sensors

Article

Can Formal Security Verification Really Be Optional? Scrutinizing the Security of IMD Authentication Protocols

Daniel Gerbi Duguma [1], Ilsun You [2,*], Yonas Engida Gebremariam [2] and Jiyoon Kim [1,*]

[1] Department of Information Security Engineering, Soonchunhyang University, Asan-si 31538, Choongchungnam-do, Korea; danielgerbi2005@gmail.com

[2] Department of ICT Environmental Health System, Soonchunhyang University, Asan-si 31538, Choongchungnam-do, Korea; yonas.engidag@gmail.com

[*] Correspondence: isyou@sch.ac.kr (I.Y.); 74jykim@sch.ac.kr (J.K.)

check for updates

Citation: Duguma, D.G.; You, I.; Gebremariam, Y.E.; Kim, J. Can Formal Security Verification Really Be Optional? Scrutinizing the Security of IMD Authentication Protocols. *Sensors* **2021**, *21*, 8383. https://doi.org/10.3390/s21248383

Academic Editor: Massimo Ficco

Received: 22 October 2021
Accepted: 13 December 2021
Published: 15 December 2021

Abstract: The need for continuous monitoring of physiological information of critical organs of the human body, combined with the ever-growing field of electronics and sensor technologies and the vast opportunities brought by 5G connectivity, have made implantable medical devices (IMDs) the most necessitated devices in the health arena. IMDs are very sensitive since they are implanted in the human body, and the patients depend on them for the proper functioning of their vital organs. Simultaneously, they are intrinsically vulnerable to several attacks mainly due to their resource limitations and the wireless channel utilized for data transmission. Hence, failing to secure them would put the patient's life in jeopardy and damage the reputations of the manufacturers. To date, various researchers have proposed different countermeasures to keep the confidentiality, integrity, and availability of IMD systems with privacy and safety specifications. Despite the appreciated efforts made by the research community, there are issues with these proposed solutions. Principally, there are at least three critical problems. (1) Inadequate essential capabilities (such as emergency authentication, key update mechanism, anonymity, and adaptability); (2) heavy computational and communication overheads; and (3) lack of rigorous formal security verification. Motivated by this, we have thoroughly analyzed the current IMD authentication protocols by utilizing two formal approaches: the Burrows–Abadi–Needham logic (BAN logic) and the Automated Validation of Internet Security Protocols and Applications (AVISPA). In addition, we compared these schemes against their security strengths, computational overheads, latency, and other vital features, such as emergency authentications, key update mechanisms, and adaptabilities.

Keywords: implantable medical device; IMD security; IMD authentication protocol; formal security verification

1. Introduction

The need for continuous monitoring of physiological information of critical organs of the human body, combined with the ever-growing field of electronics and sensor technologies, and the colossal opportunities brought by 5G connectivity, have made implantable medical devices (IMDs) the most necessitated devices in the health arena. This is clearly shown by the global IMD market share, which was worth USD 96.6 billion in 2018 [1] and grew to around USD 103.3 Billion in 2019, and will likely rise to USD 148.8 Billion in 2024 [2].

IMDs possess several applications to help manage numerous health conditions. These include controlling the heart rhythm using cardiac pacemakers, heart support using ventricular assist devices, and chronic spinal pain reliefs using spinal cord stimulators [3]. Furthermore, they extend their applications by enabling wireless communication technologies that help manage the interaction between IMDs and external devices in wireless body area networks (WBANs) [4,5]. IMDs functioning in WBANs have made a significant contribution in resolving several challenges in both medical and non-medical fields, yet they have their hurdles.

Despite their critical roles in improving human health conditions, IMDs have various challenges, among which, limitations of resource (power, storage, computation, etc.) and security concerns are the most serious. The former challenge is directly related to their small size and inflexibility since they are implanted in the human body. Concerning the latter, IMDs are susceptible to many security and privacy threats that put a patient's life in danger [6]. Some of the most common security problems that IMDs face are impersonation, requesting confidential information, causing a shock to the patient, reprogramming of IMD, etc. Moreover, security assaults (e.g., side-channel attacks) targeting a wide range of internet of things (IoT) processors, such as the Cortex-A platform, also threaten the wellbeing of IMDs [7].

To date, many countermeasures have been taken to keep the confidentiality, integrity, and availability of IoT systems, along with different privacy and safety mechanisms [8–12]. In particular, to IMDs, different researchers have proposed several solutions that can be categorized into three main groups: cryptographic, access control, and misbehavior detection. The first group of solutions utilizes cryptographic rudiments (including public-key encryption, symmetric-key encryption, cryptographic hash functions, etc.) [13,14]. Access control mechanisms [15–17], on the other hand, protect IMDs from unauthorized access by employing different techniques, such as certificates and lists, designation-based, juxtaposition-based, and biometric-based [6]. The last type of method involves malicious behavior detection to shield IMDs from a range of attacks that may not be easily addressed by the former two solutions [18,19].

IMDs are very sensitive as they are implanted in the human body, and the patients depend on them for the proper functioning of their vital organs. Moreover, due to their resource limitations and the open channel utilized for data transmission, they are intrinsically vulnerable to several attacks, such as distributed denial of service with different attacker intentions [20]. Hence, failing to secure them would put the life of the patient in jeopardy, and damage the reputations of the manufacturer. Consequently, it is imperative to carefully examine the security of the IMD authentication protocols for any vulnerabilities. To do so, we followed two methods. First, we conducted an extensive literature review to understand the operations, architectural perspectives, critical security, and privacy requirements and proposed solutions. We also leveraged empirical data that approximated delays introduced by cryptographic operations for comparative analysis of the authentication protocols. Next, we used two well-known security verification approaches, BAN logic [21] and AVISPA [22], to formally analyze the authentication protocols. Unfortunately, many security protocols designed for IMDs are not formally verified, or they use only one verification method [23–30].

The main contributions of this research work can be summarized as follows:

- We examined various security and privacy requirements along with numerous threats that surround IMDs.
- We performed formal security validation of the contemporary authentication schemes based on BAN logic and AVISPA against several security goals.
- We compared these schemes concerning security strength, computational overhead, latency, and additional features, such as emergency authentication, adaptiveness, and key update mechanisms.

The rest of the paper continues as follows. Section 2 describes the components of a typical IMD system architecture. Section 3 outlines various security and privacy requirements, issues, and proposed solutions. Section 4 presents the formal security analysis of different IMD authentication protocols using BAN logic and AVISPA. Section 5 puts forward the discussion of the results found in Section 4. Section 6 describes the comparative analysis of the authentication protocols concerning functionality, computational overhead, and communication latency. Finally, Section 7 concludes the paper.

2. Typical IMD System Architecture

IMDs play a critical role in sensing vital physiological information, which is then sent out to an external device via the wireless medium for different actions, such as remote monitoring and drug delivery. Typically, such systems are assembled from various components, as shown in Figure 1, among which the following are the main ones.

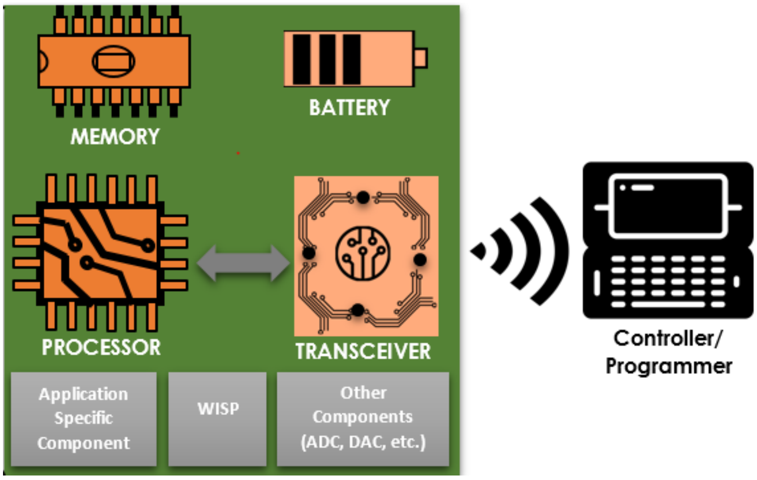

MEMORY
BATTERY
PROCESSOR
TRANSCEIVER
Application Specific Component
WISP
Other Components (ADC, DAC, etc.)
Controller/ Programmer

Figure 1. A typical IMD system architecture.

- Sensor devices. These are small, in-body implanted, battery-powered, and wireless communication enabled sensors to sense, collect, and send patient information to a controller. In general, there are three categories (based on the data measured/collected) of such sensors: those that measure vital physiological information (such as glucose level, EEG, ECG, etc.), those that gather main environmental parameters, such as humidity, temperature, and pressure, and those that measure signals related to the human body movements [31].
- Battery. Implanted sensors need the power to sense information on the body and produce an output. The source of energy for active implants comes from batteries. These batteries can be chargeable or non-chargeable, depending on the sensor type [32], and external or through independent power sources [33]. While the former approach uses optical charging, ultrasonic transducer, and inductive coupling, the latter uses the body environment energy to generate electrical energy for IMDs. Either way, efficient power management is a must since it is difficult (or not desirable) to change batteries now and then. Hence, batteries fixed with these implants should serve for a prolonged period.
- Memory. Memory is vital for the proper functioning of IMDs. It enables implants to store sensed data, configurations, and other important information (such as security keys). The device memory is generally non-volatile (read-only memory (ROM)), retaining its contents regardless of the power supply. In addition, the electrically erasable programmable ROM (EEPROM) and flash memories can be good candidates [32].
- Processing unit. The processing unit is the brain of the entire IMD system, which processes instructions and control signals. The processing unit actively directs the communication between IMDs and external devices, efficient power and transceiver management, and is responsible for other essential tasks, such as sensing and processing data [32].
- Transceiver. To communicate different sensed data to the external devices (such as a programmer) and receive other information from the external devices, IMDs need to establish a wireless medium. An electronic device, known as a transceiver (transmitter and receiver), assists this exchange of information. A specifically designed transceiver called the Medical Implant Communication System (MICS) is available for medical implants with low-power, short-range, and high data rate features [34].

- Application-Specific Components. These components are optional, meaning they may not appear in all implanted devices. One good illustration is the Smart Implant Security Core (SISC) [35]. Communication between IMD and a programmer via wireless medium passes through this device. It runs an energy-efficient security protocol by using energy harvesting when it performs authentication with the programmer. Apart from that, SISC helps defend against denial-of-service attacks, particularly resource exhaustion attacks.
- Wireless Identification and Sensing Platform (WISP). One of the significant constraints of implanted devices is related to power. These devices reside in the human body, making them challenging to recharge or frequently change. Hence, a device called WISP is proposed [32]. Using WISP, therefore, it is possible to conserve the battery of an IMD, especially during an authentication process, as it harvests energy from the reader via radiofrequency.
- Programmer/Controller. Sensing or measuring vital physiological states is only half of the primary goal of using implants. The sensors should also convey the sensed information to an external device (a specially designed controller or a smartphone) near the IMDs. Apart from collecting sensed information from the implants, programmers/controllers assist in configuration setup and regulation of therapy, among others.

3. Security and Privacy Requirements, Threats, and Proposed Solutions

IMDs encounter several challenges, from their conception through their operation. These devices are implanted and severely limited in terms of power, storage, and computing capabilities, making it challenging to build effective communication technologies and security mechanisms. In this regard, IMDs must satisfy various security requirements to withstand the ever-increasing attacks that target them.

The privacy of patients is of paramount importance. Two critical issues in this regard are user anonymity and non-traceability [6,36]. The former refers to a strong requirement that it should be impossible (or difficult enough) for the attacker to intercept the patient's identity from the messages exchanged. Often, this is the first step towards an impersonation attack in which an adversary identifies the user's real identity to fool the other party. Non-traceability, on the other hand, protects the IMD by making it difficult for an attack to know where the patient is or from where he is communicating. As a result, the locations of patients remain confidential, and any acts they conduct cannot be traced back to them by an unauthorized entity.

3.1. Security and Privacy Requirements

Here, we describe nine essential security requirements relevant to the IMDs:

- Confidentiality: the physiological information collected by IMDs is often sent out to a reader via a wireless medium, which both authorized and malicious users can observe. Accordingly, it is essential to encrypt this information to protect the data transmitted from exploitation by the adversaries sitting between the IMD and the reader.
- Integrity: protecting the integrity of the information transmitted via the wireless link in IMD reader communication defends against unauthorized modification. In addition, when illegitimate users tamper with the data, it should be known by the authorized users that the data is modified.
- Availability: this is one of the three security triads (confidentiality, integrity, and availability) that has the objective of making the IMD-enabled system accessible to authorized users despite the presence of adversaries.
- Mutual authentication: unless authorized access is in place, an adversary can impersonate the IMD or the reader to fool the other. Hence, communicating parties need to make sure whom they are talking to before disclosing important information.
- Authorization: once the confidentiality, integrity, and availability of IMDs are guaranteed, and the users (a human user or a device such as a reader) are authenticated, proper authorization to identify the privileges of these users' proceeds. For instance,

a doctor who may issue commands to the IMD should be distinct from a nurse who may only read information to monitor the patient.

- Non-repudiation: there are cases in which one party's actions (knowingly or not) bring unwanted consequences. For instance, in an IMD-enabled health care system, there can be many participants in the process of diagnosing, monitoring, and treating patients. These professionals should not be able to repudiate the actions they took during the process so that, if anything terrible happened next, it is possible to know who did what.
- Session key agreement: communicating entities need to agree on a session key and use that key to encrypt the exchanged information. Session keys are symmetric keys that are primarily derived from another key (called a master key) to restrict ciphertexts and minimize the exposure of an attack. Furthermore, using session keys improves communication performance since these keys do not need to be stored and searched. Moreover, symmetric key encryption is faster.
- Perfect forward secrecy: satisfying this security requirement means the past sessions will not be compromised even if a master key is compromised. In the context of IMDs, if the long-term key is stolen, and if this is known, the key can be updated, and only minimal information would be disclosed while all past communications can be kept safe from future compromises.
- Emergency authentication: if we deal with patients with implanted devices, there can always be emergencies requiring human intervention. Emergency authentication is one of the paradox requirements since unauthorized users need to access the implants to override the authorization and authentication properties, which calls for a clear definition of an emergency.

Concerning privacy, there are at least five privacy requirements [12,37] that should be satisfied:

- Device-existence privacy: this privacy requirement challenges the protocol designers to conceal the device's information of an IMD-enabled system and prohibit an adversary from learning its existence.
- Device-type privacy: in the cases where the presence of a device cannot be wholly concealed or its privacy cannot be maintained, the type of the device should stay anonymous. By doing so, it is possible to protect the patient from device-type specific attacks.
- Specific-device ID privacy: the unique ID (or serial number) of an IMD should not be disclosed to unauthorized users. Doing so protects the patients by prohibiting attackers from tracking down their locations.
- Measurement and log privacy: the information measured, collected, and analyzed in either IMD or the reader should be kept private. Keeping the privacy of logs enables the investigation and trace actions taken during the communication.
- Bearer privacy: these are often related to information such as patients' names, record history, tests, IMD characteristics, etc., which should be kept private.

3.2. Security Issues and Proposed Solutions

Threats are only dangerous because of adversaries, malicious entities that usually have access to the communication media and are placed between the authorized entities to violate confidentiality (and privacy), integrity, and availability. These adversaries can be passive or active, internal or external, computationally restrained or unrestrained, and single individual vs. group [6].

In regard to IMD security, we can broadly classify adversaries based on their capabilities as passive eavesdroppers and active attackers [37–39]. The first class of adversaries can only eavesdrop on the radio communication between the legitimate entities to discover unencrypted messages. Sometimes, even if the messages are encrypted, passive adversaries may observe patterns to violate the privacy of communicating parties, such as learning the existence of IMD.

On the other hand, active attackers can replay, modify, or delete messages in addition to possessing all of the capabilities of passive adversaries. These are the most dangerous types of adversaries that can bring life-threatening attacks to IMD-enabled systems. Adversaries in this category can execute replay attacks by forwarding exchanged messages later, changing critical settings of the implants by producing new commands, and exhausting the battery life of IMDs.

Different researchers have studied various security and privacy issues that challenge the normal operations of IMDs along with various proposed solutions that can be generally categorized as auditing-alone solutions, cryptographic solutions, and access control schemes [6]. The first category refers to solutions that solely depend on the access logs for the IMD. However, such techniques may not be suitable, as they cannot withstand active attacks if not used with other techniques such as access control mechanisms. The second measure utilizes cryptographic rudiments such as asymmetric-key cryptography, symmetric-key cryptography, and cryptographic hash functions. Three problems have been identified concerning the cryptographic solutions for IMDs [40]—the difficulty of implementation as most of the IMDs are already implanted in the human body, challenging to authenticate doctors during emergencies in which the patient is unconscious, and difficulty in maintaining the hardware and software of the implanted devices. The third solution refers to schemes that make use of access control help to protect IMDs from unauthorized access. The noticeable weakness in this solution is the difficulty of access during an emergency [6].

4. Formal Security Verification

Checking the safety of security protocols via a formal approach boosts users' confidence, giving more convincing proof than its informal counterpart. When it comes to security protocols, such techniques may be divided into three categories: modal logic, model checkers, and theorem provers. This section will use one from the variants of modal logic (BAN logic) and another from model checking (AVISPA) to perform formal security verification for the authentication schemes proposed to safeguard IMDs. It is worth mentioning that the last two IMD authentication protocols (shown in Sections 4.3.6 and 4.3.7) have also been analyzed, in [41,42], by the same authors.

4.1. BAN Logic Based Formal Security Verification

BAN logic uses logic of beliefs to analyze authentication protocols by following its own rules. First, the messages exchanged between the participants of the protocol are idealized. Then, reasonable assumptions will be formulated, and the objectives that the protocol intends to meet are defined. Finally, a derivation step follows where the BAN logic rules are used together with the assumptions and the intermediate results to reach the goals. Figure 2 shows a typical procedure of carrying out formal analysis using BAN logic. The BAN logic symbols and rules are shown in Tables 1 and 2, respectively.

Table 1. BAN logic notations.

Notation	Meaning
M believes U	M believes that the message U is true
M sees U	M receives the message U at any point in time
M said U	M previously sent the message U
M controls U	M has jurisdiction over U
Fresh (U)	U is fresh
$M \overset{S}{\leftrightarrow} N$	S is a secret key shared between M and N
$\overset{S}{\rightarrow} M$	S is the M's public key
$M \overset{S}{\Leftrightarrow} N$	S is a shared secret between M and N.
$\{U\}_K$	U is encrypted with a key K
U, V	U is combined with V

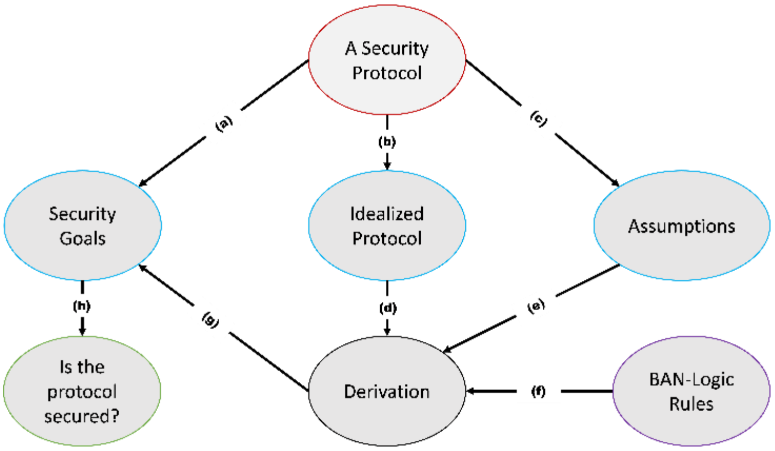


Figure 2. A typical BAN logic formal analysis procedure. (**a**) Security goals are extracted from the protocol's security requirements. (**b**) The security protocol is put in idealized form. (**c**) Realistic assumptions about the protocol is made. (**d**–**f**) Derivation uses these inputs to derive the stated goals. (**g**) The security goals are checked if the derivation satisfies them. (**h**) Based on the results of (**g**), the protocol is validated as safe or not.

Table 2. BAN logic rules.

Rule Name	**Rule**
Message Meaning Rule (MM)	$\frac{\text{M believes M}\overset{S}{\leftrightarrow}\text{N, M sees } \{U\}_S}{\text{M believes N said U}}$ $\frac{\text{M believes M}\overset{S}{\Leftrightarrow}\text{N,M sees } \langle U\rangle_S}{\text{M believes N said U}}$ $\frac{\text{M believes } \overset{S}{\rightarrow}\text{N,M sees } \{U\}_{L-1}}{\text{M believes N said U}}$
Nonce Verification (NV) Rule	$\frac{\text{M believes \#(U), M believes N said U}}{\text{M believes N believes U}}$
Jurisdiction (JR) Rule	$\frac{\text{M believes N controls U, M believes N believes U}}{\text{M believes U}}$
Freshness (FR) Rule	$\frac{\text{M believes fresh(U)}}{\text{M believes fresh(U,V)}}$
Decomposition (DR) Rule	$\frac{\text{M sees (U,V)}}{\text{M sees U}}$
Belief Conjunction (BC) Rule	$\frac{\text{M believes U,M believes V}}{\text{M believes (U,V)}}$ $\frac{\text{M believes N believes (U,V)}}{\text{M believes N believes U}}$ $\frac{\text{M believes N said (U,V)}}{\text{M believes N said U}}$
Diffie–Hellman (DH) Rule	$\frac{\text{M believes N said } \overset{g^V}{\rightarrow}\text{N,M believes } \overset{g^U}{\rightarrow}\text{M}}{\text{M believes M}\overset{g^{UV}}{\leftrightarrow}\text{ N}}$ $\frac{\text{M believes N said } \overset{g^V}{\rightarrow}\text{N,M believes } \overset{g^U}{\rightarrow}\text{M}}{\text{M believes M}\overset{g^{UV}}{\Leftrightarrow}\text{N}}$

4.2. *AVISPA Based Formal Security Analysis*

The previous section shows that BAN logic has been extensively used to verify authentication protocols by transforming them into a particular format and validating them through different logical rules. Unfortunately, BAN logic has limitations in accurately specifying a protocol in the idealization phase [21,43]. For that reason, most authentication protocols use automated formal security verification tools alongside BAN logic.

AVISPA provides a language called the high-level protocol specification language (HLPSL) [44] for describing security protocols and specifying their intended security properties, as well as a set of tools to validate them formally. An hlpsl2if translates the HLPSL specification into the Intermediate Format (IF). IF is a lower-level language that is read directly by the back-ends of the AVISPA Tool. The IF specification of a protocol is then input to the back-ends of the AVISPA Tool to analyze the stated security goals. Figure 3 shows this process.

The HLPSL specification is consists of basic roles, transitions, and composed roles used in three modules: role, session, and environment. Basic role refers to the specification of each of the modeled protocol participants and the initially known information as a parameter. These roles are then called to specify how the resulting participants interact by connecting various basic roles into a composed role. The transition part of an HLPSL specification encompasses a set of transitions between different roles. Each transition symbolizes the acceptance of a message and the sending of a response message.

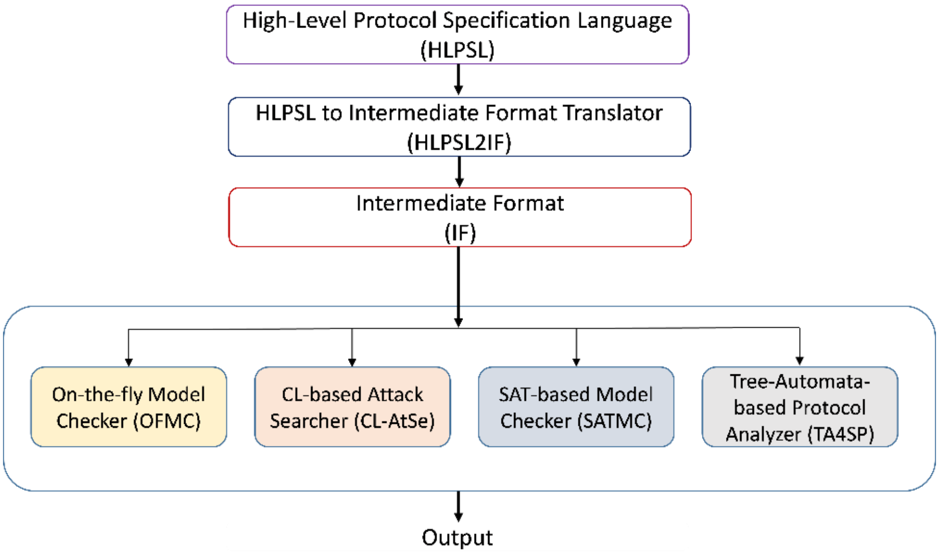

High-Level Protocol Specification Language (HLPSL)
HLPSL to Intermediate Format Translator (HLPSL2IF)
Intermediate Format (IF)
On-the-fly Model Checker (OFMC)
CL-based Attack Searcher (CL-AtSe)
SAT-based Model Checker (SATMC)
Tree-Automata-based Protocol Analyzer (TA4SP)
Output

Figure 3. AVISPA system structure.

4.3. Formal Security Analysis of IMD Authentication Protocols

4.3.1. Khan et al.'s Protocol

The protocol proposed by Khan et al. [23] is a privacy-preserving key agreement protocol for WBANs. The protocol has four main participants: the system administrator (SA), the hub node (HN), the intermediary nodes (IN), and the normal nodes (N). HN is often considered a trusted high-end server that does not have computing resource constraints. The Ns are implanted sensors with computational limitations. The intermediary nodes have better processing, battery, and storage than Ns, and they are placed between HN and Ns to relay traffic. Furthermore, the protocol is executed in three main phases: initialization, registration, and authentication. Figure 4 shows the final phase of the protocol. Figure 5 presents the OFMC and CL-AtSe back-end results of the protocol.

1. BAN logic based Formal Security Analysis

- **Idealization**

(I1) $\mathrm{SN} \rightarrow \mathrm{HN} : \langle \mathrm{id}'_{\mathrm{N}}, \mathrm{r}_{\mathrm{N}}, \mathrm{t}_{\mathrm{N}}, \mathrm{SN} \overset{\mathrm{x_N}}{\leftrightarrow} \mathrm{HN} \rangle_{\mathrm{SN} \overset{\mathrm{id_N}}{\leftrightarrow} \mathrm{HN}}$

(I2) $\mathrm{HN} \rightarrow \mathrm{SN} : \langle \mathrm{r}_{\mathrm{N}}, \mathrm{f}_{\mathrm{N}}, \mathrm{SN} \overset{\mathrm{x_N}}{\leftrightarrow} \mathrm{HN}, \mathrm{SN} \overset{\mathrm{ks}}{\leftrightarrow} \mathrm{HN} \rangle_{\mathrm{SN} \overset{\mathrm{id_N}}{\leftrightarrow} \mathrm{HN}}$

- **Assumption**

(A1) HN believes SN $\overset{\mathrm{id_N}}{\leftrightarrow}$ HN
(A2) HN believes fresh$(\mathrm{t_N})$
(A3) HN believes SN controls $\mathrm{id}'_{\mathrm{N}}$
(A4) HN believes SN controls SN $\overset{\mathrm{x_N}}{\leftrightarrow}$ HN
(A5) SN believes SN $\overset{\mathrm{id_N}}{\leftrightarrow}$ HN
(A6) SN believes fresh$(\mathrm{f_N})$
(A7) SN believes HN controls SN $\overset{\mathrm{ks}}{\leftrightarrow}$ HN

- **Goals**

(G1) HN believes N belives $\mathrm{id'}_N$

(G2) HN believes $\mathrm{id'}_N$

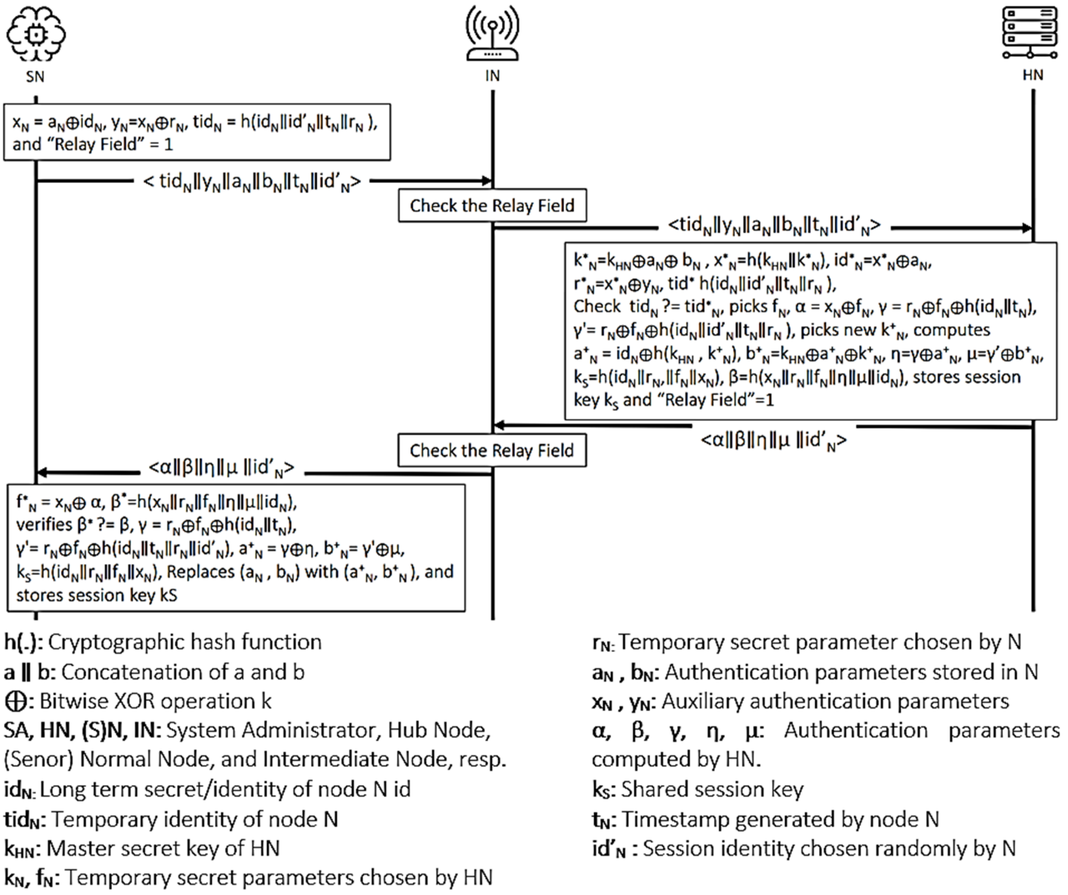
(G3) HN believes SN belives $\mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN}$

(G4) HN belives $\mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN}$

(G5) SN believes HN belives $\mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN}$

(G6) SN believes HN belives $\mathrm{SN} \overset{k_s}{\leftrightarrows} \mathrm{HN}$

(G7) SN belives $\mathrm{SN} \overset{k_s}{\leftrightarrows} \mathrm{HN}$



SN
IN
HN
$x_N = a_N \oplus id_N$, $y_N = x_N \oplus r_N$, $tid_N = h(id_N \| id'_N \| t_N \| r_N)$, and "Relay Field" = 1
$< tid_N \| y_N \| a_N \| b_N \| t_N \| id'_N >$
Check the Relay Field
$<tid_N \| y_N \| a_N \| b_N \| t_N \| id'_N>$
$k^*_N = k_{HN} \oplus a_N \oplus b_N$, $x^*_N = h(k_{HN} \| k^*_N)$, $id^*_N = x^*_N \oplus a_N$, $r^*_N = x^*_N \oplus y_N$, tid* $h(id_N \| id'_N \| t_N \| r_N)$, Check tid_N ?= tid^*_N, picks f_N, $\alpha = x_N \oplus f_N$, $\gamma = r_N \oplus f_N \oplus h(id_N \| t_N)$, $\gamma' = r_N \oplus f_N \oplus h(id_N \| id'_N \| t_N \| r_N)$, picks new k^+_N, computes $a^+_N = id_N \oplus h(k_{HN}, k^+_N)$, $b^+_N = k_{HN} \oplus a^+_N \oplus k^+_N$, $\eta = \gamma \oplus a^+_N$, $\mu = \gamma' \oplus b^+_N$, $k_S = h(id_N \| r_N, \| f_N \| x_N)$, $\beta = h(x_N \| r_N \| f_N \| \eta \| \mu \| id_N)$, stores session key k_S and "Relay Field"=1
$<\alpha \| \beta \| \eta \| \mu \; \| id'_N>$
Check the Relay Field
$<\alpha \| \beta \| \eta \| \mu \; \| id'_N>$
$f^*_N = x_N \oplus \alpha$, $\beta^* = h(x_N \| r_N \| f_N \| \eta \| \mu \| id_N)$, verifies β^* ?= β, $\gamma = r_N \oplus f_N \oplus h(id_N \| t_N)$, $\gamma' = r_N \oplus f_N \oplus h(id_N \| t_N \| r_N \| id'_N)$, $a^+_N = \gamma \oplus \eta$, $b^+_N = \gamma' \oplus \mu$, $k_S = h(id_N \| r_N \| f_N \| x_N)$, Replaces (a_N, b_N) with (a^+_N, b^+_N), and stores session key kS
h(.): Cryptographic hash function
a ‖ b: Concatenation of a and b
⊕: Bitwise XOR operation k
SA, HN, (S)N, IN: System Administrator, Hub Node, (Senor) Normal Node, and Intermediate Node, resp.
id_N: Long term secret/identity of node N id
tid_N: Temporary identity of node N
k_{HN}: Master secret key of HN
k_N, f_N: Temporary secret parameters chosen by HN
r_N: Temporary secret parameter chosen by N
a_N, b_N: Authentication parameters stored in N
x_N, y_N: Auxiliary authentication parameters
α, β, γ, η, μ: Authentication parameters computed by HN.
k_S: Shared session key
t_N: Timestamp generated by node N
id'_N : Session identity chosen randomly by N

Figure 4. Khan et al.'s protocol.

- **Derivations**

(D1) HN sees $\langle \mathrm{id'}_N,\ r_N,\ t_N, \mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN} \rangle_{\mathrm{SN} \overset{id_N}{\leftrightarrows} \mathrm{HN}}$ (I1)

(D2) HN believes SN said $\left[\mathrm{id'}_N,\ r_N,\ t_N, \mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN}\right]$ By (D1), (A1), MM

(D3) HN believes SN belives $\left[\mathrm{id'}_N,\ r_N,\ t_N, \mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN}\right]$ By (D2), (A2), NV, FR

(D4) HN believes SN belives $\mathrm{id'}_N$ By (D3), BC

(D5) HN believes $\mathrm{id'}_N$ By (D4), (A3), JR.

(D6) HN believes SN belives $\mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN}$ By (D3), BC

(D7) HN belives $\mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN}$ By (D6), (A4), JR

(D8) SN sees $\langle r_N, f_N, \mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN},\ \mathrm{SN} \overset{k_s}{\leftrightarrows} \mathrm{HN} \rangle_{\mathrm{SN} \overset{id_N}{\leftrightarrows} \mathrm{HN}}$ (I2)

(D9) SN believes HN said $\left[r_N, f_N, \mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN},\ \mathrm{SN} \overset{k_s}{\leftrightarrows} \mathrm{HN} \right]$ By (D8), (A5), MM

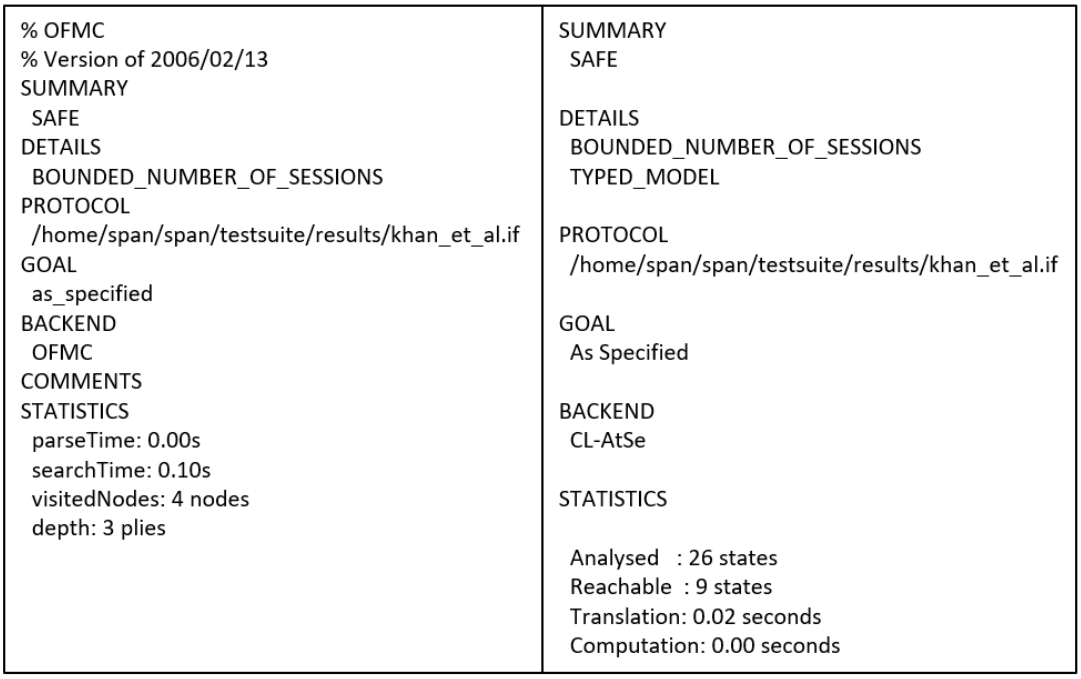
(D10) SN believes HN belives $\left[r_N, f_N, \mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN},\ \mathrm{SN} \overset{k_s}{\leftrightarrows} \mathrm{HN} \right]$ By (D9), (A6), NV, FR

(D11) SN believes HN belives $\mathrm{SN} \overset{x_N}{\leftrightarrows} \mathrm{HN}$ By (D10), BC

(D12) SN believes HN believes $\mathrm{SN} \overset{k_s}{\leftrightarrows} \mathrm{HN}$ By (D10), BC

(D13) SN believes $\mathrm{SN} \overset{k_s}{\leftrightarrows} \mathrm{HN}$ By (D12), (A7), JR

2. AVISPA based Formal Security Analysis Result



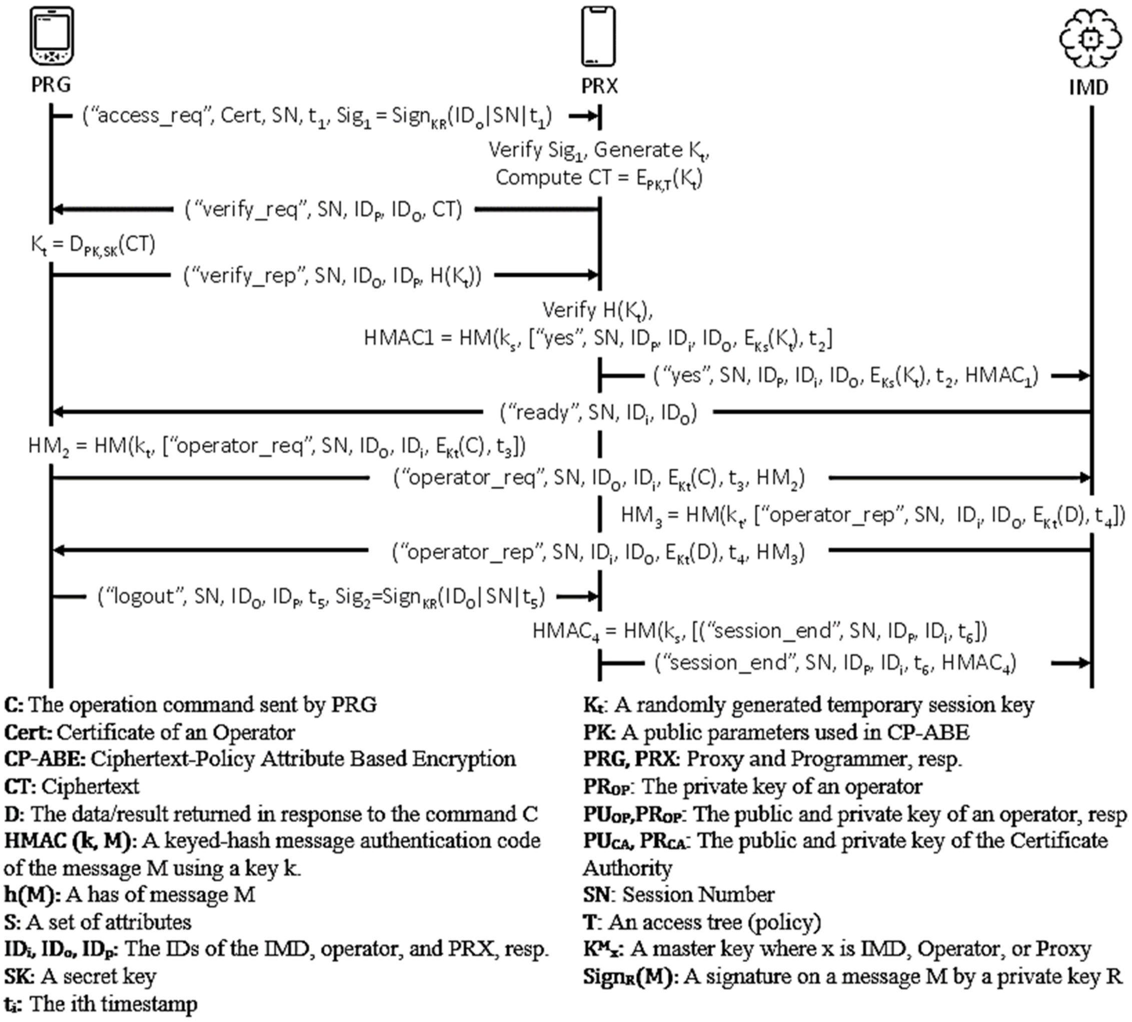
```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/khan_et_al.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.10s
 visitedNodes: 4 nodes
 depth: 3 plies
```

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/khan_et_al.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 26 states
 Reachable  : 9 states
 Translation: 0.02 seconds
 Computation: 0.00 seconds
```

Figure 5. AVISPA result of Khan et al.'s protocol.

4.3.2. Wu et al.'s Protocol

This protocol [24] is a proxy-based access control protocol that uses attribute-based encryption, particularly the ciphertext policy attribute-based encryption (CP-ABE). The protocol is executed by three participants—IMD, operator, and proxy. The IMDs have unique identifications ID_i and a master key $K_i{}^M$, which is only used for the initial pairing process with the proxy. All operators with the public parameters PK used in CP-ABE, unique identifications ID_o, a public and private key pair (PU_{OP} and PR_{OP}, respectively), and a certificate Cert must first be registered at a Central Health Authority (CHA). The CHA will then generate the secret key SK. The operator uses a programmer to communicate with the IMD and proxy after it obtains the required information by manual inputting or reading in from a smart card. With the identification of ID_p and connection with an IMD programmer through an audio cable, the proxy device performs the access control for the IMD. Figure 6 shows the flow of messages in the protocol. Figure 7 illustrates the OFMC and CL-AtSe back-end results of the protocol.


PRG
PRX
IMD
("access_req", Cert, SN, t1, Sig1 = SignKR(IDo|SN|t1)
Verify Sig1, Generate Kt,
Compute CT = EPK,T(Kt)
("verify_req", SN, IDP, IDO, CT)
Kt = DPK,SK(CT)
("verify_rep", SN, IDO, IDP, H(Kt))
Verify H(Kt),
HMAC1 = HM(ks, ["yes", SN, IDP, IDi, IDO, EKs(Kt), t2]
("yes", SN, IDP, IDi, IDO, EKs(Kt), t2, HMAC1)
("ready", SN, IDi, IDO)
HM2 = HM(kt, ["operator_req", SN, IDO, IDi, EKt(C), t3])
("operator_req", SN, IDO, IDi, EKt(C), t3, HM2)
HM3 = HM(kt, ["operator_rep", SN, IDi, IDO, EKt(D), t4])
("operator_rep", SN, IDi, IDO, EKt(D), t4, HM3)
("logout", SN, IDO, IDP, t5, Sig2=SignKR(IDO|SN|t5)
HMAC4 = HM(ks, [("session_end", SN, IDP, IDi, t6])
("session_end", SN, IDP, IDi, t6, HMAC4)

C: The operation command sent by PRG
Cert: Certificate of an Operator
CP-ABE: Ciphertext-Policy Attribute Based Encryption
CT: Ciphertext
D: The data/result returned in response to the command C
HMAC (k, M): A keyed-hash message authentication code of the message M using a key k.
h(M): A has of message M
S: A set of attributes
IDi, IDo, IDp: The IDs of the IMD, operator, and PRX, resp.
SK: A secret key
ti: The ith timestamp
Kt: A randomly generated temporary session key
PK: A public parameters used in CP-ABE
PRG, PRX: Proxy and Programmer, resp.
PROP: The private key of an operator
PUOP,PROP: The public and private key of an operator, resp
PUCA, PRCA: The public and private key of the Certificate Authority
SN: Session Number
T: An access tree (policy)
KMx: A master key where x is IMD, Operator, or Proxy
SignR(M): A signature on a message M by a private key R

Figure 6. Wu et al.'s protocol.

1. BAN logic-based formal security analysis.

- **Idealization**

(I1) $\text{PRG} \rightarrow \text{PRX} : \langle \text{ID}_\text{O}, \text{SN}, \ t_1 \rangle_{\text{PU}^{-1}{}_{\text{OP}}}$

(I2) $\text{PRX} \rightarrow \text{PRG} : \langle \text{PRG} \overset{\text{K}_\text{t}}{\leftrightarrow} \text{IMD} \rangle_{\text{PKT}}$

(I3) $\text{PRX} \rightarrow \text{IMD} : \langle \text{PRG} \overset{\text{K}_\text{t}}{\leftrightarrow} \text{IMD}, \rangle_{\text{PRX} \overset{\text{K}_\text{S}}{\leftrightarrow} \text{IMD}}, \langle \text{SN}, \ \text{ID}_\text{P}, \text{ID}_\text{I}, \ \text{ID}_\text{O}, \ t_2 \rangle_{\text{PRX} \overset{\text{K}_\text{S}}{\leftrightarrow} \text{IMD}}$

(I4) $\text{PRG} \rightarrow \text{IMD} : \langle \text{PRG} \overset{\text{K}_\text{t}}{\leftrightarrow} \text{IMD}, \ \text{C} \rangle_{\text{PRG} \overset{\text{K}_\text{t}}{\leftrightarrow} \text{IMD}}, \langle \ \text{PRG} \overset{\text{K}_\text{t}}{\leftrightarrow} \text{IMD}, \ \text{SN}, \ \text{ID}_\text{O}, \text{ID}_\text{I}, \ t_3 \rangle_{\text{PRG} \overset{\text{K}_\text{t}}{\leftrightarrow} \text{IMD}}$

(I5) $\text{IMD} \rightarrow \text{PRG} : \langle \text{PRG} \overset{\text{K}_\text{t}}{\leftrightarrow} \text{IMD}, \ \text{D} \rangle_{\text{PRG} \overset{\text{K}_\text{t}}{\leftrightarrow} \text{IMD}}, \langle \ \text{PRG} \overset{\text{K}_\text{t}}{\leftrightarrow} \text{IMD}, \ \text{SN}, \ \text{ID}_\text{I}, \text{ID}_\text{O}, \ t_4 \rangle_{\text{PRG} \overset{\text{K}_\text{t}}{\leftrightarrow} \text{IMD}}$

- **Assumption**

(A1) PRX believes $\overset{\text{PU}_{\text{OP}}}{\rightarrow}$ PRG

(A2) PRX believes $\text{fresh}(t_1)$

(A3) PRX believes PRG Controls ID_O

(A4) PRX believes $\overset{\text{PKT}^{-1}}{\rightarrow}$ PRG

(A5) PRG believes $\text{fresh}(\text{K}_\text{t})$

(A6) PRG believes PRX Controls PRX $\overset{\text{K}_\text{t}}{\leftrightarrow}$ PRG

(A7) IMD believes PRX $\overset{\text{K}_\text{s}}{\leftrightarrow}$ IMD

(A8) IMD believes fresh (K_t)

(A9) IMD believes fresh(t_2)

(A10) IMD believes PRX Controls PRX $\overset{K_t}{\leftrightarrow}$ IMD

(A11) IMD believes PRX Controls ID_P

(A12) IMD believes fresh(t_3)

(A13) IMD believes PRG Controls ID_O

(A14) IMD believes fresh(t_4)

(A15) PRG believes IMD Controls ID_I

- **Goals**

(G1) PRX believes ID_O

(G2) PRG believes PRX believes PRG $\overset{K_t}{\leftrightarrow}$ IMD

(G3) PRG believes PRG $\overset{K_t}{\leftrightarrow}$ IMD

(G4) IMD believes PRX believes PRG $\overset{K_t}{\leftrightarrow}$ IMD

(G5) IMD believes PRG $\overset{K_t}{\leftrightarrow}$ IMD

(G6) IMD believes ID_P

(G7) IMD believes ID_O

(G8) IMD believes PRG believes PRG $\overset{K_t}{\leftrightarrow}$ IMD

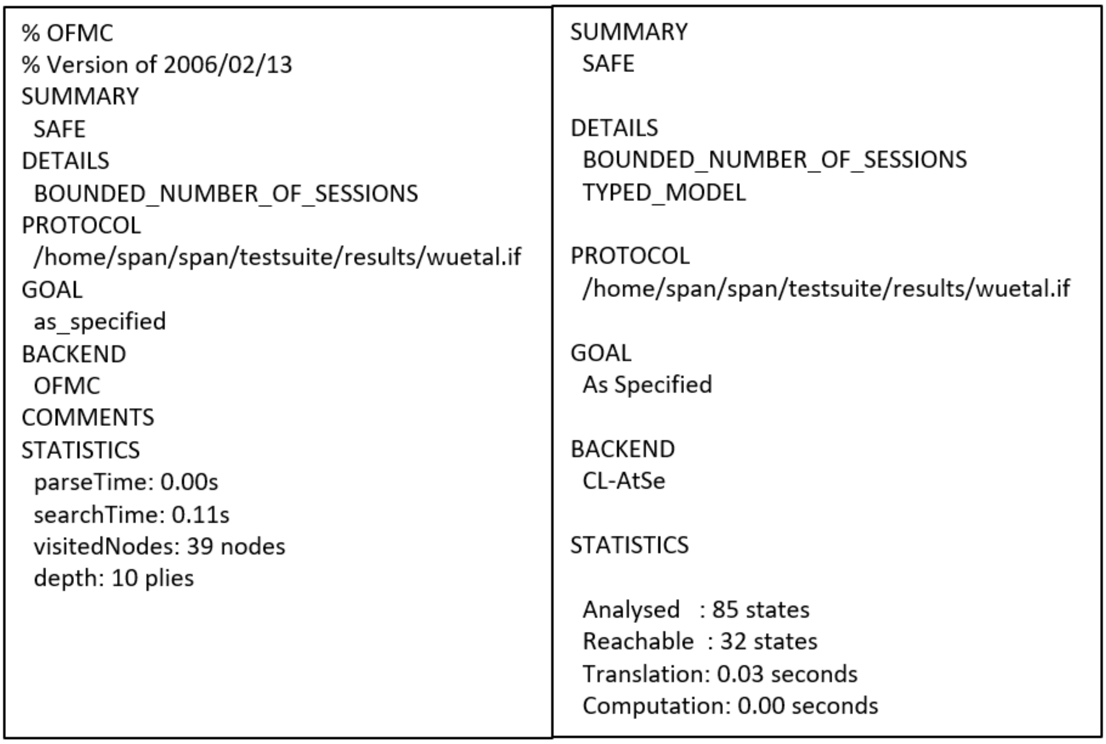
(G9) PRG believes IMD believes PRG $\overset{K_t}{\leftrightarrow}$ IMD

(G10) PRG believes ID_I

- **Derivations**

(D1)	PRX sees $\langle ID_O, SN,\ t_1\rangle_{PU^{-1}{}_{OP}}$	(I1)
(D2)	PRX believes PRG said $[ID_O,\ SN,\ t_1]$	By (D1), (A1), MM
(D3)	PRX believes PRG believes $[ID_O,\ SN,\ t_1]$	By (D2), (A2), NV, FR
(D4)	PRX believes PRG believes ID_O	By (D3), BC
(D5)	PRX believes ID_O	By (D4), (A3), JR
(D6)	PRG sees $\langle PRG\ \overset{K_t}{\leftrightarrow}\ IMD\rangle_{PKT}$	(I2)
(D7)	PRG believes PRX said PRG $\overset{K_t}{\leftrightarrow}$ IMD	By (D6), (A4), JR
(D8)	PRG believes PRX believes PRG $\overset{K_t}{\leftrightarrow}$ IMD	By (D7), (A5), NV, FR
(D9)	PRG believes PRG $\overset{K_t}{\leftrightarrow}$ IMD	By (D8), (A6), JR
(D10)	IMD sees $\langle PRG \overset{K_t}{\leftrightarrow} IMD\rangle_{PRX \overset{K_S}{\leftrightarrow} IMD}$, $\langle SN,\ ID_P, ID_I,\ ID_O,\ t_2\rangle_{PRX \overset{K_S}{\leftrightarrow} IMD}$	(I3)
(D11)	IMD believes PRX said PRG $\overset{K_t}{\leftrightarrow}$ IMD	By (D10), DR, (A7), MM
(D12)	IMD believes PRX said $[SN,\ ID_P, ID_I,\ ID_O,\ t_2]$	By (D10), DR, (A7), MM
(D13)	IMD believes PRX believes PRG $\overset{K_t}{\leftrightarrow}$ IMD	By (D11), (A8), NV, FR
(D14)	IMD believes PRX believes $[SN,\ ID_P, ID_I,\ ID_O,\ t_2]$	By (D12), (A9), NV, FR
(D15)	IMD believes PRX believes ID_P	By (D14), BC
(D16)	IMD believes PRG $\overset{K_t}{\leftrightarrow}$ IMD	By (D13), (A10), JR
(D17)	IMD believes ID_P	By (D15), (A11), JR
(D18)	IMD sees $\langle PRG \overset{K_t}{\leftrightarrow} IMD,\ SN,\ ID_O, ID_I,\ t_3\rangle_{PRG \overset{K_t}{\leftrightarrow} IMD}$	By (I4), DR
(D19)	IMD believes PRG said $\left[PRG \overset{K_t}{\leftrightarrow} IMD,\ SN,\ ID_O, ID_I,\ t_3\right]$	By (D18), (D16), MM
(D20)	IMD believes PRG believes $\left[PRG \overset{K_t}{\leftrightarrow} IMD,\ SN,\ ID_O, ID_I,\ t_3\right]$	By (D19), (A12), NV, FR
(D21)	IMD believes PRG believes ID_O	By (D20), BC
(D22)	IMD believes ID_O	By (D21), (A13), JR
(D23)	IMD believes PRG believes PRG $\overset{K_t}{\leftrightarrow}$ IMD	By (D20), BC
(D24)	PRG sees $\langle PRG \overset{K_t}{\leftrightarrow} IMD,\ SN,\ ID_I, ID_O,\ t_4\rangle_{PRG \overset{K_t}{\leftrightarrow} IMD}$	By (I5), DR
(D25)	PRG believes IMD said $\left[PRG \overset{K_t}{\leftrightarrow} IMD,\ SN,\ ID_I, ID_O,\ t_4\right]$	By (D24), (D9), MM
(D26)	PRG believes IMD believes $\left[PRG \overset{K_t}{\leftrightarrow} IMD,\ SN,\ ID_I, ID_O,\ t_4\right]$	By (D25), (A14), NV, FR
(D27)	PRG believes IMD believes PRG $\overset{K_t}{\leftrightarrow}$ IMD	By (D26), BC
(D28)	PRG believes IMD believes ID_I	By (D26), BC
(D29)	PRG believes ID_I	By (D28),(I15), JR

2. AVISPA-based formal security analysis result.



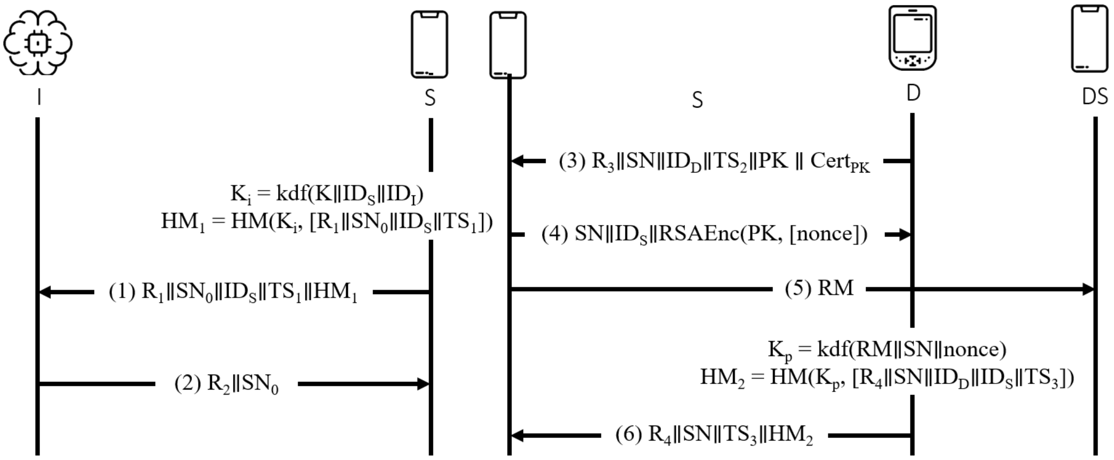
```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/wuetal.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.11s
 visitedNodes: 39 nodes
 depth: 10 plies
```

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/wuetal.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 85 states
 Reachable  : 32 states
 Translation: 0.03 seconds
 Computation: 0.00 seconds
```

Figure 7. AVISPA result of Wu et al.'s protocol.

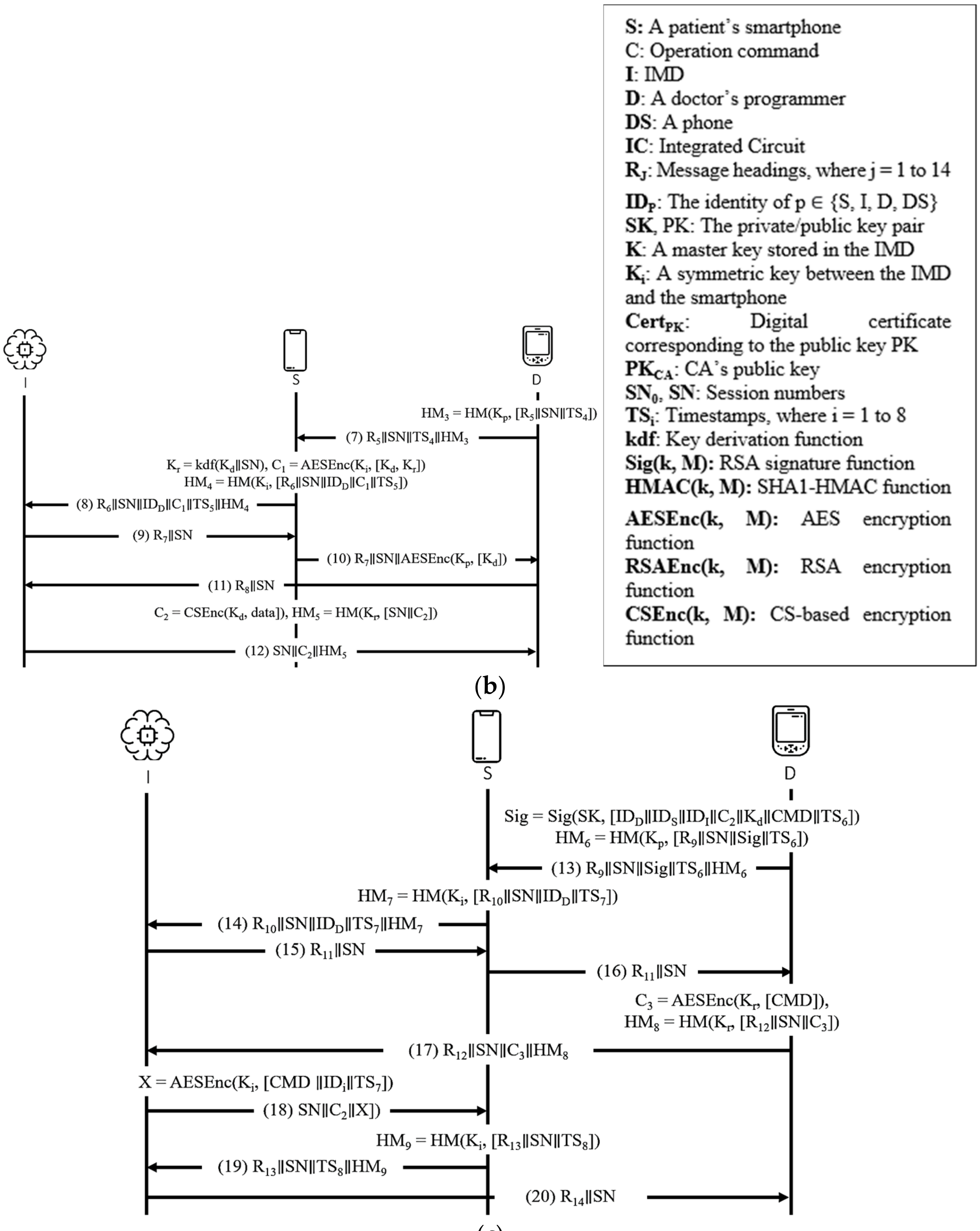
4.3.3. Chi et al.'s Protocol

This protocol [25] uses a compressing-based encryption mechanism and public key infrastructure, and other cryptographic protocols, such as RSA, AES, and HMAC. The protocol comprises three participants—IMD, smartphone, and programmer. The IMD communicates with the patient's smartphone via Bluetooth, and it interacts with the doctor's programmer through the wireless medium. The smartphone refers to both the patient and doctor smartphones, in which the patient's smartphone links with the IMD utilizing Bluetooth and connects with a programmer wirelessly. The protocol involves four stages—initialization, pairing, authentication, and authorization, as shown in Figures 8 and 9 presents the OFMC and CL-AtSe back-end results of the protocol.


I
S
S
D
DS
(3) $R_3\|SN\|ID_D\|TS_2\|PK \| Cert_{PK}$
$K_i = kdf(K\|ID_S\|ID_I)$
$HM_1 = HM(K_i, [R_1\|SN_0\|ID_S\|TS_1])$
(4) $SN\|ID_S\|RSAEnc(PK, [nonce])$
(1) $R_1\|SN_0\|ID_S\|TS_1\|HM_1$
(5) RM
$K_p = kdf(RM\|SN\|nonce)$
$HM_2 = HM(K_p, [R_4\|SN\|ID_D\|ID_S\|TS_3])$
(2) $R_2\|SN_0$
(6) $R_4\|SN\|TS_3\|HM_2$

(**a**)

Figure 8. *Cont.*



S: A patient's smartphone
C: Operation command
I: IMD
D: A doctor's programmer
DS: A phone
IC: Integrated Circuit
$\mathbf{R_J}$: Message headings, where j = 1 to 14
$\mathbf{ID_P}$: The identity of p ∈ {S, I, D, DS}
SK, PK: The private/public key pair
K: A master key stored in the IMD
$\mathbf{K_i}$: A symmetric key between the IMD and the smartphone
$\mathbf{Cert_{PK}}$: Digital certificate corresponding to the public key PK
$\mathbf{PK_{CA}}$: CA's public key
$\mathbf{SN_0}$, **SN**: Session numbers
$\mathbf{TS_i}$: Timestamps, where i = 1 to 8
kdf: Key derivation function
Sig(k, M): RSA signature function
HMAC(k, M): SHA1-HMAC function
AESEnc(k, M): AES encryption function
RSAEnc(k, M): RSA encryption function
CSEnc(k, M): CS-based encryption function

I
S
D
$HM_3 = HM(K_p, [R_5\|SN\|TS_4])$
(7) $R_5\|SN\|TS_4\|HM_3$
$K_r = kdf(K_d\|SN)$, $C_1 = AESEnc(K_i, [K_d, K_r])$
$HM_4 = HM(K_i, [R_6\|SN\|ID_D\|C_1\|TS_5])$
(8) $R_6\|SN\|ID_D\|C_1\|TS_5\|HM_4$
(9) $R_7\|SN$
(10) $R_7\|SN\|AESEnc(K_p, [K_d])$
(11) $R_8\|SN$
$C_2 = CSEnc(K_d, data])$, $HM_5 = HM(K_r, [SN\|C_2])$
(12) $SN\|C_2\|HM_5$
(b)
I
S
D
$Sig = Sig(SK, [ID_D\|ID_S\|ID_I\|C_2\|K_d\|CMD\|TS_6])$
$HM_6 = HM(K_p, [R_9\|SN\|Sig\|TS_6])$
(13) $R_9\|SN\|Sig\|TS_6\|HM_6$
$HM_7 = HM(K_i, [R_{10}\|SN\|ID_D\|TS_7])$
(14) $R_{10}\|SN\|ID_D\|TS_7\|HM_7$
(15) $R_{11}\|SN$
(16) $R_{11}\|SN$
$C_3 = AESEnc(K_r, [CMD])$,
$HM_8 = HM(K_r, [R_{12}\|SN\|C_3])$
(17) $R_{12}\|SN\|C_3\|HM_8$
$X = AESEnc(K_i, [CMD \|ID_i\|TS_7])$
(18) $SN\|C_2\|X])$
$HM_9 = HM(K_i, [R_{13}\|SN\|TS_8])$
(19) $R_{13}\|SN\|TS_8\|HM_9$
(20) $R_{14}\|SN$
(c)

Figure 8. Chi et al.'s protocol. (**a**) Initialization phase. (**b**) Pairing phase. (**c**) Authentication and authorization phase.

1. BAN logic-based formal security analysis.

- **Idealization**

(I1) $S \rightarrow I : \langle R_1, SN_O, ID_S, TS_1, S \overset{K_i}{\leftrightarrow} I \rangle_{S \overset{K_i}{\leftrightarrow} I}$

(I2) $D \rightarrow S : \langle R_3, SN, ID_D, TS_2 \rangle_{PK^{-1}}$

(I3) $S \rightarrow D : \langle nonce \rangle_{PK}$

(I4) $D \rightarrow S : \langle R_4, SN, ID_D, ID_S, TS_3, D \overset{K_p}{\leftrightarrow} S \rangle_{D \overset{K_p}{\leftrightarrow} S}$

(I5) $S \rightarrow I : \langle\, R_6, SN, ID_D, C_1, TS_{5_{S \overset{K_i}{\leftrightarrow} I}}, I \overset{K_d}{\leftrightarrow} D, I \overset{K_r}{\leftrightarrow} D \rangle_{S \overset{K_i}{\leftrightarrow} I}$

(I6) $S \rightarrow D : \langle I \overset{K_d}{\leftrightarrow} D \rangle_{D \overset{K_p}{\leftrightarrow} S}$

(I7) $I \rightarrow D : \langle SN, C_2, I \overset{K_r}{\leftrightarrow} D, \rangle_{I \overset{K_r}{\leftrightarrow} D}, \langle data, I \overset{K_d}{\leftrightarrow} D \rangle_{I \overset{K_d}{\leftrightarrow} D}$

(I8) $I \rightarrow S : \langle CMD, ID_I, TS_7 \rangle_{S \overset{K_i}{\leftrightarrow} I}$

- **Assumption**

(A1) I believes $S \overset{K}{\leftrightarrow} I$

(A2) I believes ID_I

(A3) I believes ID_S

(A4) I believes fresh(TS_1)

(A5) S believes $\overset{PK}{\rightarrow} D$

(A6) S believes fresh(TS_2)

(A7) S believes D Controls SN

(A8) D believes $\overset{PK}{\rightarrow} D$

(A9) D believes fresh(nonce)

(A10) D believes S Controls nonce

(A11) D believes RM

(A12) D believes SN

(A13) S believes RM

(A14) S believes nonce

(A15) S believes fresh(TS_3)

(A16) I believes fresh$\left(I \overset{K_d}{\leftrightarrow} D \right)$

(A17) I believes S Controls $I \overset{K_d}{\leftrightarrow} D$

(A18) I believes S Controls $I \overset{K_r}{\leftrightarrow} D$

(A19) D believes fresh$\left(I \overset{K_d}{\leftrightarrow} D \right)$

(A20) D believes S Controls $I \overset{K_d}{\leftrightarrow} D$

(A21) D believes fresh$\left(I \overset{K_r}{\leftrightarrow} D \right)$

(A22) S believes $S \overset{K_i}{\leftrightarrow} I$

(A23) S believes fresh(TS_7)

- **Goals**

(G1) I believes S belives $S \overset{K_i}{\leftrightarrow} I$

(G2) I belives $S \overset{K_i}{\leftrightarrow} I$

(G3) S believes I belives $S \overset{K_i}{\leftrightarrow} I$

(G4) D believes S belives $D \overset{K_p}{\leftrightarrow} S$

(G5) D belives $D \overset{K_p}{\leftrightarrow} S$

(G6) S believes D belives $D \overset{K_p}{\leftrightarrow} S$

(G7) S belives $D \overset{K_p}{\leftrightarrow} S$

(G8) I believes S belives $D \overset{K_d}{\leftrightarrow} S$

(G9) I believes S belives $D \overset{K_r}{\leftrightarrow} S$

(G10) I belives $D \overset{K_d}{\leftrightarrow} S$

(G11) I belives $D \overset{K_r}{\leftrightarrow} S$

(G12) D believes S belives $D \overset{K_d}{\leftrightarrow} S$

(G13) D belives $D \overset{K_d}{\leftrightarrow} S$

(G14) D belives $D \overset{K_r}{\leftrightarrow} S$

(G15) I believes D belives $D \overset{K_d}{\leftrightarrow} S$

(G16) I believes D belives $D \overset{K_r}{\leftrightarrow} S$

(G17) D believes I belives $D \overset{K_d}{\leftrightarrow} S$

- **Derivations**

(D1)	I sees $\langle R_1,\ SN_O, ID_S, TS_1, S \overset{K_i}{\leftrightarrow} I\rangle_{S\overset{K_i}{\leftrightarrow}I}$	(I1)
(D2)	I believes $S \overset{K_i}{\leftrightarrow} I$	(A1), (A2), (A3), BC
(D3)	I believes S said $\left[R_1,\ SN_O, ID_S, TS_1, S \overset{K_i}{\leftrightarrow} I\right]$	By (D1), (D2), MM
(D4)	I believes S believes $\left[R_1,\ SN_O, ID_S, TS_1, S \overset{K_i}{\leftrightarrow} I\right]$	By (D2), (A4), NV, FR
(D5)	I believes S believes $S \overset{K_i}{\leftrightarrow} I$	By (D4), BC
(D6)	S sees $\langle R_3,\ SN, ID_D, TS_2\rangle_{PK^{-1}}$	(I2)
(D7)	S believes D said $[R_3,\ SN, ID_D, TS_2]$	By (D6), (A5), MM
(D8)	S believes D believes $[R_3,\ SN, ID_D, TS_2]$	By (D7), (A6), NV, FR
(D9)	S believes D believes SN	By (D8), BC
(D10)	S believes SN	By (D9), (A7), JR
(D11)	D sees $\langle \text{nonce}\rangle_{PK}$	(I3)
(D12)	D believes S said [nonce]	By (D11), (A8), MM
(D13)	D believes S believes nonce	By (D12), (A9), NV, FR
(D14)	D believes nonce	By (D13), (A10), JR
(D15)	D belives $D \overset{K_p}{\leftrightarrow} S$	By (D14), (A11), (A12), BC
(D16)	S belives $D \overset{K_p}{\leftrightarrow} S$	By (D10), (A13), (A14), BC
(D17)	S sees $\langle R_4,\ SN, ID_D,\ ID_S, TS_3, D \overset{K_p}{\leftrightarrow} S\rangle_{D\overset{K_p}{\leftrightarrow}S}$	(I4)
(D18)	S believes D said $\left[R_4,\ SN, ID_D,\ ID_S, TS_3, D \overset{K_p}{\leftrightarrow} S\right]$	By (D17), (D16), MM
(D19)	S believes D belives $\left[R_4,\ SN, ID_D,\ ID_S, TS_3, D \overset{K_p}{\leftrightarrow} S\right]$	By (D18), (A15), NV, FR
(D20)	S believes D believes $D \overset{K_p}{\leftrightarrow} S$	By (D19), BC
(D21)	I sees $\langle R_6,\ SN, ID_D, C_1,\ TS_5\rangle_{S\overset{K_i}{\leftrightarrow}I}, \langle I \overset{K_d}{\leftrightarrow} D, I \overset{K_r}{\leftrightarrow} D\rangle_{S\overset{K_i}{\leftrightarrow}I}$	(I5)
(D22)	I sees $\langle I \overset{K_d}{\leftrightarrow} D, I \overset{K_r}{\leftrightarrow} D\rangle_{S\overset{K_i}{\leftrightarrow}I}$	By (D21), DR
(D23)	I believes S said $\left[I \overset{K_d}{\leftrightarrow} D, I \overset{K_r}{\leftrightarrow} D\right]$	By (D22), (D2), MM
(D24)	I believes S belives $\left[I \overset{K_d}{\leftrightarrow} D, I \overset{K_r}{\leftrightarrow} D\right]$	By (D23), (A16), NV, FR
(D25)	I believes S belives $I \overset{K_d}{\leftrightarrow} D$	By (D24), BC
(D26)	I believes S belives $I \overset{K_r}{\leftrightarrow} D$	By (D24), BC
(D27)	I believes $I \overset{K_d}{\leftrightarrow} D$	By (D25), (A17), JR
(D28)	I believes $I \overset{K_r}{\leftrightarrow} D$	By (D26), (A18), JR
(D29)	D sees $\langle I \overset{K_d}{\leftrightarrow} D\rangle_{D\overset{K_p}{\leftrightarrow}S}$	(I6)
(D30)	D believes S said $\left[I \overset{K_d}{\leftrightarrow} D\right]$	By (D30), (A15), MM
(D31)	D believes S belives $\left[I \overset{K_d}{\leftrightarrow} D\right]$	By (D30), (A19), NV, FR
(D32)	D believes S belives $I \overset{K_d}{\leftrightarrow} D$	By (D31), BC
(D33)	D believes $I \overset{K_d}{\leftrightarrow} D$	By (D32), (A20), JR
(D34)	D sees $\langle SN,\ C_2,\ I \overset{K_r}{\leftrightarrow} D\rangle_{I\overset{K_r}{\leftrightarrow}D}, \langle \text{data},\ I \overset{K_d}{\leftrightarrow} D\rangle_{I\overset{K_d}{\leftrightarrow}D}$	(I7)
(D35)	D sees $\langle \text{data},\ I \overset{K_d}{\leftrightarrow} D\rangle_{I\overset{K_d}{\leftrightarrow}D}$	By (D34), DR

(D36) D believes I said $\left[\text{data, } I \overset{K_d}{\leftrightarrow} D\right]$ By (D35), (D33), MM

(D37) D believes I belives $\left[\text{data, } I \overset{K_d}{\leftrightarrow} D\right]$ By (D30), (A19), NV, FR

(D38) D believes I belives $I \overset{K_d}{\leftrightarrow} D$ By (D37), BC

(D39) D sees $\langle SN,\ C_2,\ I \overset{K_r}{\leftrightarrow} D\rangle_{I \overset{K_r}{\leftrightarrow} D}$ By (D34), DR

(D40) D believes $I \overset{K_r}{\leftrightarrow} D$ By (D33), (A12), BC

(D41) D believes I said $\left[SN,\ C_2,\ I \overset{K_r}{\leftrightarrow} D\right]$ By (D39), (D40), MM

(D42) D believes I believes $\left[SN,\ C_2,\ I \overset{K_r}{\leftrightarrow} D\right]$ By (D41), (A21), NV, FR

(D43) D believes I believes $I \overset{K_r}{\leftrightarrow} D$ By (D42), BC

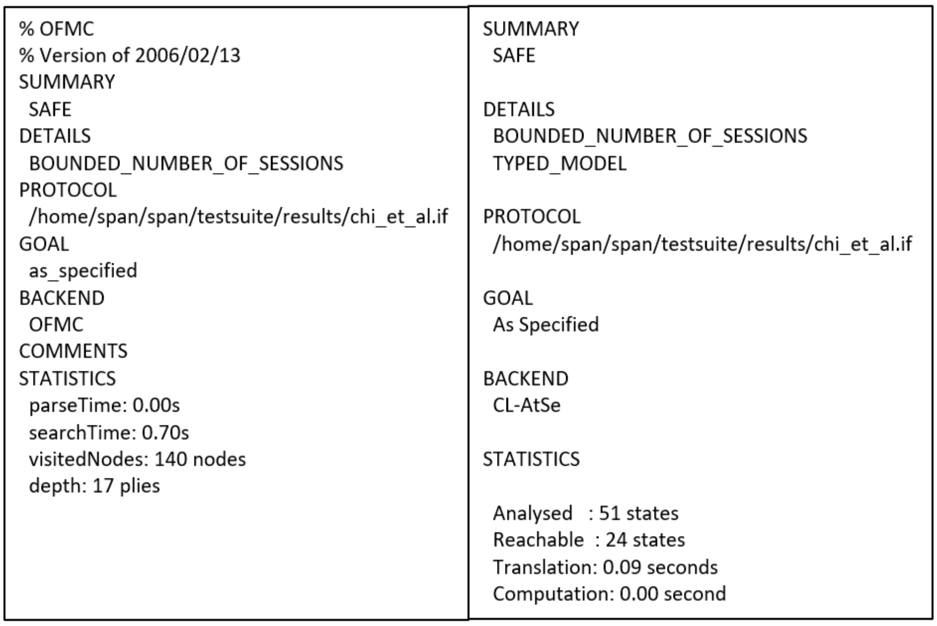
(D44) S sees $\langle CMD,\ ID_I, TS_7,\ S \overset{K_i}{\leftrightarrow} I\rangle_{S \overset{K_i}{\leftrightarrow} I}$ (I8)

(D45) S believes I said $\left[CMD,\ ID_I, TS_7,\ S \overset{K_i}{\leftrightarrow} I\right]$ By (D44), (A22), MM

(D46) S believes I belives $\left[CMD,\ ID_I, TS_7,\ S \overset{K_i}{\leftrightarrow} I\right]$ By (D45), (A23), NV, FR

(D47) S believes I belives $S \overset{K_i}{\leftrightarrow} I$ By (D46), BC

2. AVISPA-based formal security analysis result.



```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/chi_et_al.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.70s
 visitedNodes: 140 nodes
 depth: 17 plies
```

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/chi_et_al.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 51 states
 Reachable  : 24 states
 Translation: 0.09 seconds
 Computation: 0.00 second
```

Figure 9. AVISPA result of Chi et al.'s protocol.

4.3.4. Parvez et al.'s Protocol

The proposed authentication scheme [26] extended the protocol in [45] that comprises of sensors, which are resource-constrained devices that are implanted in (or wearable on) human body; mobile devices, which are small handheld devices to collect the data sent by the sensors; gateway, which is a trusted server that is used to register sensors, mobile devices and medical experts, and generates different keys for secure communication; and medical experts refers to medical professionals, such as doctors or nurses who analyze and take action with the collected information. The proposed protocol is executed in two phases—registration and authentication—as shown in Figures 10 and 11 illustrates the OFMC and CL-AtSe back-end results of the protocol.

1. BAN logic-based formal security analysis.

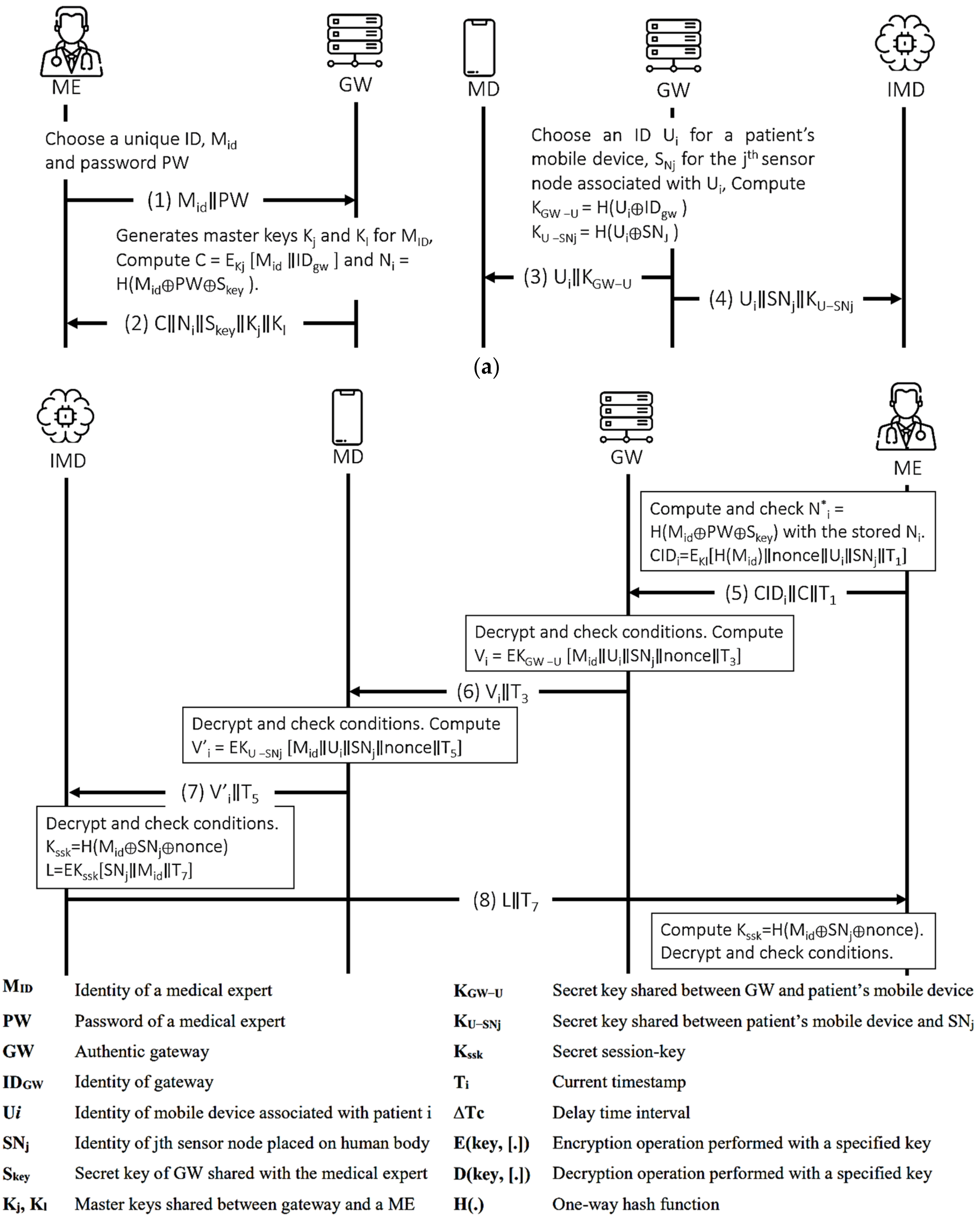
- **Idealization**

(I1) $\mathrm{ME} \rightarrow \mathrm{GW} : \langle\, \mathrm{M_{id}}, \mathrm{nonce}, \ \mathrm{U_i}, \mathrm{SN_j}, \mathrm{t_1} \rangle_{\mathrm{GW} \overset{\mathrm{K_l}}{\leftrightarrow} \mathrm{ME}}, \langle \mathrm{M_{id}}, \ \mathrm{ID_{gw}} \rangle_{\mathrm{GW} \overset{\mathrm{K_j}}{\leftrightarrow} \mathrm{ME}}$

(I2) $\mathrm{GW} \rightarrow \mathrm{MD} : \langle\, \mathrm{M_{id}}, \ \mathrm{U_i}, \mathrm{SN_j}, \mathrm{nonce}, \mathrm{t_3} \rangle_{\mathrm{GW} \overset{\mathrm{K_{GW-U}}}{\leftrightarrow} \mathrm{MD}}$

(I3) $\mathrm{MD} \rightarrow \mathrm{IMD} : \langle\, \mathrm{M_{id}}, \ \mathrm{U_i}, \mathrm{SN_j}, \mathrm{nonce}, \mathrm{t_5} \rangle_{\mathrm{MD} \overset{\mathrm{K_{U-SN_j}}}{\leftrightarrow} \mathrm{IMD}}$

(I4) $\mathrm{IMD} \rightarrow \mathrm{ME} : \langle\, \mathrm{SN_j}, \mathrm{M_{id}}, \ \mathrm{IMD} \overset{\mathrm{K_{ssk}}}{\leftrightarrow} \mathrm{ME}, \mathrm{t_7} \rangle_{\mathrm{IMD} \overset{\mathrm{K_{ssk}}}{\leftrightarrow} \mathrm{ME}}$


ME
GW
MD
GW
IMD
Choose a unique ID, M_id and password PW
(1) M_id‖PW
Generates master keys K_j and K_l for M_ID, Compute C = E_Kj [M_id ‖ID_gw] and N_i = H(M_id⊕PW⊕S_key).
(2) C‖N_i‖S_key‖K_j‖K_l
Choose an ID U_i for a patient's mobile device, S_Nj for the jth sensor node associated with U_i, Compute
K_GW-U = H(U_i⊕ID_gw)
K_U-SNj = H(U_i⊕SN_j)
(3) U_i‖K_GW-U
(4) U_i‖SN_j‖K_U-SNj
IMD
MD
GW
ME
Compute and check N*_i = H(M_id⊕PW⊕S_key) with the stored N_i.
CID_i=E_Kl[H(M_id)‖nonce‖U_i‖SN_j‖T_1]
(5) CID_i‖C‖T_1
Decrypt and check conditions. Compute V_i = EK_GW-U [M_id‖U_i‖SN_j‖nonce‖T_3]
(6) V_i‖T_3
Decrypt and check conditions. Compute V'_i = EK_U-SNj [M_id‖U_i‖SN_j‖nonce‖T_5]
(7) V'_i‖T_5
Decrypt and check conditions.
K_ssk=H(M_id⊕SN_j⊕nonce)
L=EK_ssk[SN_j‖M_id‖T_7]
(8) L‖T_7
Compute K_ssk=H(M_id⊕SN_j⊕nonce).
Decrypt and check conditions.

(**a**)

$\mathbf{M_{ID}}$	Identity of a medical expert	$\mathbf{K_{GW-U}}$	Secret key shared between GW and patient's mobile device
PW	Password of a medical expert	$\mathbf{K_{U-SNj}}$	Secret key shared between patient's mobile device and $\mathrm{SN_j}$
GW	Authentic gateway	$\mathbf{K_{ssk}}$	Secret session-key
$\mathbf{ID_{GW}}$	Identity of gateway	$\mathbf{T_i}$	Current timestamp
Ui	Identity of mobile device associated with patient i	**ΔTc**	Delay time interval
$\mathbf{SN_j}$	Identity of jth sensor node placed on human body	**E(key, [.])**	Encryption operation performed with a specified key
$\mathbf{S_{key}}$	Secret key of GW shared with the medical expert	**D(key, [.])**	Decryption operation performed with a specified key
$\mathbf{K_j, K_l}$	Master keys shared between gateway and a ME	**H(.)**	One-way hash function

(**b**)

Figure 10. Parvez et al.'s protocol. (**a**) Registration procedure. (**b**) Authentication Procedure.

- **Assumption**

(A1) GW believes GW $\overset{K_1}{\leftrightarrow}$ ME

(A2) GW believes $\mathrm{fresh}(t_1)$

(A3) GW believes ME Controls nonce

(A4) MD believes GW $\overset{K_{GW-U}}{\leftrightarrow}$ MD

(A5) MD believes $\mathrm{fresh}(t_3)$

(A6) MD believes GW Controls SN_j

(A7) MD believes GW Controls M_{id}

(A8) IMD believes MD $\overset{K_{U-SN_j}}{\leftrightarrow}$ IMD

(A9) IMD believes $\mathrm{fresh}(t_5)$

(A10) ME believes SN_j

(A11) ME believes nonce

(A12) ME believes M_{id}

(A13) ME believes $\mathrm{fresh}(t_7)$

(A14) ME believes IMD Controls K_{ssk}

- **Goals**

(G1) GW believes nonce

(G2) MD believes SN_j

(G3) MD believes M_{id}

(G4) ME believes IMD believes IMD $\overset{K_{ssk}}{\leftrightarrow}$ ME

(G5) IMD believes ME believes IMD $\overset{K_{ssk}}{\leftrightarrow}$ ME

(G6) IMD believes IMD $\overset{K_{ssk}}{\leftrightarrow}$ ME

- **Derivations**

(D1) GW sees $\langle M'_{id}, \mathrm{nonce},\ U_i, SN_j, t_1\rangle_{GW \overset{K_1}{\leftrightarrow} ME}$ By (I1), DR

(D2) GW believes ME said $[M'_{id}, \mathrm{nonce},\ U_i, SN_j, t_1]$ By (D1), (A1), MM

(D3) GW believes ME believes $[M'_{id}, \mathrm{nonce},\ U_i, SN_j, t_1]$ By (D2), (A2), NV, FR

(D4) GW believes ME believes nonce By (D3), BC

(D5) GW believes nonce By (D4), (A3), JR

(D6) MD sees $\langle M_{id},\ U_i, SN_j, \mathrm{nonce}, t_3\rangle_{GW \overset{K_{GW-U}}{\leftrightarrow} MD}$ (I2)

(D7) MD believes GW said $[M_{id},\ U_i, SN_j, \mathrm{nonce}, t_3]$ By (D6), (A4), MM

(D8) MD believes GW believes $[M_{id},\ U_i, SN_j, \mathrm{nonce}, t_3]$ By (D7), (A5), NV, FR

(D9) MD believes GW believes SN_j By (D8), BC

(D10) MD believes SN_j By (D9), (A6), JR

(D11) MD believes GW believes M_{id} By (D8), BC

(D12) MD believes M_{id} By (D11), (A7), JR

(D13) IMD sees $\langle M_{id},\ U_i, SN_j, \mathrm{nonce}, t_5\rangle_{MD \overset{K_{U-SN_j}}{\leftrightarrow} IMD}$ (I3).

(D14) IMD believes MD said $[M_{id},\ U_i, SN_j, \mathrm{nonce}, t_5]$ By (D13), (A8), MM

(D15) IMD believes MD belives $[M_{id},\ U_i, SN_j, \mathrm{nonce}, t_5]$ By (D14), (A9), NV, FR

(D16) IMD believes MD believes M_{id} By (D15), BC

(D17) IMD believes MD believes nonce By (D15), BC

(D18) ME sees $\langle SN_j, M_{id},\ IMD \overset{K_{ssk}}{\leftrightarrow} ME, t_7\rangle_{IMD \overset{K_{ssk}}{\leftrightarrow} ME}$ By (I4)

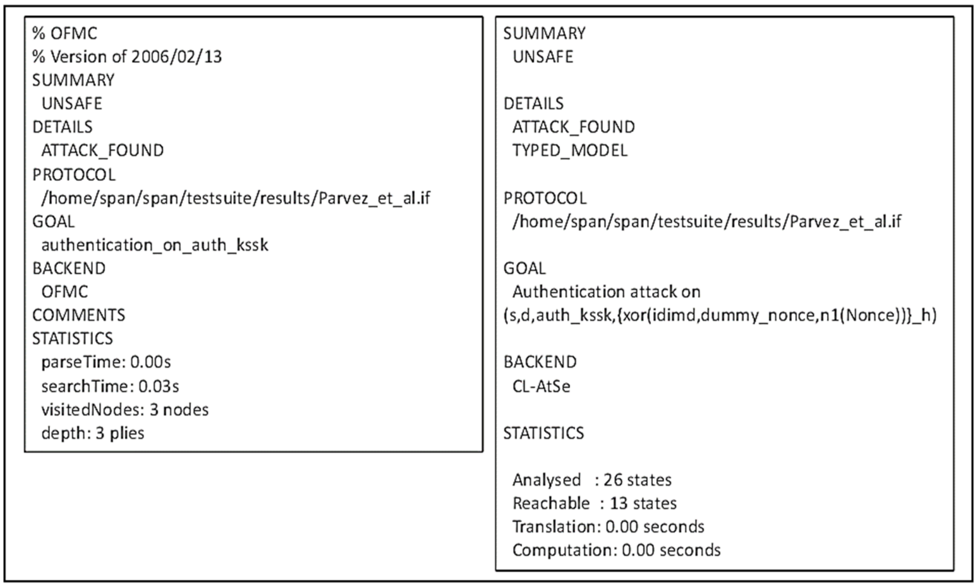
(D19) ME believes IMD $\overset{K_{ssk}}{\leftrightarrow}$ ME By (A10), (A11), (A12), BC

(D20) ME believes IMD said $\left[SN_j, M_{id},\ IMD \overset{K_{ssk}}{\leftrightarrow} ME, t_7\right]$ By (D18), (D19), MM

(D21) ME believes IMD belives $\left[SN_j, M_{id},\ IMD \overset{K_{ssk}}{\leftrightarrow} ME, t_7\right]$ By (D20), (A13), NV, FR

(D22) ME believes IMD believes IMD $\overset{K_{ssk}}{\leftrightarrow}$ ME By (D21), BC

2. AVISPA-based formal security analysis result.



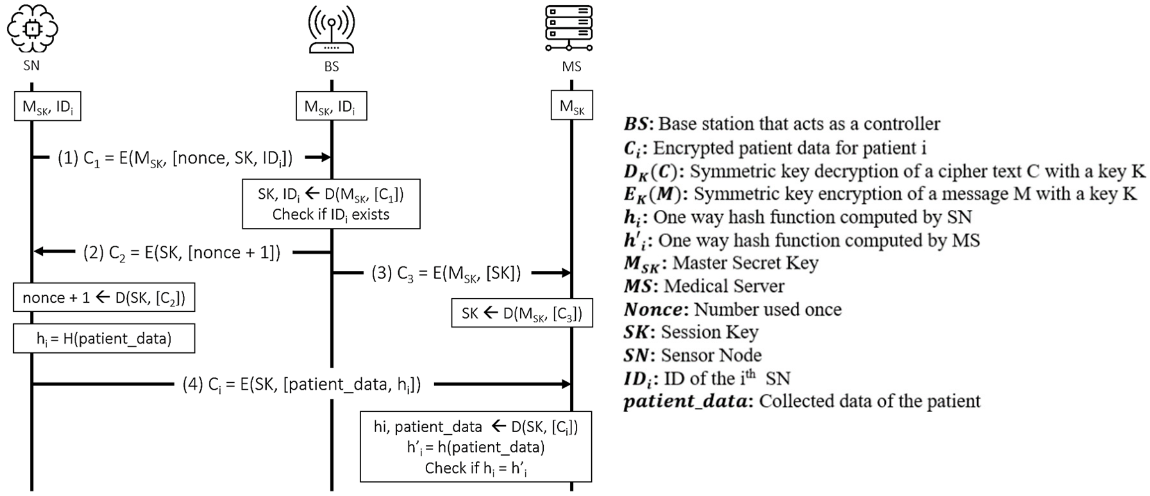
```
% OFMC
% Version of 2006/02/13
SUMMARY
 UNSAFE
DETAILS
 ATTACK_FOUND
PROTOCOL
 /home/span/span/testsuite/results/Parvez_et_al.if
GOAL
 authentication_on_auth_kssk
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.03s
 visitedNodes: 3 nodes
 depth: 3 plies
```

```
SUMMARY
 UNSAFE

DETAILS
 ATTACK_FOUND
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/Parvez_et_al.if

GOAL
 Authentication attack on
(s,d,auth_kssk,{xor(idimd,dummy_nonce,n1(Nonce))}_h)

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 26 states
 Reachable  : 13 states
 Translation: 0.00 seconds
 Computation: 0.00 seconds
```

Figure 11. AVISPA result of Parvez et al.'s protocol.

4.3.5. Iqbal et al.'s Protocol

The proposed protocol [27] works between the sensor nodes (SN), controller (BS), and a medical server (MS). The SNs are (implanted) medical devices that sense vital physiological information. In this protocol, a BS is only used to assist the authentication process so that the SN directly communicates with the MS after successful authentication is achieved. The protocol is executed in three stages: deployment, authentication, and data communication, as shown in Figures 12 and 13 presents the OFMC and CL-AtSe back-end results of the protocol.


SN
BS
MS
M_{SK}, ID_i
M_{SK}, ID_i
M_{SK}
(1) C_1 = E(M_{SK}, [nonce, SK, ID_i])
SK, ID_i ← D(M_{SK}, [C_1])
Check if ID_i exists
(2) C_2 = E(SK, [nonce + 1])
(3) C_3 = E(M_{SK}, [SK])
nonce + 1 ← D(SK, [C_2])
SK ← D(M_{SK}, [C_3])
h_i = H(patient_data)
(4) C_i = E(SK, [patient_data, h_i])
hi, patient_data ← D(SK, [C_i])
h'_i = h(patient_data)
Check if h_i = h'_i

BS: Base station that acts as a controller
C_i: Encrypted patient data for patient i
$D_K(C)$: Symmetric key decryption of a cipher text C with a key K
$E_K(M)$: Symmetric key encryption of a message M with a key K
h_i: One way hash function computed by SN
h'_i: One way hash function computed by MS
M_{SK}: Master Secret Key
MS: Medical Server
Nonce: Number used once
SK: Session Key
SN: Sensor Node
ID_i: ID of the ith SN
patient_data: Collected data of the patient

Figure 12. Iqbal et al.'s protocol.

1. BAN logic-based formal security analysis

- **Idealization**

(I1) $\mathrm{SN} \rightarrow \mathrm{BS}: \{\mathrm{Nonce}, \mathrm{SK}, \mathrm{ID_i}\}_{\mathrm{M_{sk}}}$

(I2) $\mathrm{BS} \rightarrow \mathrm{SN}: \{\mathrm{Nonce}\}_{\mathrm{SK}}$

(I3) $\mathrm{SN} \rightarrow \mathrm{MS}: \left\{\mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{MS}\right\}_{\mathrm{M_{sk}}}$

(I4) $\mathrm{SN} \rightarrow \mathrm{MS}: \{\mathrm{M}\}_{\mathrm{SK}}$

- **Assumption**

(A1) BS believes $\mathrm{SN} \overset{\mathrm{M_{sk}}}{\leftrightarrow} \mathrm{BS}$

(A2) BS believes fresh(Nonce)

(A3) BS believes SN Controls SK

(A4) SN believes SK

(A5) SN believes fresh(Nonce)

(A6) MS believes $\mathrm{MS} \overset{\mathrm{M_{sk}}}{\leftrightarrow} \mathrm{SN}$

- **Hypotheses**

(H1) MS believes fresh$\left(\mathrm{MS} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{BS}\right)$

(H2) MS believes SN Controls $\mathrm{MS} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{BS}$

- **Goals**

(G1) BS believes SN believes $\mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{BS}$

(G2) BS believes $\mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{BS}$

(G3) SN believes BS believes $\mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{BS}$

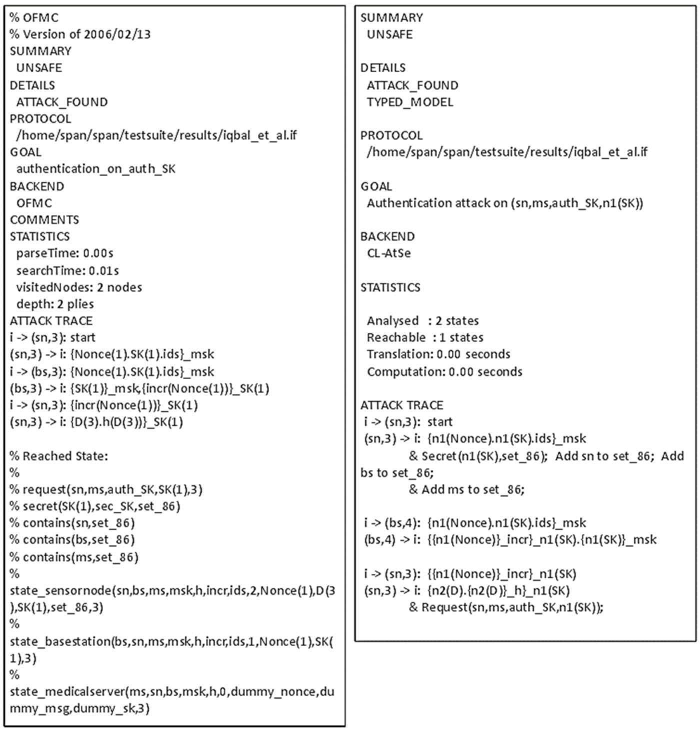
(G4) MS believes SN believes $\mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{MS}$

(G5) MS believes $\mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{MS}$

- **Derivations**

(D1)	BS sees $\langle \mathrm{Nonce}, \mathrm{SK}, \mathrm{ID_i} \rangle_{\mathrm{M_{SK}}}$	(I1)
(D2)	BS believes SN said $[\mathrm{Nonce}, \mathrm{SK}, \mathrm{ID_i}]$	By (D1), (A1), MM
(D3)	BS believes SN believes $[\mathrm{Nonce}, \mathrm{SK}, \mathrm{ID_i}]$	By (D2), (A2), NV, FR
(D4)	BS believes SN believes SK	By (D3), BC
(D5)	BS believes SK	By (D4), (A3), JR
(D6)	SN sees $\langle \mathrm{Nonce}, \mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{BS} \rangle_{\mathrm{SK}}$	(I2)
(D7)	SN believes BS said $\left[\mathrm{Nonce}, \mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{BS}\right]$	By (D6), (A4), MM
(D8)	SN believes BS believes $\mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{BS}$	By (D7), (A5), NV, FR, BC
(D9)	MS sees $\langle \mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{MS} \rangle_{\mathrm{M_{SK}}}$	(I3)
(D10)	MS believes SN said $\left[\mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{MS}\right]$	By (D9), (A6), MM
(D11)	MS believes SN believes $\mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{BS}$	By (D10), (H1), NV, FR
(D12)	MS believes $\mathrm{SN} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{BS}$	By (D10), (H2), JR

2. AVISPA-based formal security analysis result.



```
% OFMC
% Version of 2006/02/13
SUMMARY
 UNSAFE
DETAILS
 ATTACK_FOUND
PROTOCOL
 /home/span/span/testsuite/results/iqbal_et_al.if
GOAL
 authentication_on_auth_SK
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.01s
 visitedNodes: 2 nodes
 depth: 2 plies
ATTACK TRACE
i -> (sn,3): start
(sn,3) -> i: {Nonce(1).SK(1).ids}_msk
i -> (bs,3): {Nonce(1).SK(1).ids}_msk
(bs,3) -> i: {SK(1)}_msk,{incr(Nonce(1))}_SK(1)
i -> (sn,3): {incr(Nonce(1))}_SK(1)
(sn,3) -> i: {D(3).h(D(3))}_SK(1)

% Reached State:
%
% request(sn,ms,auth_SK,SK(1),3)
% secret(SK(1),sec_SK,set_86)
% contains(sn,set_86)
% contains(bs,set_86)
% contains(ms,set_86)
%
state_sensornode(sn,bs,ms,msk,h,incr,ids,2,Nonce(1),D(3
),SK(1),set_86,3)
%
state_basestation(bs,sn,ms,msk,h,incr,ids,1,Nonce(1),SK(
1),3)
%
state_medicalserver(ms,sn,bs,msk,h,0,dummy_nonce,du
mmy_msg,dummy_sk,3)
```

```
SUMMARY
 UNSAFE

DETAILS
 ATTACK_FOUND
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/iqbal_et_al.if

GOAL
 Authentication attack on (sn,ms,auth_SK,n1(SK))

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 2 states
 Reachable  : 1 states
 Translation: 0.00 seconds
 Computation: 0.00 seconds

ATTACK TRACE
 i -> (sn,3):  start
 (sn,3) -> i:  {n1(Nonce).n1(SK).ids}_msk
           & Secret(n1(SK),set_86);  Add sn to set_86;  Add
bs to set_86;
           & Add ms to set_86;

 i -> (bs,4):  {n1(Nonce).n1(SK).ids}_msk
 (bs,4) -> i:  {{n1(Nonce)}_incr}_n1(SK).{n1(SK)}_msk

 i -> (sn,3):  {{n1(Nonce)}_incr}_n1(SK)
 (sn,3) -> i:  {n2(D).{n2(D)}_h}_n1(SK)
           & Request(sn,ms,auth_SK,n1(SK));
```

Figure 13. AVISPA result of Iqbal et al.'s protocol.

4.3.6. He and Zeadally's Protocol

He and Zeadally's authentication protocol [28] comprises a programmer/controller, the AAL server, and a user. The controller is responsible for communicating with the IMDs and receiving collected physiological information. Once such information is collected, it can be accessed by a remote user after the AAL server authenticates the user. Furthermore, the controller may communicate with different devices, such as home robots for immediate nearby assistance, located in the patient's premises. The protocol is also executed in two stages: registration and authentication, as shown in Figures 14 and 15 illustrates the OFMC and CL-AtSe back-end results of the protocol.

1. BAN logic-based formal security analysis.

- **Idealization**

(I1) $\mathrm{U} \rightarrow \mathrm{A} : \left\{ \mathrm{ID_U}, \mathrm{ID_C}, \overset{\mathrm{P_U}}{\rightarrow} \mathrm{U}, \mathrm{TS_U}, \mathrm{A} \overset{\mathrm{TK_{A-U}}}{\leftrightarrow} \mathrm{U} \right\}_{\mathrm{A} \overset{\mathrm{TK_{A-U}}}{\leftrightarrow} \mathrm{U}} \langle \overset{\mathrm{P_U}}{\rightarrow} \mathrm{U}, \mathrm{TS_U}, \mathrm{A} \overset{\mathrm{K_{A-U}}}{\leftrightarrow} \mathrm{U} \rangle_{\mathrm{A} \overset{\mathrm{K_{A-U}}}{\leftrightarrow} \mathrm{U}}$

(I2) $\mathrm{A} \rightarrow \mathrm{C} : \left\{ \mathrm{ID_U}, \mathrm{ID_C}, \overset{\mathrm{P_U}}{\rightarrow} \mathrm{U}, \mathrm{TS_{A_1}}, \mathrm{A} \overset{\mathrm{K_{A-C}}}{\leftrightarrow} \mathrm{C} \right\}_{\mathrm{A} \overset{\mathrm{K_{A-C}}}{\leftrightarrow} \mathrm{C}}$

(I3) $\mathrm{C} \rightarrow \mathrm{A} : \left\{ \mathrm{ID_U}, \mathrm{ID_C}, \overset{\mathrm{P_C}}{\rightarrow} \mathrm{C}, \mathrm{TS_C}, \mathrm{A} \overset{\mathrm{K_{A-C}}}{\leftrightarrow} \mathrm{C} \right\}_{\mathrm{A} \overset{\mathrm{K_{A-C}}}{\leftrightarrow} \mathrm{C}}$

(I4) $\mathrm{A} \rightarrow \mathrm{U} : \left\{ \mathrm{ID_U}, \mathrm{ID_C}, \overset{\mathrm{P_C}}{\rightarrow} \mathrm{C}, \mathrm{TS_{A_2}}, \mathrm{A} \overset{\mathrm{TK_{A-U}}}{\leftrightarrow} \mathrm{U} \right\}_{\mathrm{A} \overset{\mathrm{TK_{A-U}}}{\leftrightarrow} \mathrm{U}}$

- **Assumption**

(A1) A believes $\mathrm{A} \overset{\mathrm{K_{A-U}}}{\leftrightarrow} \mathrm{U}$

(A2) A believes $\#(\mathrm{TS_U})$

(A3) A believes $\overset{\mathrm{Q_A}}{\rightarrow} \mathrm{A}$

(A4) C believes $\mathrm{A} \overset{\mathrm{K_{A-C}}}{\leftrightarrow} \mathrm{C}$

(A5) C believes $\#(\mathrm{TS_{A_1}})$

(A6) C believes $\overset{Q_C}{\rightarrow}$ C

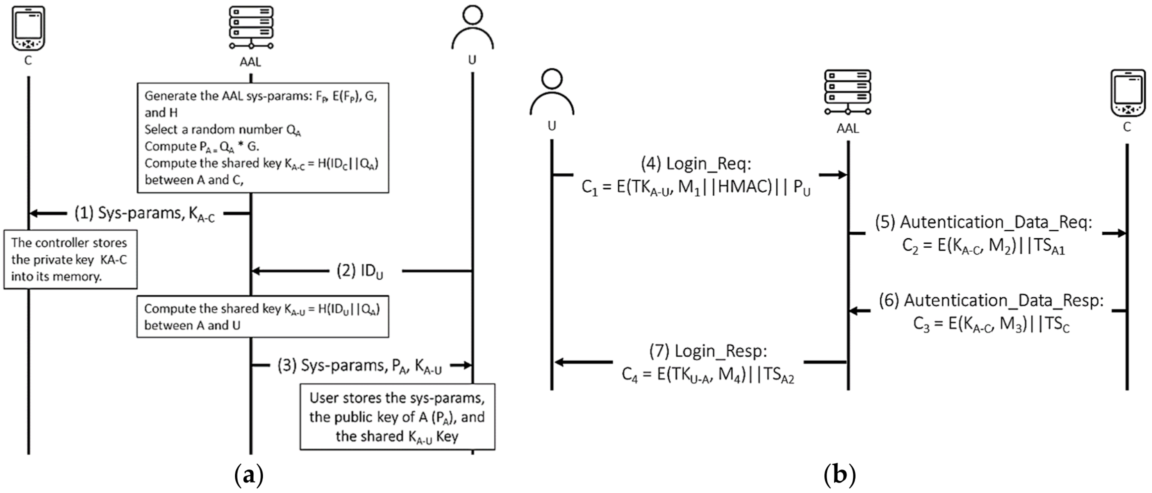
(A7) A believesA $\overset{K_{A-C}}{\leftrightarrow}$ C

(A8) A believes $\#(TS_C)$

(A9) U believes A $\overset{TK_{A-U}}{\leftrightarrow}$ U

(A10) U believes $\#(TS_{A_2})$

(A11) U believes $\overset{Q_U}{\rightarrow}$ U


C
AAL
U
Generate the AAL sys-params: F_p, E(F_p), G, and H
Select a random number Q_A
Compute P_A = Q_A * G.
Compute the shared key K_{A-C} = H(ID_C||Q_A) between A and C,
(1) Sys-params, K_{A-C}
The controller stores the private key KA-C into its memory.
(2) ID_U
Compute the shared key K_{A-U} = H(ID_U||Q_A) between A and U
(3) Sys-params, P_A, K_{A-U}
User stores the sys-params, the public key of A (P_A), and the shared K_{A-U} Key
(a)
U
AAL
C
(4) Login_Req:
C₁ = E(TK_{A-U}, M₁||HMAC)|| P_U
(5) Autentication_Data_Req:
C₂ = E(K_{A-C}, M₂)||TS_{A1}
(6) Autentication_Data_Resp:
C₃ = E(K_{A-C}, M₃)||TS_C
(7) Login_Resp:
C₄ = E(TK_{U-A}, M₄)||TS_{A2}
(b)

AAL, C, U	Ambient Assisted Living Server, Controller, and User.	K_{X-Y}	Shared keys between entities X and Y.
D(k,c)	A symmetric decryption of a cipher c using a key k	Q_X	Private keys of entity X.
E(Fp)	An elliptic curve group over the field Fp	P_X	Public keys of entity X.
E(k,m)	A symmetric encryption of a message m using a key k	SK_{X-Y}	A session key between entities X and Y
G	A generator of a subgroup of E(Fp) with the order of n	TK_{X-Y}	A temporary key between entities X and Y
H(m)	A hash of a message m	TS_X	A timestamp generated by entity X.
HM(k,m)	A keyed hash function of a message m using a key k	TS_{CLR},T_{SENC}	A timestamp received in clear and encrypted
HM_{RCVD},HM_{CPTD}	The received and computed HMAC values, resp.	TS_{curt}	The current timestamp
ID_X	Unique identifier of entity X.	σ	A deviation between TS_{curt} and the received timestamp

Figure 14. He and Zeadally's protocol. (**a**) Registration phase. (**b**) Authentication phase.

- **Hypotheses**

(H1) A believes U Controls $\overset{P_U}{\rightarrow}$ U

- **Goals**

(G1) A believes A $\overset{TK_{A-U}}{\leftrightarrow}$ U

(G2) A believes U believes A $\overset{K_{A-U}}{\leftrightarrow}$ U

(G3) A believes U believes ID_U

(G4) A believes U believes A $\overset{TK_{A-U}}{\leftrightarrow}$ U

(G5) C believes A believes ID_U

(G6) C believes C $\overset{SK_{C-U}}{\leftrightarrow}$ U

(G7) C believes A believes C $\overset{K_{A-C}}{\leftrightarrow}$ A

(G8) A believes C believes ID_C

(G9) A believes C believes C $\overset{K_{A-C}}{\leftrightarrow}$ A

(G10) U believes A believes ID_C

(G11) U believes C $\overset{SK_{C-U}}{\leftrightarrow}$ U

(G12) U believes A believes U $\overset{TK_{A-U}}{\leftrightarrow}$ A

- **Derivations**

(D1) A sees $\langle ID_U, ID_C, TS_U, A \overset{TK_{A-U}}{\leftrightarrow} U\rangle_{A \overset{TK_{A-U}}{\leftrightarrow} U}, \langle \overset{P_U}{\rightarrow} U, TS_U, A \overset{K_{A-U}}{\leftrightarrow} U\rangle_{A \overset{K_{A-U}}{\leftrightarrow} U}$ (I1)

(D2) A believes U said $\left[\overset{P_U}{\rightarrow} U, TS_U, A \overset{K_{A-U}}{\leftrightarrow} U\right]$ By $(D1), (A1), MM$

(D3) A believes U believes $\left[\overset{P_U}{\rightarrow} U, TS_U, A \overset{K_{A-U}}{\leftrightarrow} U\right]$ By $(D2), (A2), FR, NV$

(D4) A believes U believes $\overset{P_U}{\rightarrow} U$ By $(D3), BC$

(D5) A believes $\overset{P_U}{\rightarrow} U$ By $(D4), (H1),$ JR

(D6) A believes $A \overset{TK_{A-U}}{\leftrightarrow} U$ By $(D5), (A3), BC$

(D7) A believes U believes $A \overset{K_{A-U}}{\leftrightarrow} U$ By $(D3), BC$

(D8) A believes U said $\left[ID_U, ID_C, TS_U, A \overset{TK_{A-U}}{\leftrightarrow} U\right]$ By $(D1), (D6), MM$

(D9) A believes U believes $\left[ID_U, ID_C, TS_U, A \overset{TK_{A-U}}{\leftrightarrow} U\right]$ By $(D8), (A2), FR, NV$

(D10) A believes U believes ID_U By $(D9), BC$

(D11) A believes U believes $U \overset{TK_{A-U}}{\leftrightarrow} A$ By $(D9), BC$

(D12) C sees $\left\{ID_U, ID_C, \overset{P_U}{\rightarrow} U, TS_A, A \overset{K_{A-C}}{\leftrightarrow} C\right\}_{A \overset{K_{A-C}}{\leftrightarrow} C}$ (I2)

(D13) C believes A said $\left[ID_U, ID_C, \overset{P_U}{\rightarrow} U, TS_A, A \overset{K_{A-C}}{\leftrightarrow} C\right]$ By $(D12), (A4), MM$

(D14) C believes A believes $\left[ID_U, ID_C, \overset{P_U}{\rightarrow} U, TS_A, A \overset{K_{A-C}}{\leftrightarrow} C\right]$ By $(D13), (A5), FR, NV$

(D15) C believes A believes ID_U By $(D14), BC$

(D16) C believes $C \overset{SK_{C-U}}{\leftrightarrow} U$ By (D13), BC, (A6), DH

(D17) C believes A believes $C \overset{K_{A-C}}{\leftrightarrow} A$ By $(D14), BC$

(D18) A sees $\left\{ID_U, ID_C, \overset{P_C}{\rightarrow} C, TS_C, A \overset{K_{A-C}}{\leftrightarrow} C\right\}_{A \overset{K_{A-C}}{\leftrightarrow} C}$ (I3)

(D19) A believes C said $\left[ID_U, ID_C, \overset{P_C}{\rightarrow} C, TS_C, A \overset{K_{A-C}}{\leftrightarrow} C\right]$ By $(D18), (A7), MM$

(D20) A believes C believes $\left[ID_U, ID_C, \overset{P_C}{\rightarrow} C, TS_C, A \overset{K_{A-C}}{\leftrightarrow} C\right]$ By $(D19), (A8), FR, NV$

(D21) A believes C believes ID_C By $(D20), BC$

(D22) A believes C believes $C \overset{K_{A-C}}{\leftrightarrow} A$ By $(D20), BC$

(D23) U sees $\left\{ID_U, ID_C, \overset{P_C}{\rightarrow} C, TS_{A_2}, A \overset{TK_{A-U}}{\leftrightarrow} U\right\}_{A \overset{TK_{A-U}}{\leftrightarrow} U}$ (I4)

(D24) U believes A said $\left[ID_U, ID_C, \overset{P_C}{\rightarrow} C, TS_{A_2}, A \overset{TK_{A-U}}{\leftrightarrow} U\right]$ By $(D23), (A9), MM$

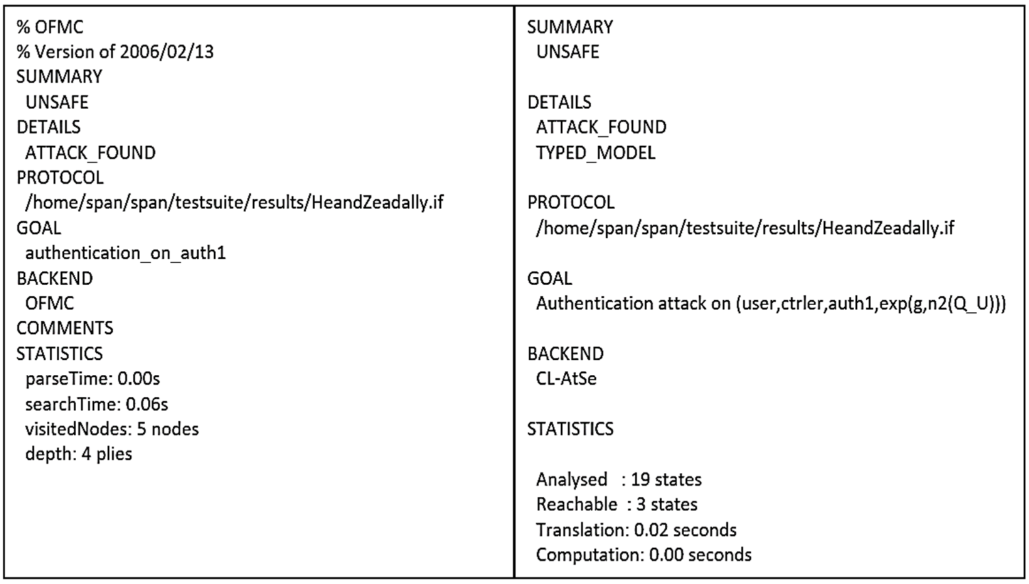
(D25) U believes A believes $\left[ID_U, ID_C, \overset{P_C}{\rightarrow} C, TS_{A_2}, A \overset{TK_{A-U}}{\leftrightarrow} U\right]$ By $(D24), (A10), FR, NV$

(D26) U believes A believes ID_C By $(D25), BC$

(D27) U believes $C \overset{SK_{C-U}}{\leftrightarrow} U$ By $(D24), BC, (A11), DH$

(D28) U believes A believes $A \overset{TK_{A-U}}{\leftrightarrow} U$ By $(D25), BC$

2. AVISPA-based formal security analysis result.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  UNSAFE
DETAILS
  ATTACK_FOUND
PROTOCOL
  /home/span/span/testsuite/results/HeandZeadally.if
GOAL
  authentication_on_auth1
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.06s
  visitedNodes: 5 nodes
  depth: 4 plies
```

```
SUMMARY
  UNSAFE

DETAILS
  ATTACK_FOUND
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/HeandZeadally.if

GOAL
  Authentication attack on (user,ctrler,auth1,exp(g,n2(Q_U)))

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 19 states
  Reachable  : 3 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

Figure 15. AVISPA result of He and Zeadally's protocol.

4.3.7. Ellouze et al.'s Protocol

This protocol [29] is a mutual authentication protocol for cardiac IMDs that integrates a powerless device called wireless identification and sensing platform (WISP) with IMDs to conserve the battery lifetime of IMDs by drawing energy from an RFID reader. The authentication scheme operates in regular and emergency modes between the WISP and the RFID reader. The final goal is to create mutual authentication between the programmer and the IMD. Figure 16 shows both modes of the protocol. The authors of this protocol performed AVISPA-based security verification and claimed that the protocol is secure. Hence, only BAN logic-based analysis is performed here.

1. BAN logic-based formal security analysis.
2. Regular mode.

- **Idealization**

(I1) $R \rightarrow W : \langle N_R,\ ID_R, W \overset{K}{\leftrightarrow} R\rangle_{W\overset{K}{\leftrightarrow}R}$

(I2) $W \rightarrow R : \langle N_R,\ N_W, ID_W, W \overset{K}{\leftrightarrow} R\rangle_{W\overset{K}{\leftrightarrow}R}$

(I3) $R \rightarrow WISP : \langle N_W, Seq_1, W \overset{K'}{\leftrightarrow} R\rangle_{W\overset{K'}{\leftrightarrow}R}$

- **Assumption**

(A1) W believes $W \overset{K}{\leftrightarrow} R$

(A2) W believes $\#(N_W)$

(A3) R believes $W \overset{K}{\leftrightarrow} R$

(A4) R believes $\#(N_R)$

- **Hypotheses**

(H1) W believes $\#(N_R)$

(H2) R believes $\#(N_W)$

- **Goals**

(G1) W believes R believes $\mathrm{ID_R}$

(G2) W believes R believes $\mathrm{W} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R}$

(G3) W believesW $\overset{\mathrm{K'}}{\leftrightarrow}$ R

(G4) R believes W believes $\mathrm{ID_W}$

(G5) R believes W believes $\mathrm{W} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R}$

(G6) R believes $\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$

(G7) W believes R believes $\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$

- **Derivations**

(D1) W sees $\langle \mathrm{N_R},\ \mathrm{ID_R}, \mathrm{W} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R} \rangle_{\mathrm{W} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R}}$ (I1)

(D2) W believes R said $\left[\mathrm{N_R},\ \mathrm{ID_R}, \mathrm{W} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R}\right]$ By (D1), (A1), MM

(D3) W believes R believes $\mathrm{ID_R}$ By (D2), (H1), FR, NV

(D4) W believes R believes $\mathrm{W} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R}$ By (D2), (H1), FR, NV

(D5) W believes $\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$ By (A1), (A2), BC

(D6) R sees $\langle \mathrm{N_R},\ \mathrm{N_W}, \mathrm{ID_W}, \mathrm{W} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R} \rangle_{\mathrm{W} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R}}$ (I2)

(D7) R believes W said $\left[\mathrm{N_R},\ \mathrm{N_W}, \mathrm{ID_W}, \mathrm{W} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R}\right]$ By (D6), (A3), MM

(D8) R believes W believes $\mathrm{ID_W}$ By (D7), (A4), FR, NV

(D9) R believes W believes $\mathrm{W} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R}$ By (D7), (A4), FR, NV

(D10) R believes $\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$ By (A3), (H2), BC

(D11) W sees $\langle \mathrm{N_W}, \mathrm{Seq_1}, \mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R} \rangle_{\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}}$ By (D8), BC

(D12) W believes R said $\left[\mathrm{N_W}, \mathrm{Seq_1}, \mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}\right]$ By (D11), (D5), MM

(D13) W believes R believes $\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$ By (D12), (A2), FR, NV

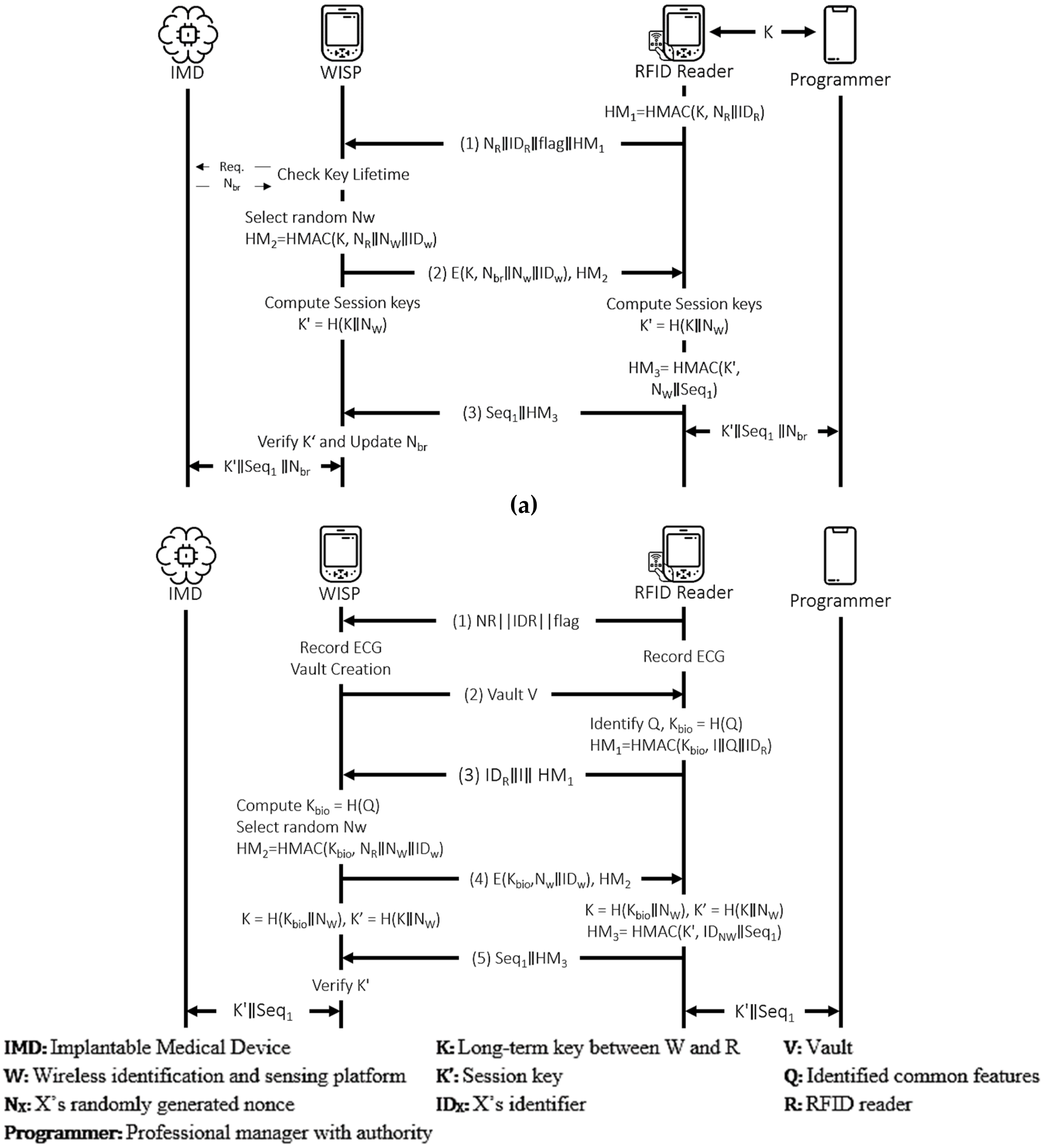
3. Emergency Mode

- **Idealization**

(I1) $\mathrm{R} \to \mathrm{W} : \langle\ \mathrm{Q}, \mathrm{N_R}, \mathrm{ID_R}, \mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R} \rangle_{\mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R}}$

(I2) $\mathrm{W} \to \mathrm{R} : \langle\ \mathrm{N_R},\ \mathrm{N_W}, \mathrm{ID_W}, \mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R} \rangle_{\mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R}}$

(I3) $\mathrm{R} \to \mathrm{W} : \langle\ \mathrm{N_W}, \mathrm{Seq_1}, \mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R} \rangle_{\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}}$


IMD
WISP
RFID Reader
Programmer
K
HM$_1$=HMAC(K, N$_R$||ID$_R$)
(1) N$_R$||ID$_R$||flag||HM$_1$
Req.
N$_{br}$
Check Key Lifetime
Select random Nw
HM$_2$=HMAC(K, N$_R$||N$_W$||ID$_w$)
(2) E(K, N$_{br}$||N$_w$||ID$_w$), HM$_2$
Compute Session keys
K' = H(K||N$_W$)
Compute Session keys
K' = H(K||N$_W$)
HM$_3$= HMAC(K', N$_W$||Seq$_1$)
(3) Seq$_1$||HM$_3$
K'||Seq$_1$ ||N$_{br}$
Verify K' and Update N$_{br}$
K'||Seq$_1$ ||N$_{br}$
(a)
IMD
WISP
RFID Reader
Programmer
(1) NR||IDR||flag
Record ECG
Vault Creation
Record ECG
(2) Vault V
Identify Q, K$_{bio}$ = H(Q)
HM$_1$=HMAC(K$_{bio}$, I||Q||ID$_R$)
(3) ID$_R$||I|| HM$_1$
Compute K$_{bio}$ = H(Q)
Select random Nw
HM$_2$=HMAC(K$_{bio}$, N$_R$||N$_W$||ID$_w$)
(4) E(K$_{bio}$,N$_w$||ID$_w$), HM$_2$
K = H(K$_{bio}$||N$_W$), K' = H(K||N$_W$)
K = H(K$_{bio}$||N$_W$), K' = H(K||N$_W$)
HM$_3$= HMAC(K', ID$_{NW}$||Seq$_1$)
(5) Seq$_1$||HM$_3$
Verify K'
K'||Seq$_1$
K'||Seq$_1$
IMD: Implantable Medical Device
W: Wireless identification and sensing platform
N$_X$: X's randomly generated nonce
Programmer: Professional manager with authority
K: Long-term key between W and R
K': Session key
ID$_X$: X's identifier
V: Vault
Q: Identified common features
R: RFID reader

(b)

Figure 16. Ellouze et al.'s protocol. (**a**) Regular Mode. (**b**) Emergency Mode.

- **Assumption**

(A1) W believes $W \overset{K_{bio}}{\leftrightarrow} R$

(A2) W believes $\#(N_W)$

(A3) R believes $W \overset{K_{bio}}{\leftrightarrow} R$

(A4) R believes $\#(N_R)$

- **Hypotheses**

(H1) W believes $\#(N_R)$

(H2) R believes $\#(N_W)$

- **Goals**

(G1) W believes R believes $\mathrm{ID_R}$

(G2) W believes R believes $\mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R}$

(G3) W believesW $\overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$

(G4) R believes W believes $\mathrm{ID_W}$

(G5) R believes W believes $\mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R}$

(G6) R believes $\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$

(G7) W believes R believes $\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$

- **Derivations**

(D1) W sees $\langle \mathrm{Q}, \mathrm{N_R}, \mathrm{ID_R}, \mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R} \rangle_{\mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R}}$ (I1)

(D2) W believes R said. $\left[\mathrm{Q}, \mathrm{N_R}, \mathrm{ID_R}, \mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R}\right]$ By (D1), (A1), MM

(D3) W believes R believes $\mathrm{ID_R}$. By (D2), (H1), FR, NV

(D4) W believes R believes $\mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R}$ By (D2), (H1), FR, NV

(D5) W believes $\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$ By (A1), (A2), BC

(D6) R sees $\langle \mathrm{N_R},\ \mathrm{N_W}, \mathrm{ID_W}, \mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R} \rangle_{\mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R}}$ (I2)

(D7) R believes W said $\left[\mathrm{N_R}, \mathrm{NW}, \mathrm{ID_W}, \mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R}\right]$ By (D6), (A3), MM

(D8) R believes W believes $\mathrm{ID_W}$ BY (D7), (A4), FR, NV

(D9) R believes W believes $\mathrm{W} \overset{\mathrm{K_{bio}}}{\leftrightarrow} \mathrm{R}$ By (D7), (A4), FR, NV

(D10) R believes $\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$ By (A3), (H2), BC

(D11) W sees $\langle \mathrm{N_W}, \mathrm{Seq_1}, \mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R} \rangle_{\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}}$ (I3)

(D12) W believes R said $\left[\mathrm{N_W}, \mathrm{Seq_1}, \mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}\right]$ By (D11), (D5), MM

(D13) W believes R believes $\mathrm{W} \overset{\mathrm{K'}}{\leftrightarrow} \mathrm{R}$ By (D12), (A2), FR, NV

5. Discussion

The authentication protocols described and analyzed in the previous section have shown the importance of formally analyzing security protocols for usage reliability.

Khan et al.'s protocol is safe as per the output of both BAN logic and AVISPA in satisfying the goals. The hub node can be sure about the validity of the temporary identification (G1 and G2) and the auxiliary authentication parameter (G3 and G4). Furthermore, the sensor node trusts the newly generated session key (G6 and G7).

The proxy-assisted access control scheme proposed by Wu et al. is the second safe protocol for the authentication goals set. The main objective of the protocol is to device a shared symmetric key $\mathrm{K_t}$ that the programmer and the IMD will use to secure the information exchanged. Accordingly, (G2) to (G5), (G8), and (G9) show that this objective is satisfied. Furthermore, other less essential facts that involve the IDs of the participating agents are authentic.

Chi et al.'s access control scheme with forensic capability is designed to safeguard IMDs from unauthorized access. The protocol is secure as per the results of BAN logic and AVISPA on authenticity and secrecy properties. The goals in the BAN logic analysis investigated the authentication between the IMD, smartphone, and the programmer through the keys $\mathrm{K_d}$, $\mathrm{K_r}$, $\mathrm{K_p}$, and $\mathrm{K_i}$.

The user authentication scheme in WBAN, as proposed by Parvez et al., is found to be unsafe, by both AVISPA and BAN logic, on the authentication of the shared key $\mathrm{K_{ssk}}$. The shared key that will be used by the medical expert and the IMD is computed from the nonce, $\mathrm{SN_j}$, and $\mathrm{M_{id}}$. In terms of BAN logic, this means the IMD has to believe these values to believe the computed session key. Consequently, the derivations (D11) to (D13) alone cannot enable the IMD to derive its belief to the shared key- which calls for two new hypotheses about the control of the nonce and $\mathrm{M_{id}}$ by the mobile device that acts as a proxy between the IMD and the external devices. Such hypotheses may not be accurate given that ME and GW generated these values, respectively. However, since the message passed from the MD to the IMD is fresh and protected by the key that both parties trust, we may still be convinced that the IMD can derive the session key. The final goal, (G5), can be derived after a new message arrives from the ME to IMD using the session key K_{ssk}.

Iqbal et al.'s authentication and key agreement scheme are proposed for node authentication in the body sensor environment. The protocol has some serious issues, typically concerning reply attacks. Specifically, the security goals (G4) and (G5) related to the mutual authentication between the medical server and the IMD cannot be satisfied as-is. The medical server cannot be sure about the freshness of the shared session key forwarded by the base station, making the message vulnerable to replay attack. Consequently, the hypotheses (H1) and (H2) need to be added to maintain authentication. More importantly, it is possible to improve the protocol by including a nonce along with the session key SK when BS sends the message to the MS.

He and Zeadally's scheme aims to improve the security of ambient assisted living. It mainly focuses on the mutual authentication between the Controller and the User via the AAL server. With this regard, the goals (G3), (G5), (G8), and (G10) refer to the secure information exchange, while (G6) and (G11) specify the secure session key exchange between the User and the Controller. The remaining goals are related to the exchange of symmetric keys among all the participants of the authentication scheme. The result of both the BAN logic and AVISPA illustrate that it is not possible to conclusively state the protocol as safe to use. That is, the derivations show that for the AAL server to believe that $TK_{A\text{-}U}$ is a key that is only known by itself and the User (G1), it must first believe that PU is the public key of the User that is encrypting the messages by the key $TK_{A\text{-}U}$ (G2). This, in turn, needs the AAL server to believe that this User has jurisdiction over the public key PU, meaning that the AAL server has to trust this User concerning PU (H1). Consequently, we cannot prove the goals (G1) and (G2) without the hypothesis we added.

Ellouze et al.'s scheme is a specific authentication protocol proposed for cardiac IMDs with powerless authentication mechanisms. The protocol operates in both emergency and regular modes to authenticate the programmer to the IMD and vice versa. The authors of this protocol have performed AVISPA based formal security analysis and reported that the protocol is safe. However, when the protocol is analyzed using BAN logic, a contrary result is found. The result from the analysis of the BAN logic in the emergency mode of the protocol shows the requirement of two additional hypotheses to satisfy the authentication between the WISP and the RFID Reader. Specifically, the WISP cannot conclusively believe the K_{Bio}. This key will be used to derive the session key K′ latter if the reader believes it without guaranteeing the freshness of NR. Furthermore, the security goal that conditions the guarantee for the WISP that the RFID Reader believes the session key K′ (G7) can only be satisfied if the freshness of NW is guaranteed. Concerning the regular mode, the same issue exists as shown in the hypotheses (H1) and (H2) for the derivation of (D3), (D4), and (D10).

6. Comparative Analysis

6.1. Comparison by Security Strength

Here, we compare the authentication schemes that are formally analyzed in Section 3. The comparisons are based on security properties, key features that IMD authentication protocols need to possess, computational overhead, and latency. Accordingly, each of the authentication protocols is checked against different security requirements (integrity (INT), confidentiality (CNF), authentication (AUT), session key agreement (SKA), perfect forward secrecy (PFS), and replay attack protection (RAP)) as shown in Table 3.

Table 3. Comparison by security strength.

Notation	INT	CNF	AUT	SKA	PFS	RAP
Khan et. al	✓	✓	✓	✓	✓	✓
Wu et. al.	✓	✓	✓	✓	✓	✓
Chi et. al.	✓	✓	✓	✓	✓	✓
Parvez et al.	✗	∆	✓	✓	✓	✗
Iqbal et. al.	✗	✗	✓	✓	✗	✗
He and Zeadally	∆	✓	✓	✓	✓	✓
Ellouze et. al.	∆	∆	✓	✓	∆	✓

✓ denotes that the scheme supports a particular requirement; ✗ denotes that the scheme does not support a particular requirement, ∆ denotes calls for the additional assumption.

6.2. Comparison by Functionality

Various vital functionalities are expected to be satisfied by authentication protocols, in particular features like emergency authentication (EMA), key update mechanisms (KUM), adaptability (ADP), application (APP), and anonymity (ANO) is used to compare the protocols. The comparison result of the authentication schemes concerning these functionalities is shown in Table 4.

Table 4. Comparison by functionality.

Notation	EMA	KUM	ADP	APP	ANO
Khan et. al	✗	✗	A	Generic	✓
Wu et. al.	✗	✗	A	Generic	✗
Chi et. al.	✓	✗	A	Generic	✓
Parvez et al.	✗	✗	A	Generic	✓
Iqbal et. al.	✗	✗	A+	Generic	✗
He and Zeadally	✗	✗	A+	Generic	✓
Ellouze et. al.	✓	✗	A-	Specific	✗

✓ denotes that the scheme supports a particular requirement; ✗ denotes that the scheme does not support a particular requirement. A+: Adaptable for the already implanted device, A: adaptable for yet to be implanted but manufactured, A-: difficult to adapt.

6.3. Comparison by Computational and Communicational Overhead

The computational and communication overheads, in terms of time, to perform the cryptographic operations (such as the number of signatures, symmetric, and asymmetric key encryption and decryption, hash functions, and XOR operations) [46–48], and size of the messages communicated [46,49], respectively, are shown in Tables 5–8. The comparison of protocols concerning computational and communication overheads is depicted in Figure 17.

Table 5. Approximate computational time in millisecond.

Notation	Meaning	Computational Time
T_{H}	Cryptographic hash function	0.32
T_{SE}	Symmetric encryption	5.6
T_{SD}	Symmetric decryption	5.6
T_{EM}	Elliptic curve point multiplication	63
T_{AE}	Asymmetric encryption	62
T_{AD}	Asymmetric decryption	36
T_{SIGN}	RSA-1024 digital signature	7
T_{VER}	RSA-1024 digital signature verification	~0
T_{XOR}	Bitwise XOR operation	0.32

Table 6. Approximate message length in Bits.

Message Type	Message Length
Public key size for an RSA encryption	1024
Length of an RSA Signature	1024
RSA-1024 digital Certificate	602
Elliptic curve point	320
Cryptographic hash function (SHA-1)	160
Key size for AES encryption	128
Identity	32
Timestamp	32
Sequence number	32
Symmetric decryption	32

Table 7. Computational overheads of the authentication protocols.

Protocol	Overhead	Time (Milliseconds)
Khan et. al	$12T_H + 23T_{XOR}$	3.84
Wu et. al.	$9T_H + 3T_{SE} +3T_{SD} + 1T_{AE} +1T_{AD} + 2T_{SIGN} + 2T_{VER}$	247.48
Chi et. al.	$16T_H + 4T_{SE} + 4T_{SD} + 1T_{AE} +1T_{AD} + 2T_{SIGN} + 2T_{V\ ER}$	260.92
Parvez et al.	$4T_H + 4T_{SE} + 4T_{SD}$	46.08
Iqbal et. al.	$4T_{SE} + 4T_{SD}$	44.80
He and Zeadally.	$4T_H + 4T_{SE} + 4T_{SD} + 6T_{EM}$	148.68
Ellouze et. al.	$6T_H + 1T_{SE} + 1T_{SD}$	13.12

Table 8. Communication overheads of the authentication protocols.

Protocol	Roundtrips	Overheads (Bits)
Khan et. al	2	1504
Wu et. al.	6	6554
Chi et. al.	9	7866
Parvez et al.	3.5	2304
Iqbal et. al.	2	1024
He and Zeadally.	3.5	3232
Ellouze et. al.	3	961

6.4. Overall Comparison of the Authentication Protocols

The comparison metrics—security strength, functionality, and efficiency—can be collectively used to understand better these schemes regarding security, competence, and capability. Such comparison can be best described in a triangular graph, as shown in Figure 18.

Figure 18 shows that Khan et al.'s scheme is located at the center since the protocol satisfies all the three metrics compared to the other protocols. On the other hand, while Iqbal et al. and Ellouze et al.'s schemes are only good at efficiency, Wu et al.'s and He and Zeadally's protocols fulfill only security and functionality, respectively. Concerning Chi et al.'s scheme, only functionality and security is satisfied while efficiency is not met. On the other hand, the Parvez et al.'s, satisfy functionality and efficiency while falling short in meeting security.

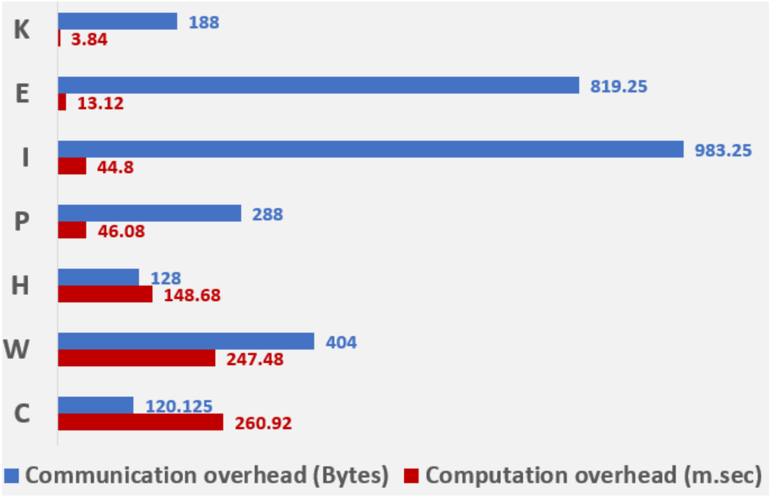


Figure 17. Computational and communication overheads of the authentication protocols.

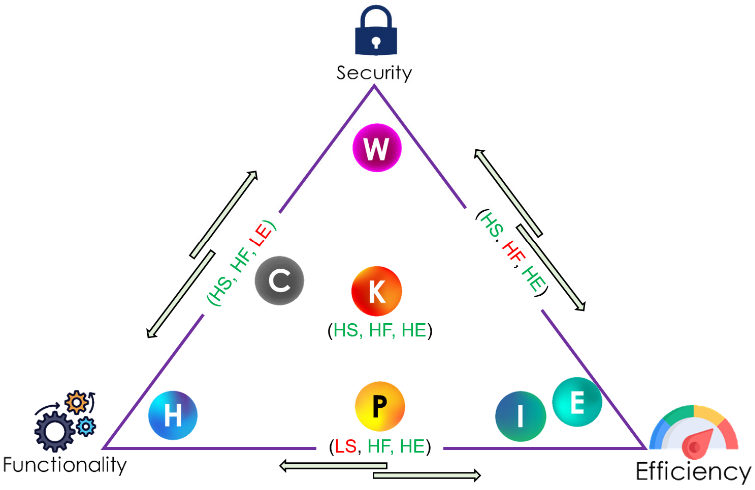


Figure 18. Overall comparison of the authentication protocols using triangular graph.

7. Conclusions

In this research, we studied various IMD-related security and privacy requirements, such as confidentiality, integrity, availability, mutual authentication, non-traceability, user anonymity, session-key agreement, forward and backward secrecy, known attack resistance, device-existence privacy, device-type privacy, specific-device ID privacy, measurement and log privacy, and bearer privacy. Furthermore, we examined some of the well-known threats of IMDs: learning the existence of IMD, eavesdropping on the wireless channel that links the IMDs to the external devices, replay attacks by forwarding exchanged messages at a later time, changing critical settings of the implants by producing new commands, and exhausting the battery life of IMDs to execute denial of service attacks. After studying various IMD-related security and privacy concepts, we have used a formal approach to test the strength of seven contemporary authentication schemes designed to thwart attacks surrounding IMD-enabled systems. Consequently, we formally analyzed these authentication schemes using AVISPA and BAN logic, and compared them against their security strength, computational and communication overheads, and other features. The result analysis indicates that Khan et al. is the lightest and fastest while preserving privacy and satisfying the security properties shown in Table 3. The protocol uses only a cryptographic hash function and a bitwise XOR function, which made its computational and communication overheads lighter. Furthermore, the protocol is adaptable with minimal effort for the already implanted devices and no trouble for the yet-to-be implanted devices. Another important lesson taken from the analysis of the protocols is the necessity of formal security verification before IMD protocols are released for public use. In addition, IMD authentication schemes need to satisfy essential functionalities such as portability and emergency authentication while remaining lightweight. Accordingly, there is an interest to design a new security protocol for IMD-enabled insulin pumps in the future, which will serve as an artificial pancreas for patients in need. While designing such protocols, the authors would like to apply the essential lessons learned during this study. The newly designed protocol should be formally analyzed while satisfying the emergency authentication, adaptability, key update mechanisms, and anonymity requirements. The authors would also put forth an effort to balance these requirements with efficient communication and computational overhead and good attack resistance.

Author Contributions: Conceptualization, D.G.D., I.Y. and J.K.; methodology, D.G.D. and I.Y.; validation, D.G.D. and J.K.; formal analysis, D.G.D. and J.K.; investigation, D.G.D. and Y.E.G.; data curation, D.G.D. and J.K.; writing—original draft preparation, D.G.D., Y.E.G. and J.K.; writing—review and editing, I.Y. and J.K.; visualization, D.G.D.; supervision, I.Y.; project administration, I.Y.; funding acquisition, I.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2020R1I1A2073603) as well as the Soonchunhyang University Research Fund.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Coherent Market Insights. U.S. Implantable Medical Devices Market Analysis. 2020. Available online: https://www.coherentmarketinsights.com/market-insight/us-implantable-medical-devices-market-3853 (accessed on 20 November 2021).
2. IMARC Implantable Medical Devices Market: Global Industry Trends, Share, Size, Growth, Opportunity and Forecast 2020–2025. 2020. Available online: https://www.imarcgroup.com/implantable-medical-devices-market (accessed on 20 November 2021).
3. Maddock, N.A.; James, N.L.; McKenzie, D.R.; Patrick, J.F. Technological advances for polymers in active implantable medical devices. In *The Design and Manufacture of Medical Devices*; Elsevier: Amsterdam, The Netherlands, 2012; pp. 239–272.
4. Kitana, A.; Traore, I.; Woungang, I. Towards an Epidemic SMS-based Cellular Botnet. *J. Internet Serv. Inf. Secur.* **2020**, *10*, 38–58.
5. Shichkina, Y.A.; Kataeva, G.V.; Irishina, Y.A.; Stanevich, E.S. The use of mobile phones to monitor the status of patients with Parkinson's disease. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2020**, *11*, 55–73.
6. Camara, C.; Peris-Lopez, P.; Tapiador, J.E. Security and privacy issues in implantable medical devices: A comprehensive survey. *J. Biomed. Inform.* **2015**, *55*, 272–289. [CrossRef]
7. Liu, N.; Yu, M.; Zang, W.; Sandhu, R.S. Cost and Effectiveness of TrustZone Defense and Side-Channel Attack on ARM Platform. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2020**, *11*, 1–15.
8. Kasturi, G.S.; Jain, A.; Singh, J. Detection and Classification of Radio Frequency Jamming Attacks using Machine learning. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2020**, *11*, 49–62.
9. Wong, S.K.; Yiu, S.-M. Location spoofing attack detection with pre-installed sensors in mobile devices. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2020**, *11*, 16–30.
10. Alizadeh, M.; Andersson, K.; Schelen, O. A Survey of Secure Internet of Things in Relation to Blockchain. *J. Internet Serv. Inf. Secur.* **2020**, *10*, 47–75.
11. Wong, S.K.; Yiu, S.-M. Identification of device motion status via Bluetooth discovery. *J. Internet Serv. Inf. Secur.* **2020**, *10*, 59–69.
12. Rushanan, M.; Rubin, A.D.; Kune, D.F.; Swanson, C.M. Sok: Security and privacy in implantable medical devices and body area networks. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 524–539.
13. Siddiqi, M.A.; Doerr, C.; Strydis, C. Imdfence: Architecting a secure protocol for implantable medical devices. *IEEE Access* **2020**, *8*, 147948–147964. [CrossRef]
14. Belkhouja, T.; Sorour, S.; Hefeida, M.S. Role-Based Hierarchical Medical Data Encryption for Implantable Medical Devices. In Proceeding of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.

15. Tutari, V.H.; Das, B.; Chowdhury, D.R. A Continuous Role-Based Authentication Scheme and Data Transmission Protocol for Implantable Medical Devices. In Proceedings of the 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), Gangtok, India, 25–28 February 2019; pp. 1–6.
16. Camara, C.; Peris-Lopez, P.; De Fuentes, J.M.; Marchal, S. Access control for implantable medical devices. *IEEE Trans. Emerg. Top. Comput.* **2020**, *9*, 1126–1138. [CrossRef]
17. Zhang, Z.; Xu, X.; Han, S.; Liang, Y.; Liu, C. Wearable Proxy Device-Assisted Authentication Request Filtering for Implantable Medical Devices. In Proceedings of the 2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Korea, 25–28 May 2020; pp. 1–6.
18. Astillo, P.V.; Choudhary, G.; Duguma, D.G.; Kim, J.; You, I. TrMAps: Trust Management in Specification-based Misbehavior Detection System for IMD-Enabled Artificial Pancreas System. *IEEE J. Biomed. Health Inform.* **2021**, *25*, 3763–3775. [CrossRef]
19. Astillo, P.V.; Duguma, D.G.; Park, H.; Kim, J.; Kim, B.; You, I. Federated intelligence of anomaly detection agent in IoTMD-enabled Diabetes Management Control System. *Futur. Gener. Comput. Syst.* **2021**, *128*, 395–405. [CrossRef]
20. Abhishta, A.; van Heeswijk, W.; Junger, M.; Nieuwenhuis, L.J.M.; Joosten, R. Why would we get attacked? An analysis of attacker's aims behind DDoS attacks. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2020**, *11*, 3–22.
21. Burrows, M.; Abadi, M.; Needham, R.M. A logic of authentication. *Proc. R. Soc. Lond. A. Math. Phys. Sci.* **1989**, *426*, 233–271.
22. Armando, A.; Basin, D.; Boichut, Y.; Chevalier, Y.; Compagna, L.; Cuéllar, J.; Drielsma, P.H.; Héam, P.-C.; Kouchnarenko, O.; Mantovani, J.; et al. The AVISPA tool for the automated validation of internet security protocols and applications. In *International Conference on Computer Aided Verification*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 281–285.
23. Khan, H.; Dowling, B.; Martin, K.M. Highly efficient privacy-preserving key agreement for wireless body area Networks. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy in Computing and Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1064–1069.
24. Wu, L.; Chi, H.; Du, X. A Secure Proxy-based Access Control Scheme for Implantable Medical Devices. *arXiv* **2018**, arXiv1803.07751.
25. Chi, H.; Wu, L.; Du, X.; Zeng, Q.; Ratazzi, P. e-SAFE: Secure, efficient and forensics-enabled access to implantable medical devices. In Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; pp. 1–9.
26. Parvez, K.; Zohra, F.T.; Jahan, M. A secure and lightweight user authentication mechanism for wireless body area network. In Proceedings of the 6th International Conference on Networking, Systems and Security, Dhaka, Bangladesh, 17–19 December 2019; pp. 139–143.
27. Iqbal, J.; Umar, A.I.; ul Amin, N.; Din, N. Efficient Key Agreement and Nodes Authentication Scheme for Body Sensor Networks. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 180–187. [CrossRef]
28. He, D.; Zeadally, S. Authentication protocol for an ambient assisted living system. *IEEE Commun. Mag.* **2015**, *53*, 71–77.
29. Ellouze, N.; Allouche, M.; Ben Ahmed, H.; Rekhis, S.; Boudriga, N. Securing implantable cardiac medical devices: Use of radio frequency energy harvesting. In Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices, Berlin, Germany, 4 November 2013; pp. 35–42.
30. Fu, C.; Du, X.; Wu, L.; Zeng, Q.; Mohamed, A.; Guizani, M. Poks based secure and energy-efficient access control for implantable medical devices. In *International Conference on Security and Privacy in Communication Systems*; Springer: Cham, Switzerland, 2019; pp. 105–125.
31. Antonescu, B.; Basagni, S. Wireless body area networks: Challenges, trends and emerging technologies. In Proceedings of the 8th International Conference on Body Area Networks, Boston, MA, USA, 30 September–2 October 2013; pp. 1–7.
32. Ellouze, N.; Allouche, M.; Ahmed, H.B.; Rekhis, S.; Boudriga, N. Security of implantable medical devices: Limits, requirements, and proposals. *Secur. Commun. Netw.* **2014**, *7*, 2475–2491. [CrossRef]
33. Amar, A.B.; Kouki, A.B.; Cao, H. Power approaches for implantable medical devices. *Sensors* **2015**, *15*, 28889–28914. [CrossRef]
34. Islam, M.N.; Yuce, M.R. Review of medical implant communication system (MICS) band and network. *ICT Express* **2016**, *2*, 188–194. [CrossRef]
35. Strydis, C.; Seepers, R.M.; Peris-Lopez, P.; Siskos, D.; Sourdis, I. A system architecture, processor, and communication protocol for secure implants. *ACM Trans. Archit. Code Optim.* **2013**, *10*, 57. [CrossRef]
36. He, D.; Zeadally, S.; Kumar, N.; Lee, J.-H. Anonymous authentication for wireless body area networks with provable security. *IEEE Syst. J.* **2016**, *11*, 2590–2601. [CrossRef]
37. Halperin, D.; Heydt-Benjamin, T.S.; Ransford, B.; Clark, S.S.; Defend, B.; Morgan, W.; Fu, K.; Kohno, T.; Maisel, W.H. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP 2008), Oakland, CA, USA, 18–22 May 2008; pp. 129–142.
38. Burleson, W.; Clark, S.S.; Ransford, B.; Fu, K. Design challenges for secure implantable medical devices. In Proceedings of the DAC Design Automation Conference 2012, San Francisco, CA, USA, 3–7 June 2012; pp. 12–17.
39. Zheng, G.; Shankaran, R.; Orgun, M.A.; Qiao, L.; Saleem, K. Ideas and challenges for securing wireless implantable medical devices: A review. *IEEE Sens. J.* **2016**, *17*, 562–576. [CrossRef]
40. Gollakota, S.; Hassanieh, H.; Ransford, B.; Katabi, D.; Fu, K. They can hear your heartbeats: Non-invasive security for implantable medical devices. In Proceedings of the ACM SIGCOMM 2011 Conference, Toronto, ON, Canada, 15–19 August 2011; pp. 2–13.

41. Duguma, D.G.; Kim, J.; Kim, B.; You, I. A Formal Security Verification on He and Zeadally's Authentication Protocol for IMD-Enabled Ambient Assisted Living System. In Proceedings of the 2020 ACM International Conference on Intelligent Computing and its Emerging Applications, GangWon, Korea, 12–15 December 2020; pp. 1–6.
42. Kim, J.; Lee, S.; Duguma, D.G.; Kim, B.; You, I. Comments on" Securing implantable cardiac medical devices" Use of radio frequency energy harvesting. In Proceedings of the 2020 ACM International Conference on Intelligent Computing and its Emerging Applications, GangWon, Korea, 12–15 December 2020; pp. 1–5.
43. Boyd, C.; Mao, W. On a Limitation of BAN Logic. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1993; pp. 240–247.
44. Von Oheimb, D. The high-level protocol specification language HLPSL developed in the EU project AVISPA. In Proceedings of the APPSEM 2005 Workshop, Frauenchiemsee, Germany, 12–15 September 2005; pp. 1–17.
45. Al-Turjman, F.; Alturjman, S. Context-sensitive access in industrial internet of things (IIoT) healthcare applications. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2736–2744. [CrossRef]
46. Challa, S.; Wazid, M.; Das, A.K.; Khan, M.K. Authentication protocols for implantable medical devices: Taxonomy, analysis and future directions. *IEEE Consum. Electron. Mag.* **2017**, *7*, 57–65. [CrossRef]
47. Saho, N.J.G.; Ezin, E.C. Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm. In Proceedings of the CARI 2020-Colloque Africain sur la Recherche en Informatique et en Mathématiques Apliquées, Thiès, Senegal, 22 September–2 October 2020.
48. Fog, A. Instruction tables: Lists of Instruction latencies, Throughputs and Micro-Operation Breakdowns for Intel, AMD and VIA CPUs. Available online: https://www.agner.org/optimize/instruction_tables (accessed on 20 November 2021).
49. FM4DD. X509 Certificate Examples for Testing and Verification. Available online: http://fm4dd.com/openssl/certexamples.htm (accessed on 20 November 2021).