking and traffic analysis.

Hence, Secretkey, SessionKey, and Hash Function are designed, and Time Stamp applied in order to defend advanced persistent threat (APT). Every transmission data are transferred per each transmission interval, therefore an attacker cannot attack, replay attacks, location tracking, traffic analysis after taking transmission data. In simulation, transmitted protocol safety is verified with Casper/FDR.

The security of data transmitted in each step of the proposed protocol is ensured.

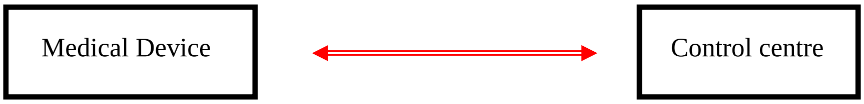


Figure 1: Data transmission and receive mechanism

Symbols in Table 1 are used in the proposed protocol for data transmission between implantable medical devices in this paper.

Symbols	Definition
Tag	Agent
Reader	Agent
DB	Server
H	Hash Function
Pkdb	PublicKey
Skdb	SecretKey
keyR, KeyT	SessionKey
i, j	Nonce
Ta, Tb	Time Stamp

Table 1: Symbols and definition

3.1 Casper specification

In this subsection, the Casper specification code of the proposed protocol is illustrated. It is used to verify the wireless communication between implantable medical devices, and also listed domain of variables and illustrated operating procedures. It is also shows that procedures are very important in security protocols. Basic variables and function types are defined under #Free variables as follows. Inside the protocol,

InverseKeys = (keyR,keyR), (pkdb,skdb), (keyT,keyT), (i,i), (j,j)

stands for each agent and function returns reverse keys.
Inside of #Protocol description, the sequential order of messages transmitted in the protocol is defined. The integers, 0, 1, …, 5 indicate the steps of message transmission.

<u>Casper specification in the protocol</u>

```
variables

R, T : Agent
DB : DatabaseServer
pkdb : PublicKey
skdb : SecretKey
keyR, keyT : SessionKey
H : HashFunction
Ta, Tb : TimeStamp
i, j :Nonce
InverseKeys = (keyR,keyR),(pkdb,skdb),(keyT,keyT),(i,i),(j,j)

#Protocol description
```

0. -> R : T
1. T -> R : Ta,j,{R,keyT}{pkdb}%enc
[(Ta==now or ts+1==now) and A!=B]
2. R -> DB : Tb,{T,keyR}{pkdb},enc%{R,keyT}{pkdb}
[(Ta'==now or ts'+1==now) and A!=B]
3. DB -> R : keyT(+)keyR(+)H(R),Tb
4. R -> T : {R}{keyT}(+)H(R),Ta,i
[(Ta==now or ts+1==now) and A!=B]
5. T -> R : H(keyT), Ta, i, skdb
[(Ta'==now or ts'+1==now) and A!=B]

#Intruder Information

Intruder = Mallory
IntruderKnowledge = {Reader, Tag, Mallory, DataBase, SM}

3.2 Operation process

Now the data transmission and processing sequence in the proposed protocol between implantable medical devices is described in the following procedure.

Step 1 : Tag → Reader
On receiving a Query from the Reader, the Tag generates the Time Stamp, Ta, Nonce j, Session Key keyT, PublicKey pkdb, which is concatenated with a generated value. The value is stored in the variable, %enc, whilst [(Ta==now or ts+1==now) and A!=B] is checked. The Tag calculates and transmits Ta,j,{R,keyT}{pkdb}%enc to the Reader. The generated value is unique, involves the Time Stamp and Hash-lock and cannot be generated by any other Tag. At the same time, the attributes of each data transmitted cannot be used for attacks.

Step 2 : Reader → DB
The Reader uses Ta,j,{R,keyT}{pkdb}%enc transmitted by the Tag and its Tb, T, keyR, R, keyT, pkdb to yield the following:
Tb,{T,keyR}{pkdb},enc%{R,keyT}{pkdb}. That is, the value of TimeStamp Tb and Ta,j,{R,keyT}{pkdb}%enc data sent by the Tag are used for concatenation. Then, the Reader checks [(Ta'==now or ts'+1==now) and A!=B] and stores it in the variable enc1%. Once the Tb,{T,keyR}{pkdb},enc%{R,keyT}{pkdb} data is generated, it is normally transmitted to the DB.

Step 3 : DB → Reader
The DB receives the value of Tb,{T,keyR}{pkdb},enc%{R,keyT}{pkdb} from the reader and performs a mathematical operation to verify it prior to the mutual authentication. Then, the DB uses the value transmitted by the Reader and applies an exclusive OR operation to the session keys, keyT and keyR, to calculate the value of keyT(+)keyR(+)H(R),Tb. Here, the hash value is calculated as the following: $h_a(R) = h_{\text{int}}\left(\left(\sum_{j=0}^{k} x_j \cdot a^j\right) \bmod p\right)$. The DB verifies the value yielded in the

formula, $h_a(R) = h_{\text{int}}\left(\left(\sum_{j=0}^{k} x_j \cdot a^j\right) \bmod p\right)$, and Ta, which is the value of TimeStamp sent by the Reader, and then generates Tb, another value of TimeStamp, prior to concatenation. Finally, the DB generates and transmits the value of keyT(+)keyR(+)H(R),Tb to the Reader. The values of hash data in hash operation are found by hashing fixed-length data as below.

As for the initial vector hash function, a random integer 2*w* is calculated in $\overline{a} = (a_0, a_1, ..., a_k)$ leading to $h_a(\overline{x})^{strong} = \left(a_0 \sum_{i=0}^{k} a_{i+1} x_i \bmod 2^{2w}\right) \div 2^w$, which is applied to a string, a value of data for transmission. Then, $h_a(\overline{x}) = h_{\text{int}}\left(\left(\sum_{j=0}^{k} x_j \cdot a^j\right) \bmod p\right)$, where $a \in [p]$ is uniformly random and h_{int} is chosen randomly from a universal family mapping integer domain $[p] \rightarrow [m]$.

Step 4 : Reader → Tag

The Reader verifies keyT(+)keyR(+)H(R),Tb transmitted by the DB prior to performing an operation and authentication. Then, the Reader performs an operation to generate its own value KeyT, which is the R, Session Key, calculates a hash value of $h_a(R) = h_{\text{int}}\left(\left(\sum_{j=0}^{k} x_j \cdot a^j\right) \bmod p\right)$ and TimeStamp Ta, generates the Nonce i, performs an Exclusive OR operation, concatenates respective data and generates the value of {R}{keyT}(+)H(R),Ta,i. Then, the Reader verifies the value of Ta==now or ts+1==now) and A!=B], and transmits the value to the Tag for further authentication, if it meets the requirement.

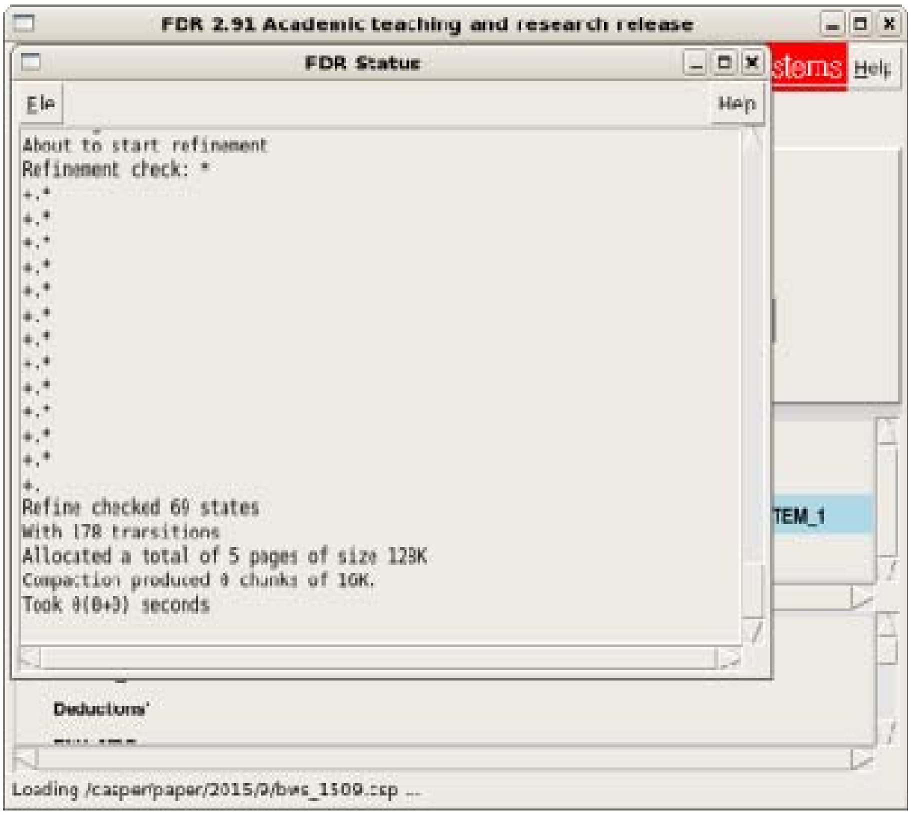
Step 5 : Tag → Reader

Lastly, the Tag receives from the Reader the value of {R}{keyT}(+) $h_a(R) = h_{\text{int}}\left(\left(\sum_{j=0}^{k} x_j \cdot a^j\right) \bmod p\right)$, Ta, I and compares it with its own value. Once the value is verified, the Tag performs an operation, $h_a(\text{keyT}) = h_{\text{int}}\left(\left(\sum_{j=0}^{k} x_j \cdot a^j\right) \bmod p\right)$, Ta, i, skdb. Then, if the value of [(Ta'==now or ts'+1==now) and A!=B] is met, the Tag transmits it to the Reader and completes its authentication session. Subsequently, the Reader receives from the Tag the value of $h_a(\text{keyT}) = h_{\text{int}}\left(\left(\sum_{j=0}^{k} x_j \cdot a^j\right) \bmod p\right)$, Ta, i, skdb and sends it to the DB, which in turn searches and verifies the value for the Tag for authentication. As the hash code and tag code can be verified upon completion of normal authentication, the system continues to operate.

4 Verification of Proposed Protocol

In this section, the proposed protocol safety, deadlock and livelock for data transmission between implantable medical devices is verified by running a model based on Casper/FDR. Fig. 1 shows the completed state following the loading of the designed source file and basic checks over grammar and process.

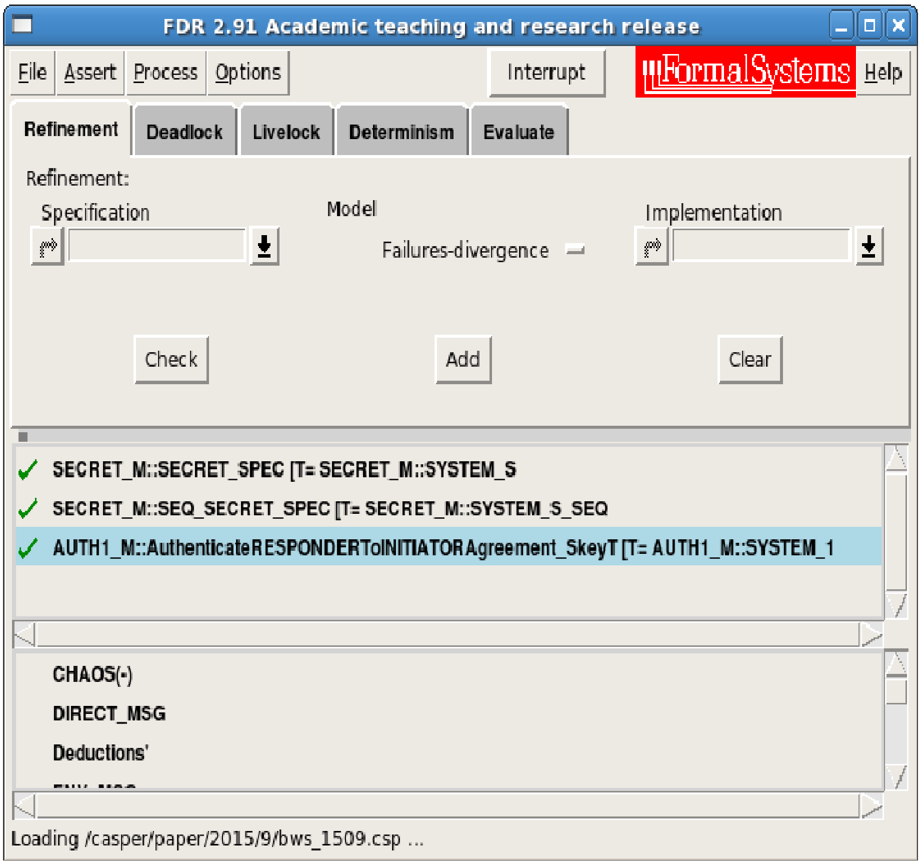
Upon completion of the verification of the proposed protocol with the program, it proves to meet all security attributes as in Fig. 1. If any security vulnerability is found by the verification program, "X" is printed. Then, debugging is performed to define and correct the issue followed by repeated verification.



```
About to start refinement
Refinement check: *
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.
Refine checked 69 states
With 178 transitions
Allocated a total of 5 pages of size 128K
Compaction produced 0 chunks of 16K.
Took 0(0+0) seconds
```

Loading /casper/paper/2015/9/bws_1509.csp ...

Figure 2: Security verification results of the protocol (part 1)



```
✓ SECRET_M::SECRET_SPEC [T= SECRET_M::SYSTEM_S
✓ SECRET_M::SEQ_SECRET_SPEC [T= SECRET_M::SYSTEM_S_SEQ
✓ AUTH1_M::AuthenticateRESPONDERToINITIATORAgreement_SkeyT [T= AUTH1_M::SYSTEM_1
```

```
CHAOS(-)
DIRECT_MSG
Deductions'
```

```
Loading /casper/paper/2015/9/bws_1509.csp ...
```

Figure 2: Security verification results of the protocol (part 2)

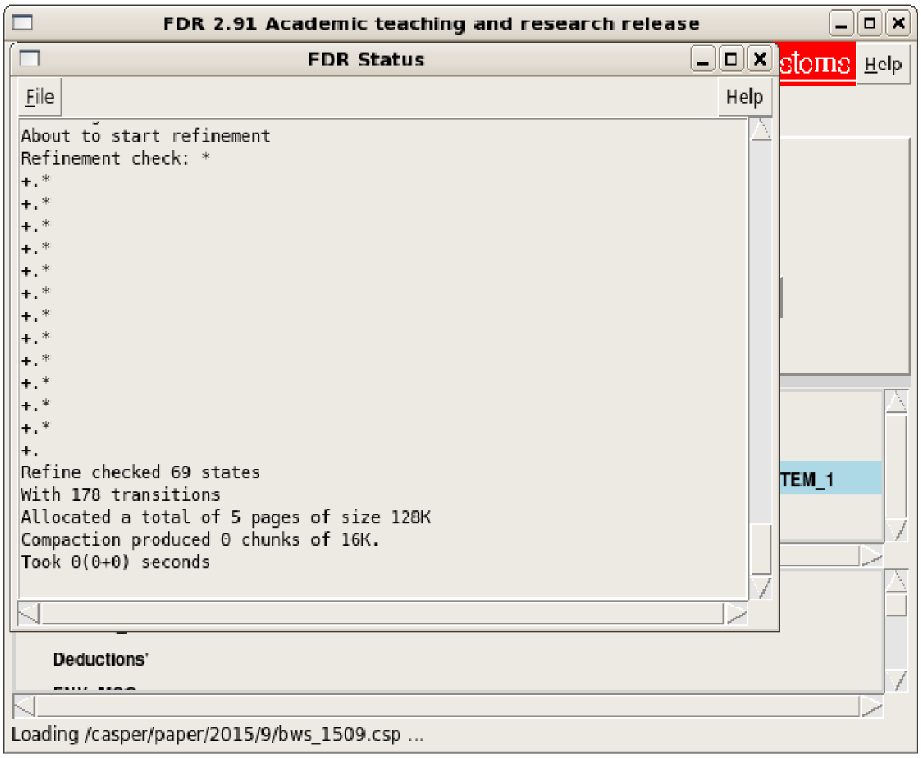
In Figure 2, three verification results are shown, each of which is represented and analyzed as follows.

1) SECRET_M::SECRET_SPEC[T=SECRET_M::SYSTEM_S
This concerns the overall security of the proposed protocol for implantable medical devices. The tick mark before messages indicates the protocol is safe and secure against various attacks without any exposure to intruders. The safety of communication between agents, the security of session keys and the presence of any issues relevant to various attacks have been verified here. The proposed protocol has been proved to be safe as in Fig. 1.

2)SECRET_M::SEQ_SECRET_SPEC[T=SECRET_M:: SYSTEM - S_SEQ
This shows whether the proposed protocol for implantable medical devices operates seamlessly in each step. The protocol has been proved to be safe in the verification of each step in terms of various errors, attacks and exposure.

3)AUTH1_M::AuthenticateRESPONDERToINITIATORAgreement_k[T=AUTH1_M::SYSTEM_1
This verifies if the Responder and the Initiator can authenticate each other via k without any security issues. The proposed protocol has been proved to ensure safety in communication between agents.

Next, Figure 3 shows a status window upon the verification of the proposed protocol, displaying the inter-session safety is satisfied with each step being completed without falling into any deadlock. In addition, the infinite repetition does not cause any issues on the system until the completion of verification.



```
About to start refinement
Refinement check: *
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.*
+.
Refine checked 69 states
With 170 transitions
Allocated a total of 5 pages of size 128K
Compaction produced 0 chunks of 16K.
Took 0(0+0) seconds
```

Loading /casper/paper/2015/9/bws_1509.csp ...

Figure 3: Post-verification status

5 Conclusions

The advancement of IoT technology has been accompanied by significant development and research in the field of medical devices. Medical devices process personal healthcare information and engage in inter-device communication, where personal information and privacy protection are very important factors. In the same vein, manipulation and leakage of patients' healthcare information could cause some serious issues. Therefore, researchers have attempted to address security-related challenges and secure the safety of communication sections via encryption and encrypted protocols. The present paper designs a protocol for safe IoT communication between medical devices using Hash-lock, TimeStamp, Nonce and Sessionkey. To verify the safety of the proposed protocol, Casper language is used for the design followed by the verification with the FDR program. The proposed protocol satisfies all the aspects of security that FDR requires for verification, i.e. safety, deadlock and livelock. Furthermore, the protocol ends well without taking up much memory space. The present findings highlight the following points. First, the formal verification of the protocol for communication between medical devices decreases mistakes whilst increasing the effectiveness in protocol verification. Second, the findings will be conducive to rectifying vulnerabilities in wireless communication and transmission and thus accelerating the pace of system development. Further studies will adopt a stronger function to develop a more effective approach to safety and security applicable to military, finance and healthcare sectors.

Acknowledgements

This research is supported by 2016 Baekseok University research fund. It is also financially supported by the Centre for Smart Grid and Information Convergence (CeSGIC) and XJTLU Key Programme Special Fund (KSF-P-02) at Xi'an Jiaotong-Liverpool University. The authors would like to thank all the parties concerned.

References

[Bae, 14] Bae W.-S.: Formal Verification of an RFID Authentication Protocol Based on Hash Function and Secret Code, Wireless Personal Communication, Vol. 79, Issue 4, pp. 2595–2609, 2014.

[Brown, 13] Brown, I.: Britain's Smart Meter Programme: A Case Study in Privacy by Design, International Review of Law, Computers & Technology, Vol. 28, Issue 2, pp. 172-184, 2014.

[Chiang, 16] Chiang, M. T. Zhang, Fog and IoT: An Overview of Research Opportunities, IEEE Internet of Things Journal, Vol. 3, Issue 6, pp. 854-864, December 2016.

[Cirani, 15] Cirani, S., Picone, M.,Gonizzi, P.,Veltri, L.,Ferrari, G.: IoT-OAS: An OAuth-based Authorization Service Architecture for Secure Services in IoT Scenarios, IEEE Sensors Journal, Vol, 15, Issue 2, pp 1224-1234, 2015.

[Formal Systems (Europe) Ltd., 10] Formal Systems (Europe) Ltd., Oxford University Computing Laboratory: Failures-Divergence Refinement, FDR2 User Manual, 19th October 2010.

[Gope, 15] Gope, P., Hwang, T.: Untraceable Sensor Movement in Distributed IoT Infrastructure, IEEE Sensors Journal, Vol. 15, Issue 9, pp 5340-5348, 2015.

[Han, 16] Han, K.-H., Bae, W.-S.: Proposing and Verifying a Security-enhanced Protocol for IoT-based Communication for Medical Devices, Cluster Computing, Vol. 19, Issue 4, pp. 2335-2341, 2016.

[Hoare, 85] Hoare C.A.R.: Communicating Sequential Processes, Prentice-Hall, 1985.

[Lin, 15] Lin, X. J. A, Sun, L. B, Qu, H. A.: Insecurity of an Anonymous Authentication for Privacy-preserving IoT Target-driven Applications, Computers and Security, Vol. 48, Issue C, pp. 142-149, 2015.

[Loukas, 15] Loukas, G.: Cyber-Physical Attacks: A Growing Invisible Threat, Oxford, UK: Butterworh-Heinemann (Elsevier), June 2015.

[Lowe, 09] Lowe, G.: Casper: A Compiler for the Analysis of Security Protocols, User Manual and Tutorial, Version 1.12, 2009.

[Niu, 15] Niu, B., Zhu, X. A, Li, Q. C, Chen, J. A, Li, H. A.: A Novel Attack to Spatial Cloaking Schemes in Location-based Services, Future Generation Computer Systems, Vol. 49, Issue C, pp. 125-132, 2015.

[Ramezani, 16] Ramezani, K., Sithirasenan, E., Su, K.: Formal Security Analysis of EAP-ERP Using Casper, IEEE Access, Vol. 4, pp. 383-396, 2016.

[Ray, 14] Ray, B. R., Abawajy, J., Chowdhury, M.: Scalable RFID Security Framework and Protocol Supporting Internet of Things, Computer Networks, Vol, 67, pp. 89-103, 2014

[Seo, 15] Seo, D. B., Jeong, C.-S., Jeon, Y.-B., Lee, K.-H.: Cloud Infrastructure for Ubiquitous M2M and IoT Environment Mobile Application, Cluster Computing, Vol. 18, Issue 2, pp. 599-608, June 2015.

[Seyed, 15] Seyed M. A., Karim B., Behzad A., Mohammad R. A.: Traceability Analysis of Recent RFID Authentication Protocols, Wireless Personal Communications, Vol. 83, Issue 3, pp. 1663-1682, 2015.

[Singh, 15] Singh, J., Pasquier, T., Bacon, J., Ko, H., Eyers, D.: Twenty Cloud Security Considerations for Supporting the Internet of Things, IEEE Internet of Things Journal, Vol. 3, Issue 3, pp. 269-284, 2015.

[Song, 07] Song J. E., Kim S. H., Chung M. A., Chung K. I.: Security Issues and Its Technology Trends in u-Healthcare. Electronics and Telecommunications Trends, Vol. 22, No.1, pp. 119-129, 2007.

[Wei, 12] Wei, J., Hu, X., Liu, W.: An Improved Authentication Scheme for Telecare Medicine Information Systems., Journal of Medical Systems, Vol. 36, Issue 6, pp. 3597-3604, 2012.

[Zanella, 14] Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of Things for Smart Cities, IEEE Internet of Things Journal, Vol. 1, Issue 1, pp. 22–32, February 2014.