Lone *et al. EURASIP Journal on Wireless Communications and Networking* (2020) 2020:146
https://doi.org/10.1186/s13638-020-01759-5

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Securing communication by attribute-based authentication in HetNet used for medical applications

Tufail A. Lone[1], Aabid Rashid[1], Sumeet Gupta[1], Sachin Kumar Gupta[1*], Duggirala Srinivasa Rao[2], Mohd Najim[3], Ashutosh Srivastava[4], Abhishek Kumar[5], Lokendra Singh Umrao[6] and Achintya Singhal[5]

* Correspondence: sachin.rs.eee@iitbhu.ac.in
[1]School of Electronics & Communication Engineering, Shri Mata Vaishno Devi University, Kakryal, Katra (J&K) 182320, India
Full list of author information is available at the end of the article

Abstract

One of the major applications of the Heterogeneous Network (HetNet) is in the healthcare system. Deploying HetNet in healthcare systems enables patients, physicians, and other stakeholders to communicate easily with each other. Due to the large growth in the network's subscribers, the security of the stored health data became one of the major concerns because unauthorized access to this data may lead to very serious complications, and unreliable transmission of data may lead to fatal risks to the patient's life. Therefore, taking data integrity into consideration, user authentication has become one of the main factors. However, significant research work has been performed at HetNet's physical layer to secure communication, but the result of this leads to an increase in hardware components. The increasing hardware components not only costs money but also power consumption. Therefore, this paper presents an alternate way of securing communication in HetNet at the network layer. However, resolving security problems at the network layer increases computational complexity. Nevertheless, earlier, some encryption techniques like identity-based encryption (IBE), symmetric key encryption (SKE), and public-key encryption (PKE) have been utilized for securing data. Due to their own disadvantages, this paper utilizes an attribute-based encryption (ABE) authentication scheme for securing health data in medical applications. With the help of this method, access to the intruders is denied which results in reduced communication overhead. This authentication scheme helps protect the essential information against attacks by the intruders. It includes a third party server that helps to authenticate and store patient's information. The whole security technique has been written in the form of HLPSL (high-level protocol specification language) codes, and the results are then validated with the help of AVISPA (automated validation of Internet security protocols and applications) tool.

Keywords: Heterogeneous networks, Authentication (ABE), Network layer, HLPSL, AVISPA

1 Introduction

Nowadays, wireless communication has developed its essence in wide solicitations of current advanced domain like safety, medical, rescue, and security purposes [1]. Due to the rise in the number of users, there is an increase in data traffic on the network, which results in increased latency. Therefore, next generation of mobile networks such as 5G and beyond is expected to tackle demands in a range of technological contexts such as Quality of Service (QoS), continuous large-transmission range, hot-spot high volume, throughput, and enormous connection [2]. This is where HetNets show a substantial role. HetNet helps in enhancing the coverage area and capacity of a network by deploying mini base stations (BS) called micro-BS, nano-BS, femto-BS, etc. [3]. HetNets also improve the QoS and throughput and decrease latency [4]. For the large deployment of these mini cells, there are high chances of interference that are key issues in HetNet [5]. Thus, communicated signal must be capable of carefully eliminating the interference. Energy usage is also growing owing to the installation of mini cells and substantial traffic, which cannot be allowed in low-power appliances such as WSN and IoT systems; thus, the emergence of technologies such as simultaneous wireless information and power transmission (SWIPT) came into existence [6].

Due to rapid development in IoT-based smart appliances, emerging wireless communication seems to have a much higher need for large data, nearly wide-reaching range, and efficient privacy performance [7]. With all of these considerations, HetNet has evolved a potential alternative by raising cell density for better reuse of spatial spectrum [8]. Communication in wireless networks is carried out via public channels, and since these channels are of broadcast nature, hence, protection of data in HetNets becomes a prime concern [9]. Consequently, information transmitted via wireless channels can be easily obtained inside the transmission range by an unintended user [10]. This leaves HetNets communication vulnerable to attacks by intruders, which can pose serious problems as users exchange sensitive information between them. Figure 1 presents an outline of the HetNet architecture in the healthcare domain. The circles shown denote the hospitals which are connected to smaller base stations, and boxes inside them are the various departments. All of them are connected to one macro base station (MBS). These hospitals can communicate with each other and also with users through small base stations and MBS in the presence of intruders.

In identifying the valid user, the physical layer attributes simplify the authentication procedure. But relying entirely on a single physical layer attribute is not considered a viable option, as the characteristic chosen might not have sufficient dynamic range for precise distinction [11]. Therefore, we need to look for alternate ways of authentication. For instance, end-to-end encryption is an example of network layer security, which prohibits data leakage to the attacker [12]. The identity-based encryption (IBE) is employed for securing health data of patients. But in the case of IBE, there is only one attribute that needs necessarily to be fulfilled to get access to the data; otherwise, authentication will fail. This means IBE does not provide a wide dynamic range for authentication; hence, it is less error-tolerant [13–15].

For the medical applications, HetNets can prove very useful in connecting various hospitals to each other, so that they can share necessary information between themselves. Therefore, the data is liable to attacks during the transmission on a network because intruders can manipulate a person's sensitive information and may pose a danger to one's life [16]. We have a wide variety of staff in hospitals, and the authentication

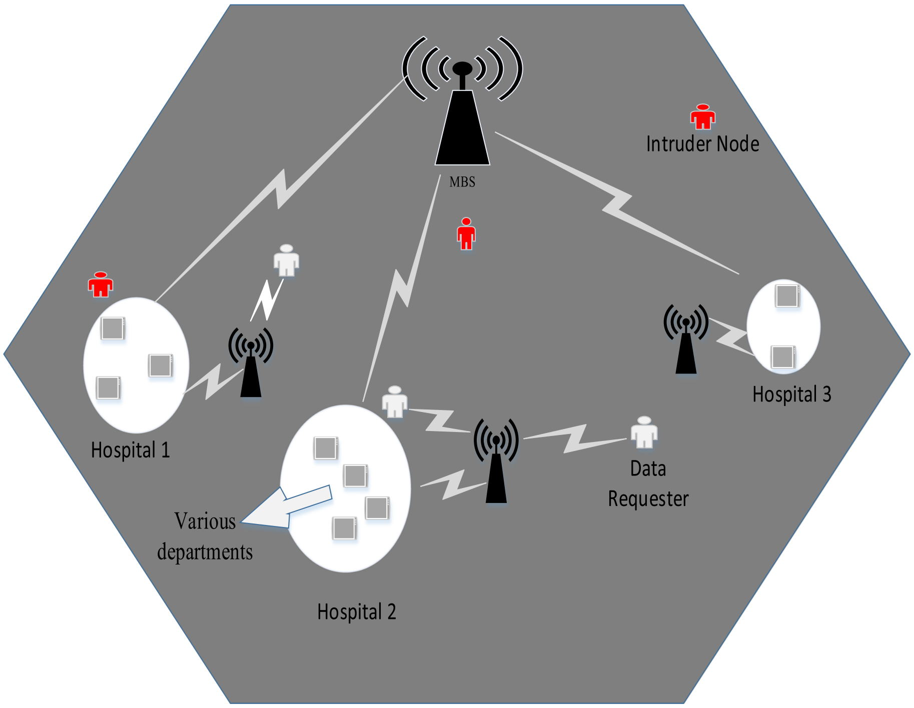


Fig. 1 Outline of HetNet architecture in healthcare

scheme implemented must have a wide dynamic range to authenticate the users. The security problems can be resolved on multiple layers of the OSI model. The physical layer protection is also not a feasible choice here because it does not have a wide dynamic range. To increase the dynamic range of the physical layer, we will require a lot of hardware which increases cost as well as power consumption. That is why, this paper proposes attribute-based authentication for verifying the users as it has a wide dynamic range, and it also minimizes the hardware and power consumption constraints as it is employed on the network layer. The key concern is to secure health records of patients, particularly if they have been deposited on a third-party server that the public does not believe entirely [17]. Therefore, in medical applications, security of data is of main concern. For HetNets used in medical applications, an attribute-based authentication scheme is proposed in this article, so that only credible users can access patient's health records. An attribute-based authentication scheme provides a wide dynamic range for authentication and hence good error tolerance.

1.1 Motivation and contribution

The introduction of electronic health recorders to collect patient information in the healthcare system has various steps. It electronically stores patient medical records and uploads them to a database server [16]. From the perspective of the medical care system, patients see several doctors during their lives, from attending a primary health clinic to hospitals. Therefore, health records are created with every clinical meeting or emergency visits [17, 18]. Keeping data integrity in view, safe routing is a very important issue within a given network (HetNet). For securing communication in HetNets, most of the research work is done at the physical layer [8, 9]. In medical applications like hospitals where we have a wide variety of users, our authentication scheme needs to be robust with a wide dynamic range for authentication. If security issues are addressed at the physical layer, we need to increase its dynamic range, which requires a lot of hardware, hence further increase in cost and power consumption. Therefore for such applications, physical layer security is not a feasible option. Although few techniques were employed at the network layer, they had limitations like IBE has less dynamic range [19]; in symmetric key encryption, exchanging the key secretly between the users is a big problem [20]. Therefore, the key objective of this article is to address security issues at the network level by employing ABE authentication as it contains characteristics like efficient key management, error tolerance, privacy preservation, emergency data storage, and retrieval.

The contribution of this paper is that the health data of patients have been successfully secured while routing it to the data requesters. This is possible by employing ABE authentication on the stored data.

The remaining article is oriented as current related work performed in the relevant field is discussed in Section 2. Section 3 addresses ABE's background. In addition, the recommended method is presented in division 4, Section 5 gives a brief introduction about AVISPA tool, Section 6 shows the formal validation of proposed scheme in AVISPA tool, Section 7 is regarding the results and discussion of the proposed approach, and finally, Section 8 comes up with the conclusion and future scope.

2 Related work

This section will be discussing different methods being employed for securing the communication within the HetNet and techniques being used in securing the health data.

2.1 Security-related work at physical layer on HetNet

Several accomplishments have been dedicated to security problems in HetNets for the past few years, such as Hu et al. [2] recently examined the PLS in HetNets backed by SWIPT to boost the safety issue. Further, they inserted artificial sound in the communicated beam together with the macrocell and femtocell base stations. Subsequently, authors in [5] realized that multi-tier structural design together with rigorous 5G latency requisites poses new security challenges due to possible repeated deliveries and validations in 5G mini cells and HetNets. Thus, introducing SDN in 5G will allow efficient authentication handovers and protection of privacy through its centralized control capability. In another research, authors of article [10] suggested a joint source allocation scheme that under fairness requirements simultaneously considers PLS, cross-level intervention, and joint power optimization and sub-carriers. Duan et al. [11] in another paper proposed SDN-supported fast validation approach utilizing weighted SCI handover to enhance authentication performance during handover and satisfy the 5G latency needs. In paper [21], authors have introduced FFFTM (Flooding Factor-based Framework for Trust Management) in MANETs for the secure transmission of data. The true flooding method is used to recognize intruder nodes depending on the evaluation of trust value. Makarfi et al. [22] presented the ordinary logarithmic expression for the system capability in a different form, to allow the study of the random variables describing the channel fading and interference in terms of the joint moment generating functions (MGF). In [23], an interference management method for PLS in a two-tier HetNet system to increase the user's secrecy rate under eavesdropping attack is proposed. Wang et al. [24] investigated the PHY layer security of a two-tier HetNet thru sub 6 GHz substantial MIMO macrocells and millimeter wave (mmWave) small cells. They evaluated the scope and secrecy efficiency using stochastic geometry by taking into account the pilot attacks from the spies.

Some of the work related to our proposed scheme is discussed in Table 1; it is quite evident that the ABE scheme has been used for securing data in networks like vehicular ad hoc network, Internet of things, and body sensor network. For securing communication in HetNet, various studies have been dedicated to the PHY layer, nevertheless, no effort is carried-out at network layer utilizing such approaches. Hence, this research article proposes an ABE authentication scheme to secure data in medical-dedicated HetNet.

2.2 Security-related work for medical application

Issues regarding protecting the privacy of patients and the security of medical details are two basic problems with the proper use of electronic medical services [33]. Different techniques are used to protect this healthcare data. The most commonly used techniques are validation, encryption, data masking, access control, monitoring, auditing, and so on [34]. In paper [35], the authentication at the physical layer is introduced by utilizing the time-varies CFO (carrier frequency offset) related through each couple of wireless communications systems. Encryption methods like IBE, SKE, and conventional PKE techniques may be utilized for securing the health data recorded by body sensors [14]. Sudarsono et al. [13] presented a secure sharing of data in the e-healthcare system utilizing IBE with signature. So that data can only be shared by authentic users based on specific public identity, and data exchanged is encrypted and authenticated such that only authorized users can exchange the data. Although IBE does not require a public key distribution infrastructure, it has a less dynamic range as it considers only one attribute that needs to be fulfilled necessarily [19]. Similarly, SKE is faster as it utilizes only one key for encryption and decryption, but exchanging this key secretly between the users is a big problem [20]. All these techniques are used for securing the essential health data of users at the network layer. The attacks on network layer capture information, modify it, and direct for re-communication [17]. Taking the above limitations into consideration, ABE authentication is taken into account to keep safe the health information from these kinds of attacks. Further, the comprehensive evaluation of the existing security protocols in the state-of-the-art is carried-out in Table 1.

3 Background

This portion provides a short-lived description with regards to ABE access control [15].

3.1 Bilinear maps

Assuming there are two multiplicative cyclic groups G_0 and G_1 of prime order p, let g be generator of G_0, and e be a bilinear map, $e: G_0 \times G_0 \rightarrow G_1$. The characteristics of bilinear map e are as given below:

Table 1 Comparative study of state-of-the-art security approaches in the domain

Type of network	Objective	Problem raised	Solution proposed	Features
HetNet [8]	To enhance PHY layer security (PLS).	Emphasis on secure downlink transmission.	Massive MIMO deployment significantly increases secrecy performance.	• Spectrum efficiency improves due to densely installed BSs. • BS having big array of antenna offers huge array gain to its authorized user.
HetNet [9]	To enhance PLS.	Increasing security during transmission in wireless HetNet.	SLS and BLS are two transmission schemes taken within such system to boost PLS by using content properties of cached files.	• Artificial interference incorporated by SLS will resist Eve that may be removed by cache-enabled consumers. • Without cached file, eves can decode nothing in BLS. • SLS and BLS are successful in achieving huge security gain as compared to normal transmission.
VANET [25]	To enhance PLS in vehicular network using reconfigurable intelligent surface (RIS).	To examine the average secrecy capacity of the system under consideration	Two vehicular network system models are presented that are RIS-based transmission: one is vehicle-to-vehicle interaction with source using access point and other one is in form of VANET with RIS-based relay installed on building.	• RIS technologies evolved as an essential model for smart radio environments where vast numbers of small, low-cost, and passive components replicate the event signal with an adaptive phase shift deprived of the need for a dedicated energy source.
VANET [26]	To enhance effectiveness of r escues with safety assurance.	Computational latency and communication overhead is minimized.	ABE access control scheme.	• Keeps communication private, avoids collision attacks, and enables fine grained access control. • Privacy and reliability improved.
VANET [27]	Collaborative transmission in VANET, when straight transmission between origin and target is not likely.	Make data transmission relays secure.	CP-ABE is utilized in proposed protocol as it offers encrypted access control approach.	• Suggested approach guarantees secrecy. • This approach depends on authentication of signature to guarantee the accuracy of delivered messages.
VANET [28]	Secure billing protocol over ABE in vehicular cloud computing.	Safe communication protocols.	ABE is deployed to ensure access control depending on the services	• Pseudonym methods are employed to protect identity of

Table 1 Comparative study of state-of-the-art security approaches in the domain *(Continued)*

Type of network	Objective	Problem raised	Solution proposed	Features
			purchased. Hash chain methodology is used to allow a vehicle to buy a service by means of an electronic voucher that it must possess.	vehicles and their required services. • The suggested approach enables reliable billing attributes with lesser computational overhead for vehicular cloud computing.
MANET [29]	To provide the DoS and intrusion detection system in MANETs that will be based on FSM.	DoS and intrusion issues in MANET.	ID-AODV protocol is suggested based on FSM.	• Detection systems are developed using the FSM principle for both attacks: packet dropping and sequence number's duplication due to DoS and intrusion attack, respectively. • ID-AODV's main technical features include network monitoring system, FSM, and attack detection model.
BSN [30]	To guarantee the security and safety of information fused at the BSN coordinator.	Privacy of information.	KP-ABE is employed to guarantee privacy of information.	• KP-ABE offers easy and safe encryption over CP-ABE because KP-ABE is a lightweight encryption scheme.
IoT [31]	To regulate the access to data.	Data protection in resource-limited systems.	CP-ABE using efficient pre-computation methods.	• The pre-computation method is extended to the CP-ABE encryption scheme that enables to reduce computational costs of encryption. • Reduce practical challenges in deployment of CP-ABE on resource-limited systems.
Under-water wireless sensor network (UWSN) [32]	Design routing protocol for proficient communication between sensors and sinks in UWSN.	Efficient communication between sensors in UWSN.	RE-PBR protocol for UWSNs is presented.	• RE-PBR takes into account three factors to balance energy usage and effective message delivery namely link quality, depth, and residual energy.

- Bilinearity: for all $m, n \epsilon G_0$, and $x, y \epsilon Z_p$, we have $e(m^x, n^y) = e(m, n)^{xy}$.
- Non-degeneracy: $e(g, g) \neq 1$

G_0 is a bilinear group if the group operation in G_0 and the bilinear map $e: G_0 \times G_0 \rightarrow G_1$ are both competently computable. Notice that the depict e is symmetric since $e(g^x, g^y) = e(g, g)^{xy} = e(g^y, g^x)$.

3.2 Attribute-based encryption

There are many types of PKE, and ABE is one of them. ABE is also related to IBE, and the distinction between the two is that ABE scheme is one-to-many while IBE scheme is one-to-one [15, 19]. In ABE, a group of features is taken into consideration, and according to that set, the message is encrypted, such that decryption of message can be performed by only those users meeting the attributes in the attribute set.

3.2.1 Setup

Firstly describe universe of attributes $V = \{1, 2, 3, \ldots, n\}$. For each attribute $i \epsilon V$, choose a number r_i uniformly at random from Z_p. Finally, choose f uniformly at random in Z_p. The published public parameters are

$$R_1 = g^{r_1}, \ldots, R_{|V|} = g^{r_{|V|}}, F = e(g, g)^f$$

The master key is:

$$r_1, \ldots, r_{|V|}, f$$

We may also require a few cryptographic hash functions. Hash functions reduce the size of a large message to a fixed length; this is called a hash digest. Hash functions are always one-way functions, i.e., hash codes can be generated by applying hash functions on message, but vice versa is not possible.

Compared to symmetric key encryption, public-key encryption is costlier. Hence, certain hash functions are required to transform some random message of "*k*" bits to finite size of "*w*" bits.

3.2.2 Key generation (T, MK)

Here, algorithm generates an output key that makes client able to decode the data encrypted using attribute set "*a*" if $Q(a) = 1$. First of all, for every node "*x*" in the tree "*Q*", a polynomial "q_x" is selected. Beginning with root node "*p*", polynomials are chosen in a top-down fashion. When polynomials for every leaf node "*x*" are determined, the user is given the following secret value:

$$D_x = g^{\frac{q_x(0)}{r_i}}, \text{where } i = \text{att}(x).$$

Decryption key "*D*" is the group of above secret values.

3.2.3 Encryption (PK, N)

Here, message $N \epsilon G_1$ is encrypted using attribute set "*a*" by selecting a random value $n \epsilon Z_p$ and distribute ciphertext as:

$$E = \left(a, E^{'} = NY^{n}, \left\{Ei = T_{i}^{n}\right\}_{i \in a}\right)$$

3.2.4 Decryption

To generate N, parameters like a private key (S_i) and ciphertext (C) are taken as input. Decryption is going to succeed if the user's private key satisfies the access building present in C.

4 Proposed technique

ABE authentication scheme is used in the recommended system to make our health data accessible to those who meet the threshold amount of attributes. To get the required information from the memory servers by users, our routing will adhere to some access tree in order to avoid unnecessary data being routed to users. In this proposed scheme, the reliable equation model is implemented; the BS and the mini cells rely on whatever information comes from the registered users. Knowledge of attackers is also taken into account during the authentication process. The attacker can attack the communication channel in many ways, such as eavesdrop, hijack, and modify. Utilizing attribute-based authentication for the stored health record will help to route data to the desired targets and it will also prevent data from being exploited by an attacker.

The step by step process is explained here. In this process, the MBS acts as a trustworthy and reliable authority and manages the entire network by providing public-private keys. All of these keys are utilized for encryption and decryption algorithm. MBS authenticates users based on their credentials (S), and once they get authenticated, they receive their respective private keys (Si). Once attributes of user get matched with the attribute set (Z) of MBS, then confirmation information is directed to the owner of data that the consumer is authenticated to communicate. In the end, the owner of data must communicate safely with the intended user.

Suppose, doctor of oncology division of hospital 'A' wants to access a file (refer to Fig. 2). He requests to access to that particular file. The access is granted to the doctor for that specific file as soon as he satisfies the said attributes. It is mandatory that the file should not get routed to the unintended department. At the same time, if a doctor from the gynecology department from the same hospital also requests to access the same file, his request is denied because he does not satisfy the attributes required to access the file.

In Fig. 3, pictorial representation of the authentication process between the user and base station has been shown. The data requester has been granted its private key, i.e., "S_R", and the data owner is also granted the private key, i.e., "S_O". The data requester sends credentials for the verification process based on "S" value. On verification, an acknowledgement is provided to the message owner which indicates that message requester is allowed to interconnect. This ensures secure communication between the owner of the data and the data requester.

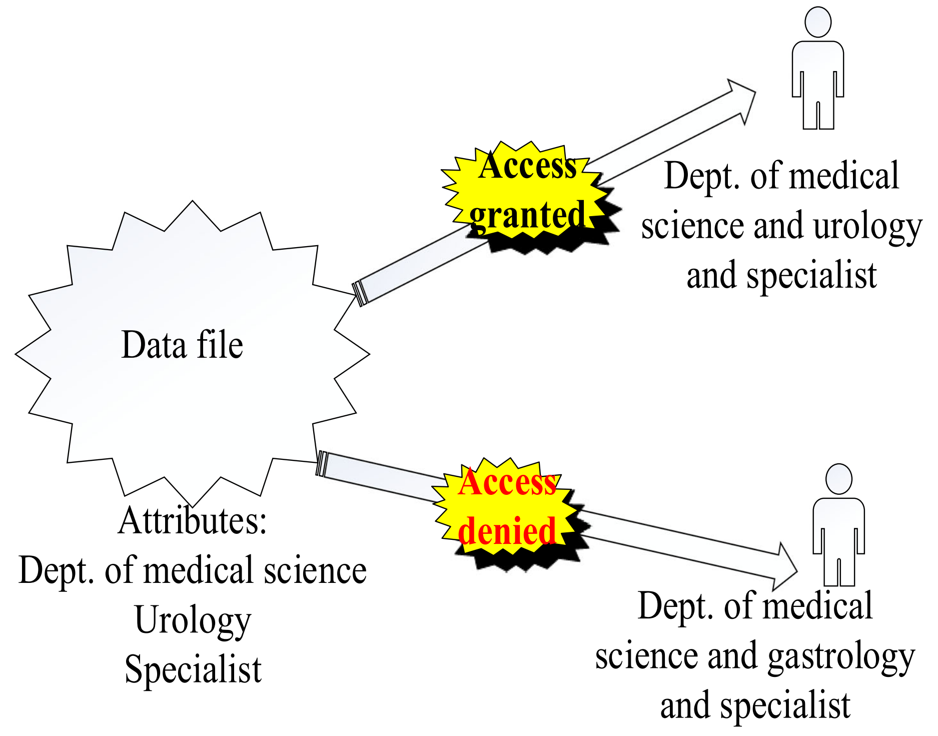

Access granted
Dept. of medical science and urology and specialist
Data file
Attributes:
Dept. of medical science
Urology
Specialist
Access denied
Dept. of medical science and gastrology and specialist

Fig. 2 Data routing using ABE

4.1 Advantage of attribute-based authentication

The advantage of using attribute-based authentication over identity-based authentication is that it is error-tolerant. That means if we have 10 attributes (say) in the attribute list we can set a threshold of 7 attributes. Anyone satisfying the said condition can get access the data while as in identity-based authentication of all the said identities needs

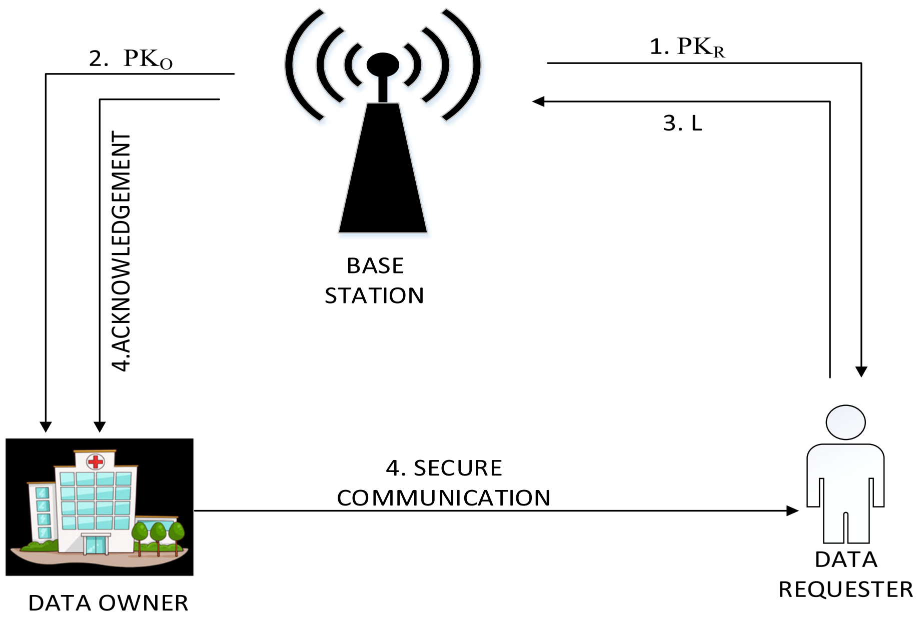


Fig. 3 Authentication of user by BS

to be fulfilled then only one can get access to the data. Therefore, it will make things difficult in our healthcare system.

4.2 Proposed algorithm

The significance of routing data in the healthcare organization employing attribute-based authentication scheme is presented in Fig. 4, where the flowchart for the whole technique has been depicted. The data requester sends its credentials to the base station for authentication. If the credentials of the data requester get matched with the attribute list of the base station, then the authentication is successful and the base station sends a signal to the owner of the data that the user is verified. Now, the data requester gets access to the data; otherwise, it denies the request by detecting the intruder.

Unsecure routing cannot be afforded in medical applications because the patient's health data is secret, and if it is not routed to desired users, it could cost somebody's life. Hence, our information essentials to be protected and routed to desired users. The following steps are taken to implement attribute-based authentication in HetNet and have been defined from Eqs. 1 to 6 in an algorithm manner. The prototype of HLPSL code is shown in the following steps:

$$BS \rightarrow R : Sd\left(\left\{\mathrm{N}_{\mathrm{y}}\right\}\right)\_K_r \tag{1}$$

Base station (BS) sends a nonce number "N_{y}" for authentication to data requester (R) and the whole message is encrypted using R's public key "K_{r}".

$$R : Rx\left(\left\{\mathrm{N}_{\mathrm{y}}\right\}\right)\_K_r \tag{2}$$

Data requester (R) receives nonce number "N_{y}" from BS.

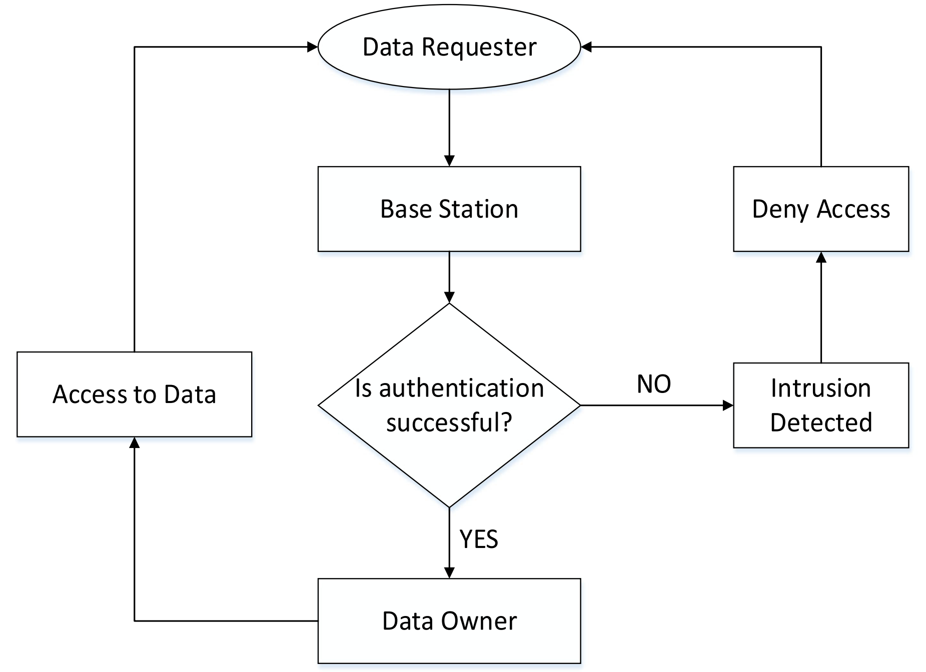


Fig. 4 Flowchart of proposed algorithm

$$R\rightarrow BS : Sd\left(\left\{\mathrm{N_y}, \mathrm{S}\right\}\right)\_K_s \tag{3}$$

Data requester (R) sends request to base station (BS) for verification on attribute values (S) along with a nonce number “N_{y}” and the whole message is encrypted using base station’s (BS) public key K_{s}.

$$BS : Rx\left(\mathrm{R.BS}\left(\left\{\mathrm{N_y}, \mathrm{S}\right\}\right)\_K_s\right)\mathrm{in}(\mathrm{R.S}, \mathrm{Z}) \tag{4}$$

Base station (BS) checks the nonce number sent by data requester’s (R) along with attributes (S) in its attribute-trust list (Z).

$$BS\rightarrow O : Sd\{BS.O.ok\} \tag{5}$$

After authentication, base station (BS) will send confirmation message (ok) to data owner (O) that data requester (R) is authenticated and you can proceed with the next packet.

$$O\rightarrow BS : Rx\{BS.O.ok\}\&Sd\{O.BS.ok\} \tag{6}$$

Data owner (O) sends back acknowledgement message (ok) to base station (BS) and says that it is ready to communicate.

Now, in the above entire prototype, the key generation is done in two major steps:

➢ Step_1. Setup phase at MBS:

$$\begin{aligned}\mathrm{MBS} : \mathrm{Input} &= \{Z\}\\ \mathrm{Output} &= \{M_{\mathrm{sk}}\}\end{aligned}$$

During this phase, the private key generator (here MBS) generates a master secret key (M_{sk}) based on attributes defined in Z.

➢ Step_2. Key generation phase:

$$\begin{aligned}\mathrm{MBS} : \mathrm{input} &= \{M_{\mathrm{sk}}\}\\ \mathrm{Output} &= \{S_{\mathrm{i}},\ \ K_{\mathrm{i}}\}\end{aligned}$$

The private key generator will distribute public keys (K_{i}) and secret keys (S_{i}) to the users connected to it using the master secret key.

Further, symbolizations using the above equations are specified in Table 2.

5 AVISPA tool

AVISPA examines network safety protocols and applications which are coded using HLPSL. HLPSL comprises of basic roles describing various candidates and configuration of characters that describe situations of essential roles. The roles are not dependent on one another, obtaining some preliminary data by parameters, interacting with other roles via channels [36]. AVISPA’s output format is accessed through one of the four back-ends, i.e., OFMC, CL-AtSe, SATMC, and TA4SP [37]. Figure 5 shows the architecture of the AVISPA tool. AVISPA is a push-

Table 2 Symbolizations utilized in the suggested scheme

Notation	Description
BS	Base station
M_{sk}	Master secret key
O	Data owner
R	Data requester
MBS	Macro base station
N_y	Nonce number
K_r, K_s	Public keys of BS and data requester
S	Credentials of user (attributes)
Rx	Packet received
Z	Attribute trust list
Sd	Packet sent
S_i, K_i	Secret and public keys to *i* users

button tool that is used to automatically authenticate network security-sensitive protocols and their implementations. It offers a formal semantic that is role-oriented and expressive for validation. Every participant plays an individual role during execution of protocol [37].

6 Validation of proposed scheme in AVISPA

The proposed technique introduced in the HLPSL codes has been validated using the AVISPA tool. This validation helps to decide whether the proposed approach is suitable for use in real scenarios.

Figure 6 shows the description of the role played by BS in HLPSL. The BS sends a nonce number (N_y) to the user that wants to communicate with it. This

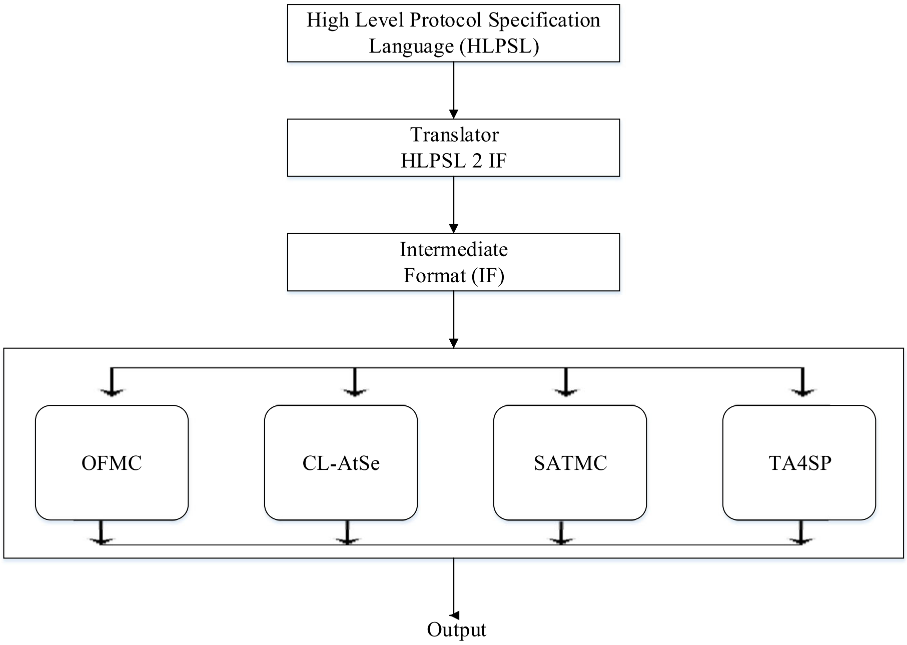
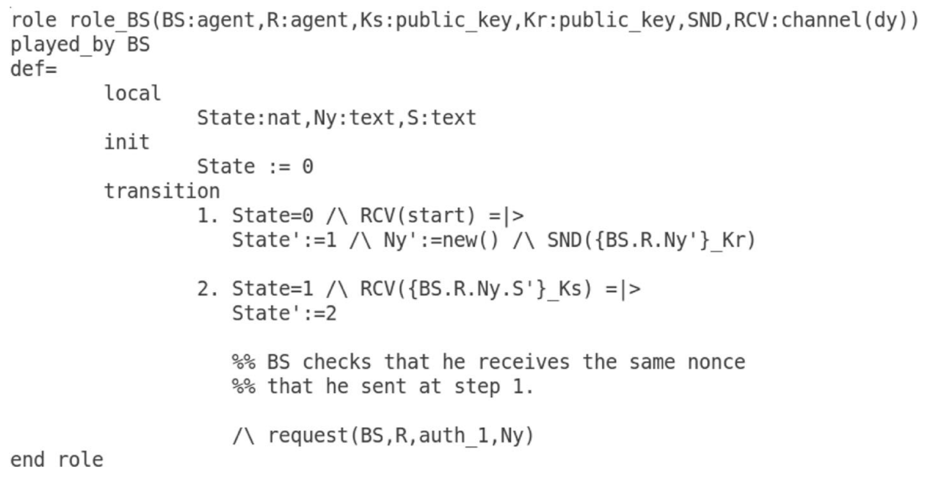


Fig. 5 AVISPA tool's architecture



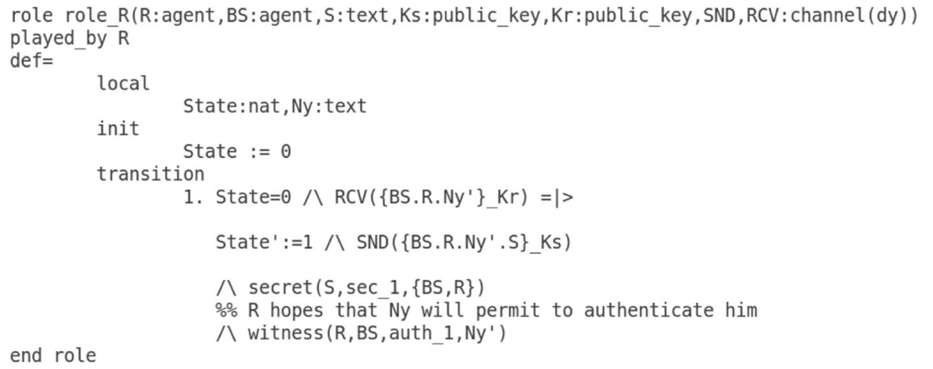
```
role role_BS(BS:agent,R:agent,Ks:public_key,Kr:public_key,SND,RCV:channel(dy))
played_by BS
def=
        local
                State:nat,Ny:text,S:text
        init
                State := 0
        transition
                1. State=0 /\ RCV(start) =|>
                   State':=1 /\ Ny':=new() /\ SND({BS.R.Ny'}_Kr)

                2. State=1 /\ RCV({BS.R.Ny.S'}_Ks) =|>
                   State':=2

                   %% BS checks that he receives the same nonce
                   %% that he sent at step 1.

                   /\ request(BS,R,auth_1,Ny)
end role
```

Fig. 6 Role description of BS for proposed scheme in HLPSL

nonce number is encrypted using the secret key of BS and public key (K_r) of that particular user (R) before transmitting it over the channel. Then the channel changes its state from 0 to 1 during this process. The channel (dy) implies that the channel is for "Dolev-Yao" threat model. Attributes are defined via variable "S". The BS hopes that it receives the same nonce number back along with attributes of R.

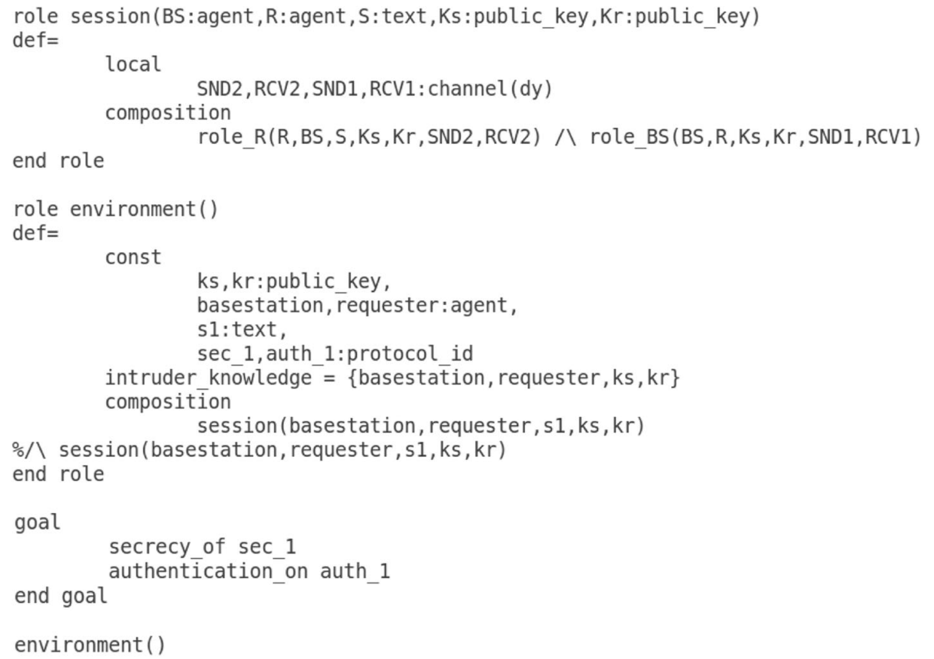
Figure 7 displays the description of role played by data requester (R) in HLPSL. The data requester accepts the message and decrypts it via the secret key of R and the public key of base stations (K_s). After decrypting the message, R sends the same nonce number back along with credentials "S" and hopes to get authenticated on these values.

Figure 8 expresses the description of role session, goal, and environment for the proposed scheme in HLPSL. Here, the session section presents the two basic roles base station (BS) and data requester (R) with valid arguments. The role environment comprises of all the global perpetual and the composition of two sessions where intruder knowledge is also given. The intruder also engages in the protocol execution. In this implementation, the following secrecy and authentication goals have been verified: (i) secrecy_of sec_1: means that the M_{sk}



```
role role_R(R:agent,BS:agent,S:text,Ks:public_key,Kr:public_key,SND,RCV:channel(dy))
played_by R
def=
        local
                State:nat,Ny:text
        init
                State := 0
        transition
                1. State=0 /\ RCV({BS.R.Ny'}_Kr) =|>

                   State':=1 /\ SND({BS.R.Ny'.S}_Ks)

                   /\ secret(S,sec_1,{BS,R})
                   %% R hopes that Ny will permit to authenticate him
                   /\ witness(R,BS,auth_1,Ny')
end role
```

Fig. 7 Role description of data requester (R) for proposed scheme in HLPSL



```
role session(BS:agent,R:agent,S:text,Ks:public_key,Kr:public_key)
def=
        local
                SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                role_R(R,BS,S,Ks,Kr,SND2,RCV2) /\ role_BS(BS,R,Ks,Kr,SND1,RCV1)
end role

role environment()
def=
        const
                ks,kr:public_key,
                basestation,requester:agent,
                s1:text,
                sec_1,auth_1:protocol_id
        intruder_knowledge = {basestation,requester,ks,kr}
        composition
                session(basestation,requester,s1,ks,kr)
%/\ session(basestation,requester,s1,ks,kr)
end role

goal
        secrecy_of sec_1
        authentication_on auth_1
end goal

environment()
```

Fig. 8 Role description of session, goal, and environment for proposed scheme in HLPSL

and SK are only known to MBS (BS). (ii) authentication_on auth_1: means that the BS has authenticated data requester (*R*) over attribute values.

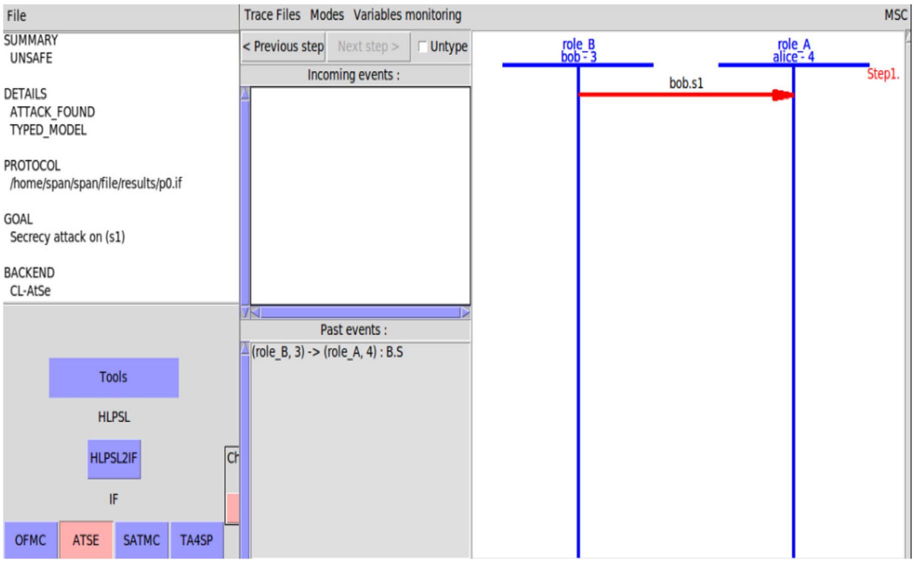
7 Results and discussion

To understand the outcome of the suggested ABE authentication scheme in a better way, three different cases have been taken: when no authentication scheme is used, authentication using single key “K_s”, and attribute-based authentication.

7.1 Case 1: when no authentication scheme is used

Figure 9 shows the protocol simulation, and Fig. 10 shows the intruder simulation when no authentication scheme is used. Here, Bob wants to communicate with Alice over the public channel without encrypting the data. This data is at the highest risk of being attacked by an intruder as the message is sent in plain-text. The intruder can easily receive all the data sent from Bob to Alice, and hence, intruders can modify the data. When this malicious data is received by Alice, it assumes that it is being sent by Bob, which is not true, and in a crucial application like healthcare, it can prove hazardous. From both Figs. 9 and 10, it is apparent that when two users communicate without using any authentication scheme intruder can easily attack the data, thereby putting the information at great risk.

The simulation output under CL-AtSe back-end of this security protocol gives the “SUMMARY” if the protocol is “SAFE” or “UNSAFE” or whether the study is indeterminate. Here, this one is unsafe for this case.



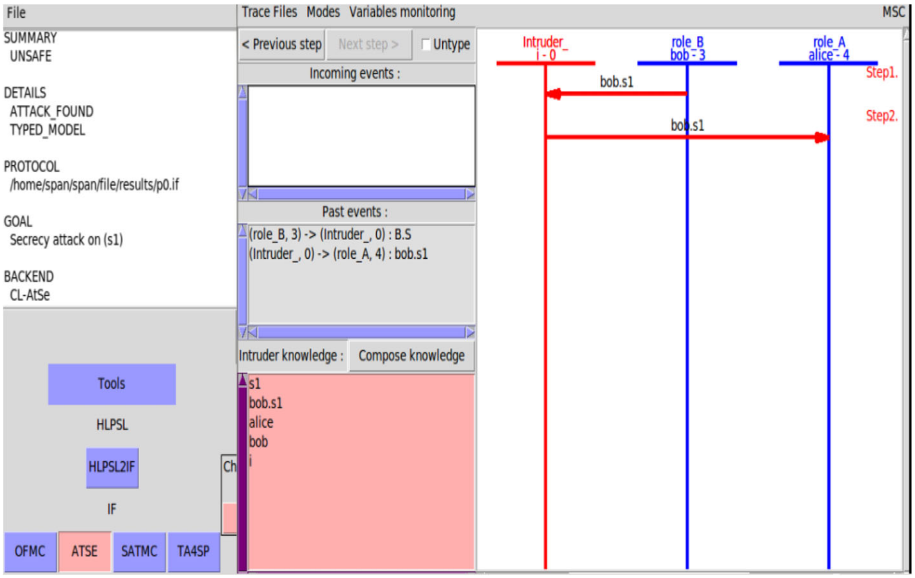
```
SUMMARY
 UNSAFE

DETAILS
 ATTACK_FOUND
 TYPED_MODEL

PROTOCOL
 /home/span/span/file/results/p0.if

GOAL
 Secrecy attack on (s1)

BACKEND
 CL-AtSe
```

Past events :
(role_B, 3) -> (role_A, 4) : B.S

Fig. 9 Protocol simulation of case 1 in AVISPA using CL-AtSe

7.2 Case 2: authentication using single key K_s

Figures 11 and 12 show the protocol and intruder simulation by using a single key, respectively. Here, the sender (data requester) first encrypts data using key "K_s" and then sends it to the receiver (base station). The same key is used by the target user to decrypt data. If somehow intruder gets the knowledge of the secret key, an intruder could easily get access to data and modify it. Exchanging the key secretly between users is the problem in this case. So this is a weak authentication technique. The simulation output under CL-AtSe back-end of this security protocol shows that this protocol is safe.

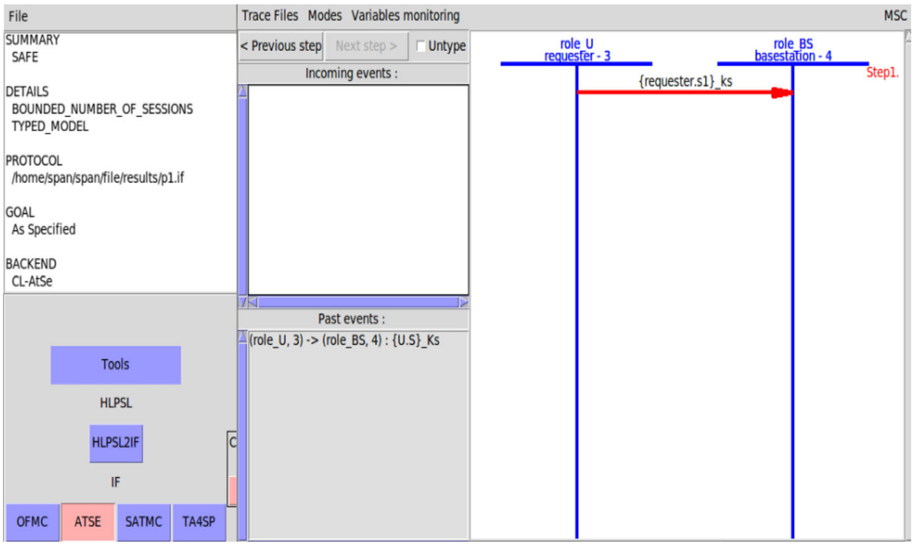


```
SUMMARY
 UNSAFE

DETAILS
 ATTACK_FOUND
 TYPED_MODEL

PROTOCOL
 /home/span/span/file/results/p0.if

GOAL
 Secrecy attack on (s1)

BACKEND
 CL-AtSe
```

Past events :
(role_B, 3) -> (Intruder_, 0) : B.S
(Intruder_, 0) -> (role_A, 4) : bob.s1

Intruder knowledge :
s1
bob.s1
alice
bob
i

Fig. 10 Intruder simulation of case 1 in AVISPA using CL-AtSe



```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/file/results/p1.if

GOAL
 As Specified

BACKEND
 CL-AtSe
```

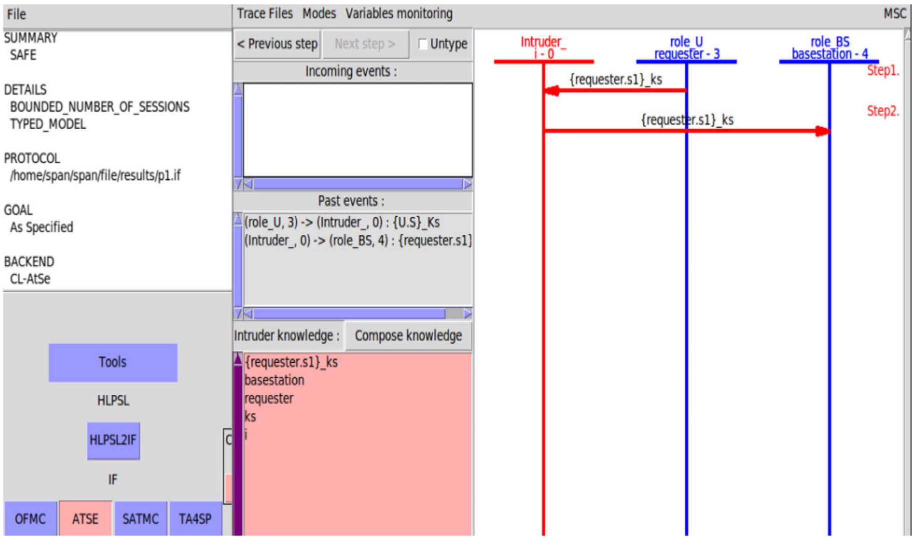
```
Past events :
(role_U, 3) -> (role_BS, 4) : {U.S}_Ks
```

Fig. 11 Protocol simulation of case 2 in AVISPA using CL-AtSe

7.3 Case 3: attribute-based authentication

Figure 13 demonstrates the protocol simulation of proposed security protocol in the AVISPA using CL-AtSe. Here, the proposed security protocol is simulated in the presence of intruders who can pose a threat to our information.

Figure 14 shows intruder simulation of proposed work in the AVISPA using CL-AtSe in the presence of the intruder. The communication process is initiated by the base station. It acts as a private key generator (PKG) and provides public and private keys to all users connected to it, with the help of master secret key (M_{sk}). During the authentication process, the base station sends a nonce number to the user (data requester) encrypted with the public key (K_R) of that particular user. These nonce numbers are random numbers and are not the same for any two users. Data requester sends back this nonce number along with credentials (S) to the BS, encrypted via the public key of

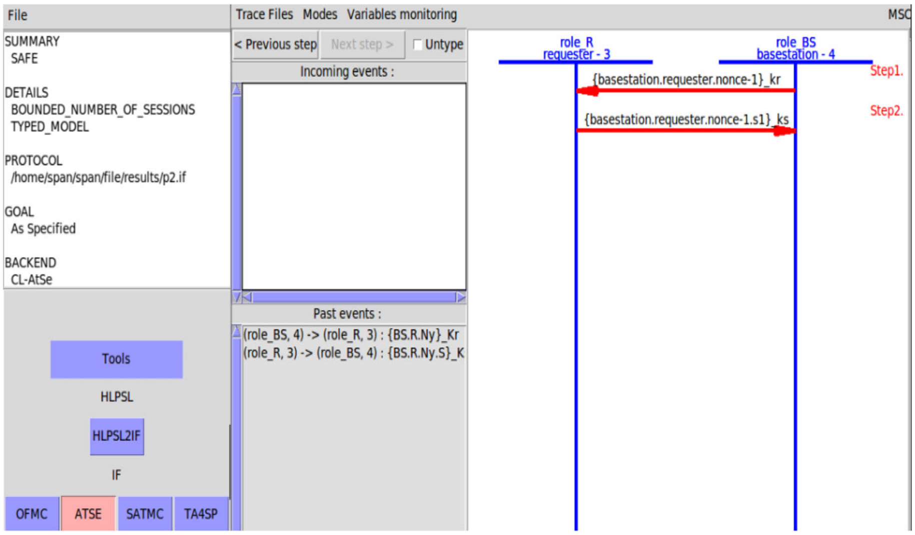


```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/file/results/p1.if

GOAL
 As Specified

BACKEND
 CL-AtSe
```

```
Past events :
(role_U, 3) -> (Intruder_, 0) : {U.S}_Ks
(Intruder_, 0) -> (role_BS, 4) : {requester.s1}
```

```
Intruder knowledge :
{requester.s1}_ks
basestation
requester
ks
i
```

Fig. 12 Intruder simulation of case 2 in AVISPA using CL-AtSe



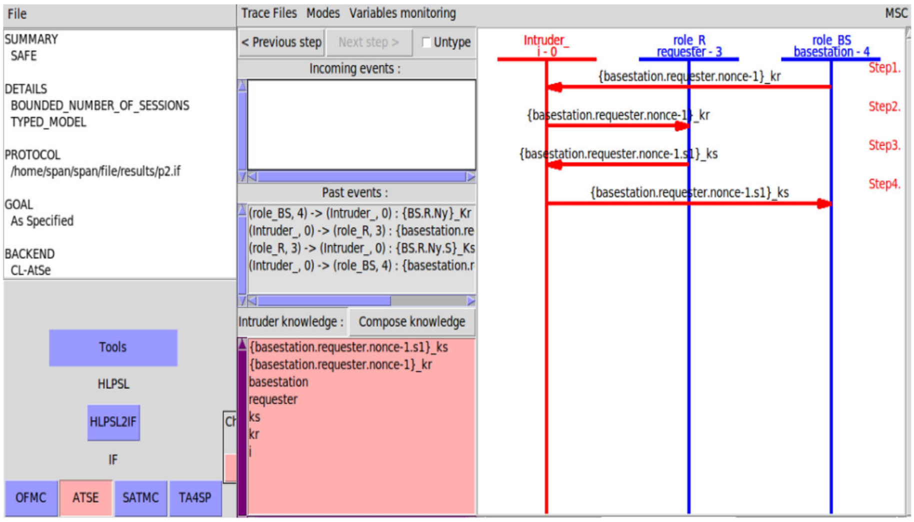
```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/file/results/p2.if

GOAL
 As Specified

BACKEND
 CL-AtSe
```

```
(role_BS, 4) -> (role_R, 3) : {BS.R.Ny}_Kr
(role_R, 3) -> (role_BS, 4) : {BS.R.Ny.S}_K
```

```
{basestation.requester.nonce-1}_kr
{basestation.requester.nonce-1.s1}_ks
```

Fig. 13 Protocol simulation of case 3 in AVISPA using CL-AtSe

BS's (K_S). If the base station acknowledges that he received the same nonce number and the credentials of the user are present in the attribute trust list, then the base station authenticates the data requester. So here nonce number also becomes one of the attributes. The intruder may attempt to attack the crucial health data, yet the attacker is unable to violate the privacy of the entire network because of the implemented authentication scheme because it becomes difficult for an intruder to guess all the attributes on which authentication takes place. In addition to this, the nonce number that acts as one of the attributes is generated at the time of communication and is extremely difficult for an intruder to guess it. Therefore, due to this, communication inside the network is safe from attacks by adversaries. Under CL-AtSe back-end, simulation performance of this security protocol gives the "SUMMARY" if the protocol is "SAFE" or "UNSAFE" or whether the study is indeterminate. Here it is safe for this case.



```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/file/results/p2.if

GOAL
 As Specified

BACKEND
 CL-AtSe
```

```
(role_BS, 4) -> (Intruder_, 0) : {BS.R.Ny}_Kr
(Intruder_, 0) -> (role_R, 3) : {basestation.re
(role_R, 3) -> (Intruder_, 0) : {BS.R.Ny.S}_Ks
(Intruder_, 0) -> (role_BS, 4) : {basestation.r
```

```
{basestation.requester.nonce-1.s1}_ks
{basestation.requester.nonce-1}_kr
basestation
requester
ks
kr
i
```

```
{basestation.requester.nonce-1}_kr
{basestation.requester.nonce-1}_kr
{basestation.requester.nonce-1.s1}_ks
{basestation.requester.nonce-1.s1}_ks
```

Fig. 14 Intruder simulation of case 3 in AVISPA using CL-AtSe

It is clear from case 1 that we need to secure the data from intruders before transmission. Our authentication scheme needs to be robust so that intruder cannot attack the data easily. As in case 2, a weak authentication scheme is used which does not provide a robust authentication against intruders. Case 3 provides an error-tolerant and robust authentication scheme with a wide dynamic range.

8 Conclusion and future scope

The research study performed in this article suggests a security protocol in HetNets to authenticate the data requesters. The HetNet employed in healthcare system must be protected against any form of malicious attack. Hence, the attribute-based authentication scheme is exploited to ensure that the user trying to access the health record of a patient is genuine. It contains characteristics like efficient key management, error tolerance, privacy preservation, emergency data storage and retrieval, and health data mining suitability. It offers authentication in which patients authenticate and store their own health data on the third-party server without any threat. Thus, by preventing the transfer of information to the attacker, we are not only satisfying the authentication requirements but also increasing the privacy of the data. Furthermore, it can also be used in other sensitive fields such as military surveillance and so on to enhance security. The suggested security protocol is written in HLPSL codes and is validated in the AVISPA. The findings suggest that the recommended protocol is secured from harmful intrusion attacks, and data security and privacy is achieved in the communication system. In attribute-based authentication scheme, we only need to meet the threshold amount of attributes for authentication, unlike in identity-based authentication where we need to meet all the parameters. Hence, in future work, we need to define some essential attributes in addition to other attributes which every user will need to fulfill. In this paper, communication between the users is happening through a third-party trusted authority. If somehow this third party becomes compromised, then the whole of the data becomes vulnerable to the malicious attacks. Therefore, in the future, some more can be done on making the third party more secure.

Abbreviations

HetNet: Heterogeneous network; HLPSL: High-level protocol specification language; AVISPA: Automated validation of Internet security protocols and applications; SWIPT: Simultaneous wireless information and power transfer; IoT: Internet of things; SDN: Software-defined networking; MIMO: Multi-input multi-output; SCI: Secure context information; BS: Base station; BSN: Body sensor network; MBS: Macro-base station; DoS: Denial of service; SLS: Symbol-level scheme; BLS: Bit-level scheme; PLS: Physical layer security; VANET: Vehicular ad hoc network; IBE: Identity-based encryption; ABE: Attribute-based encryption; CP-ABE: Cipher-text policy attribute-based encryption; KP-ABE: Key policy attribute-based encryption; OF: Output format OF; OFMC: On-the-fly model-checker; SATMC: SAT-based model-checker; CL-AtSe: Constraint logic-based attack searcher; TA4SP: Tree Automata based on Automatic Approximations for the Analysis of Security Protocols; F3TM: Flooding factor-based framework for trust management; MGF: Moment generating functions; RIS: Reconfigurable intelligent surface; ID-AODV: Interruption detection system for Ad hoc on-demand distance vector; FSM: Finite state machine; UWSN: Underwater wireless sensor network; RE-PBR: Reliable and energy-efficient pressure-based routing; MANET: Mobile ad hoc network; PKG: Private key generator; M_{sk}: Master secret key

Authors' contributions

Tufail A. Lone, Sumeet Gupta, and Sachin Kumar Gupta are the main authors of the current paper. They contributed to the development of the ideas, design of the study, theory, result analysis, and paper writing. Aabid Rashid contributed to the result analysis and paper revision. All authors read and approved the final manuscript.

Funding

Not applicable.

Availability of data and materials

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]School of Electronics & Communication Engineering, Shri Mata Vaishno Devi University, Kakryal, Katra (J&K) 182320, India. [2]Department of Electronics & Communication Engineering, JNTUH College of Engineering Hyderabad, Hyderabad, Telangana 500085, India. [3]Department of Electrical and Electronic Engineering, College of Engineering, University of Jeddah, Jeddah 21589, Saudi Arabia. [4]Systems Engineering, Department of Electrical Engineering, IIT (BHU), Varanasi, UP 221005, India. [5]Department of Computer Science, Banaras Hindu University, Varanasi, UP 221005, India. [6]Department of Computer Science and Engineering, Feroze Gandhi Institute of Engineering and Technology, Raebareli, UP 229316, India.

Received: 15 January 2020 Accepted: 6 July 2020
Published online: 14 July 2020

References

1. K.N. Qureshi, A.H. Abdullah, O. Kaiwartya, S. Iqbal, R.A. Butt, F. Bashir, A dynamic congestion control scheme for safety applications in vehicular ad hoc networks. J. Comput. Electr. Eng. **72**, 774–788 (2018)
2. X. Hu, B. Li, K. Huang, Z. Fei, K.K. Wong, Secrecy energy efficiency in wireless powered heterogeneous networks: a distributed ADMM approach. IEEE Access **6**, 20609–20624 (2018)
3. M. Forouzesh, P. Azmi, N. Mokari, K.K. Wong, H.P. Nik, Robust physical layer security for power domain non-orthogonal multiple access-based HetNets and HUDNs: SIC avoidance at eavesdroppers. IEEE Access **7**, 107879–107896 (2019). https://doi.org/10.1109/ACCESS.2019.2932805
4. J. Cao, M. Ma, Y. Fu, H. Li, Y. Zhang, in *IEEE transactions on dependable and secure computing*. CPPHA: capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets (2019), pp. 1–13. https://doi.org/10.1109/TDSC.2019.2916593
5. X. Duan, X. Wang, Authentication handover and privacy protection in 5G HetNets using software-defined networking. IEEE Commun. Mag. **53**(4), 28–35 (2015)
6. J. Xu, L. Liu, R. Zhang, Multiuser MISO beam forming for simultaneous wireless information and power transfer. IEEE Trans. Signal Process. **62**(18), 4798–4810 (2014)
7. Y.C. Wang, S. Lee, Small-cell planning in LTE HetNet to improve energy efficiency. Int. J. Commun. Syst. **31**(5), e3492 (2018). https://doi.org/10.1002/dac.3492 Wiley
8. Y. Deng, L. Wang, K.K. Wong, A. Nallanathan, M. Elkashlanz, S. Lambotharan, in *International Conference on Wireless Communications & Signal Processing (WCSP), Nanjing*. Safeguarding massive MIMO aided HetNets using physical layer security (2015), pp. 1–5. https://doi.org/10.1109/WCSP.2015.7341120
9. W. Zhao, Z. Chen, K. Li, N. Liu, B. Xia, L. Luo, Caching-aided physical layer security in wireless cache-enabled heterogeneous networks. IEEE Access **6**, 68920–68931 (2018). https://doi.org/10.1109/ACCESS.2018.2880339
10. G. Shiqi, X. Chengwen, F. Zesong, K. Jingming, Resource allocation for physical layer security in heterogeneous network with hidden eavesdropper. China Commun. **13**(3), 82–95 (2016)
11. X. Duan, X. Wang, in *IEEE International Conference on Communication (ICC), Kuala Lumpur*. Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer (2016), pp. 1–6. https://doi.org/10.1109/ICC.2016.7510994
12. J. Richter, E. Franzy, S. Engelmann, S. Pfennigy, E.A. Jorswieck, in *IEEE 18th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), Berlin*. Physical layer security vs. network layer secrecy: who wins on the untrusted two-way relay channel? (2013), pp. 164–168. https://doi.org/10.1109/CAMAD.2013.6708110
13. Sudarsono, A., Yuliana, M., Darwito, H. A.: A secure data sharing using identity-based encryption scheme for e-healthcare system. 3rd International Conference on Science in Information Technology, (ICSITech), IEEE, Bandung, 429-434, 2017, doi: https://doi.org/10.1109/ICSITech.2017.8257151
14. C.C. Tan, H. Wang, S. Zhong, Q. Li, IBE-Lite: a lightweight identity-based cryptography for body sensor networks. IEEE Trans. Inf. Technol. Biomed. **13**(6), 926–932 (2009). https://doi.org/10.1109/TITB.2009.2033055
15. J. Bethencourt, A. Sahai, B. Waters, in *IEEE Symposium on Security and Privacy, Berkeley, CA*. Ciphertext-policy attribute-based encryption (2007), pp. 321–334. https://doi.org/10.1109/SP.2007
16. M.H. Raju, M.U. Ahmed, M.A.R. Ahad, in *A Handbook of Internet of Things in Biomedical and Cyber Physical System, Chapter 3*. Security analysis and a potential layer to layer security solution of medical cyber-physical systems (2019), pp. 61–86
17. M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parall. Distr. Syst. **24**(1), 131–143 (2012)
18. H. Qian, J. Li, Y. Zhang, J. Han, Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. Int. J. Inf. Secur. **14**, 487–497 (2015). https://doi.org/10.1007/s10207-014-0270-9
19. A. Sahai, B. Waters, in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Fuzzy identity-based encryption, vol 3494 (Springer, 2005), pp. 457–473. https://doi.org/10.1007/11426639_27
20. A. Monika, M. Pradeep, A comparative survey on symmetric key encryption techniques. Int. J. Comp. Sci. Eng. **4**(5), 877 (2012)
21. M.N. Ahmed, A.H. Abdullah, H. Chizari, O. Kaiwartya, F3TM: flooding factor based trust management framework for secure data transmission in MANETs. J. King Saud Univ. Comp. Inf. Sci. **29**(3), 269–280 (2017)
22. A.U. Makarfi, R. Kharel, K.M. Rabie, O. Kaiwartya, G. Nauryzbayev, in *IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA*. Physical layer security in vehicular communication networks in the presence of interference (2019), pp. 1–6. https://doi.org/10.1109/GLOBECOM38437.2019.9013138
23. Fang, D., Qian, Y., Hu, R. Q.: Interference management for physical layer security in heterogeneous networks. 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and

Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, 133-138, 2017.

24. W. Wang, K.C. Teh, S. Luo, K.H. Li, Physical layer security in heterogeneous networks with pilot attack: a stochastic geometry approach. IEEE Trans. Commun. **66**(12), 6437–6449 (2018)
25. Makarfi, A. U., Rabie, K. M., Kaiwartya, O., Li, X., Kharel, R.: Physical layer security in vehicular networks with reconfigurable intelligent surfaces. arXiv preprint arXiv:1912.12183, 2019.
26. L.Y. Yeh, Y.C. Chen, J.L. Huang, ABACS: an attribute-based access control system for emergency services over vehicular ad hoc networks. IEEE J. Sel. Area Commun. **29**(3), 630–642 (2011). https://doi.org/10.1109/JSAC.2011.110312
27. M. Bouabdellah, F. Bouanani, H. Benazza, in *International Conference on Advanced Communication Systems and Information Security (ACOSIS), Marrakesh*. A secure cooperative transmission model in VANET using attribute based encryption (2016), pp. 1–6. https://doi.org/10.1109/ACOSIS.2016.7843940
28. L. Nkenyereye, Y. Park, K.H. Rhee, A secure billing protocol over attribute-based encryption in vehicular cloud computing. EURASIP J. Wirel. Commun. Netw., 196 (2016). https://doi.org/10.1186/s13638-016-0687-0
29. M.N. Ahmed, A.H. Abdullah, O. Kaiwartya, FSM-F: finite state machine based framework for denial of service and intrusion detection in MANET. PLoS One **11**(6) (2016). https://doi.org/10.1371/journal.pone.0156885
30. Y.L. Tan, B.M. Goi, R. Komiya, S.Y. Tan, in *International Conference on Informatics Engineering and Information Science, Communications in Computer and Information Science*. A study of attribute-based encryption for body sensor networks, vol 251 (Springer, 2011), pp. 238–247. https://doi.org/10.1007/978-3-642-25327-0_21
31. N. Oualha, K.T. Nguyen, in *25th International Conference on Computer Communication and Networks, (ICCCN), Waikoloa, HI*. Lightweight attribute-based encryption for the internet of things (2016), pp. 1–6. https://doi.org/10.1109/ICCCN.2016.7568538
32. A. Khasawneh, M.S.B.A. Latiff, O. Kaiwartya, H. Chizari, A reliable energy-efficient pressure-based routing protocol for underwater wireless sensor network. Wirel. Netw. **24**(6), 2061–2075 (2018). https://doi.org/10.1007/s11276-017-1461-x
33. H. Javdani, H. Kashanian, Internet of things in medical applications with a service-oriented and security approach: a survey. Health Technol. **8**(1-2), 39–50 (2018). https://doi.org/10.1007/s12553-017-0180-8 IUPESM and Springer-Verlag Berlin Heidelberg
34. K. Abouelmehdi, A.B. Hessane, H. Khaloufi, Big healthcare data: preserving security and privacy. J. Big Data **5**(6) (2018). https://doi.org/10.1186/s40537-017-0110-7
35. W. Hou, X. Wang, J.Y. Chouinard, A. Refaey, Physical layer authentication for mobile systems with time-varying carrier frequency offsets. IEEE Trans. Commun. **62**(5), 1658–1667 (2014)
36. AVISPA. Automated validation of internet security protocols and applications. < http://www.avispa-project.org/. Accessed Nov 2015.
37. AVISPA. AVISPA web tool. http://www.avispa-project.org/webinterface/expert.php/. Accessed Nov 2015.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.