Bulletin of the Iranian Mathematical Society (2018) 44:1243–1265
https://doi.org/10.1007/s41980-018-0087-9

ORIGINAL PAPER

An Omniscience-Free Temporal Logic of Knowledge for Verifying Authentication Protocols

S. Ahmadi[1] · **M. S. Fallah**[1]

Received: 5 June 2017 / Accepted: 29 November 2017 / Published online: 21 June 2018

Abstract
Since the advent of BAN logic, many logics have been proposed for verifying authentication protocols. In one line of research, scholars have presented logics that can be utilized in verifying timed requirements of the protocols. Although many temporal epistemic logics have been developed to this end, there is no complete logic of this kind to prevent logical omniscience. Thus, they may lead to misleading judgments about the properties of the protocol being analyzed. In this paper, we propose a complete and omniscience-free temporal epistemic logic for analyzing authentication protocols. The main challenging issue in devising this logic is formulating intuitive models that on one hand reflect what is naturally meant by a protocol execution and on the other hand make it possible to achieve properties such as completeness. We show that such models can build on interpreted systems and that the resulting logic is useful in analyzing authentication protocols.

Keywords Formal verification · Authentication protocols · Temporal epistemic logics · Logical omniscience

Mathematics Subject Classification Primary 68Q60; Secondary 03B70

1 Introduction

Different deductive systems have been devised for the verification of authentication protocols. In particular, since the introduction of the modal logic BAN [9], many

Communicated by Ali Enayat.

✉ M. S. Fallah
msfallah@aut.ac.ir

S. Ahmadi
sharar.ahmadi@aut.ac.ir

[1] Department of Computer Engineering and Information Technology, Amirkabir University of Technology, Tehran, Iran

epistemic logics have been proposed for this purpose [2,5,6,13,14,18,22,24,33,36,37]. The rationale behind using such logics is that the knowledge of the agents involved in the protocol changes as messages are exchanged during the protocol execution. The sole modality of knowledge, however, is not enough for the analysis of protocols in which the order of actions taken by the principals may result in different beliefs, especially when there is an interaction between time and knowledge [4]. To attain an effective verification method for such protocols, a natural solution is to add a temporal dimension to a core epistemic logic. The need for proving properties of specific steps of an authentication protocol amplifies the necessity of temporal operators. This has been a research topic in the past two decades [4,6–8,10,19,25,28,29,31,32,34].

At the same time, epistemic logics with standard Kripke semantics result in *omniscience* where agents know all logical truths [21]. Verifying authentication protocols using such logics may lead to wrong judgments. In actual fact, the logical omniscience bypasses the limitations placed on the knowledge of an agent who receives an encrypted message but does not have the correct key to extract the plain information from that message.

There are some attempts at resolving the problem of logical omniscience in the epistemic logics proposed for the specification and verification of cryptographic protocols. In [12], the problem is dealt within a logic where the authors modify the truth definition of the modal operator "knows". They indeed make use of specific message renaming functions to evaluate statements in the worlds accessible from a given world. This logic, which is referred to as WS5 throughout this paper, does not have any temporal operators and can be thought of as a weakened S5, hence the name. The problem of omniscience has also been tackled in [6] where the authors suggest the goals of the protocol be translated into statements so that the bad effects of omniscience can be prevented. The presented logic, however, is not omniscience-free. The logical omniscience can also be defeated using exact models of the knowledge an agent may acquire during a protocol execution [20]. Another endeavor is the so-called temporal deductive logic [25] which is a sound and complete temporal epistemic logic. Although part of the logic linking every explicit knowledge to an awareness statement is omniscience-free, the problem remains in the part involving implicit knowledge.

Having said all this, there is no complete and omniscience-free temporal epistemic logic for the verification of authentication protocols. To attain such a logic, we extend WS5 with temporal operators. The result is called Temporal WS5, or TWS5 for short. The logic TWS5 allows knowledge and time operators to appear in each other's scope. Thus, it is more powerful than logics in which temporal operators cannot be located in the scope of knowledge operators [31]. Moreover, similar to some other works, e.g., [19,25,32], TWS5 does not have any axiom connecting timed and epistemic statements. It is shown that TWS5 is useful in analyzing some authentication protocols that cannot be verified by similar logics.

The main challenging issue in developing TWS5 is finding intuitive models in such a way that completeness remains provable. Such models, at the same time, must reflect what is naturally meant by a protocol execution. We define the semantics of TWS5 in terms of validity over possible states of a Kripke model that is generated by a so-called message passing interpreted system [16]. Each possible state corresponds to a set of

$$
\begin{aligned}
&\mathbf{P_{00}}: \quad R \to S : n_r \\
&\mathbf{P_{01}}: \quad S \to R : \{f(k_1).n_r\}_{pr_s} \\
&\mathbf{P_1}: \quad S \to R : \{m_1\}_{k_s}.f(k_2).mac\big(g(k_1), \{m_1\}_{k_s}.f(k_2)\big) \\
&\mathbf{P_2}: \quad S \to R : \{m_2\}_{k_s}.f(k_3).k_1.mac\big(g(k_2), \{m_2\}_{k_s}.f(k_3).k_1\big) \\
&\mathbf{P_3}: \quad S \to R : \{m_3\}_{k_s}.f(k_4).k_2.mac\big(g(k_3), \{m_3\}_{k_s}.f(k_4).k_2\big) \\
&\vdots \\
&\mathbf{P_{i-1}}: \quad S \to R : \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac\big(g(k_{i-1}), \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}\big) \\
&\mathbf{P_i}: \quad S \to R : \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i), \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big) \\
&\mathbf{P_{i+1}}: \quad S \to R : \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big) \\
&\vdots
\end{aligned}
$$

Fig. 1 A variant of the stream authentication protocol TESLA

messages sent or received by agents involved in an execution of the protocol up to a particular time. We prove that TWS5 is complete.

Although there are many dynamic epistemic logics used for modeling knowledge protocols, we do not investigate them in this paper because they are inconvenient in a cryptographic setting for generating equivalence relations among messages [15,38]. The rest of this paper is organized as follows: In Sect. 2, we present a motivating example that justifies why an effective logic for verifying authentication protocols should be temporal and omniscience-free. Section 3 is an overview of an omniscience-free epistemic logic which we call it WS5. In Sect. 4, we propose the syntax and semantics of our logic TWS5. The proof of completeness is given in Sect. 5. In Sect. 6, we show that TWS5 is useful in verifying authentication protocols. Section 7 concludes the paper.

2 Motivating Example

We give an example to show why an effective epistemic logic for verifying authentication protocols must have temporal operators and be omniscience-free. Our example is the protocol in Fig. 1. It is a variant of the stream authentication protocol TESLA [35]. Using this protocol, the sender S sends a stream of messages he has encrypted by his secret key k_s to the receiver R. The protocol is intended to preserve the authenticity of the source and messages.

In this protocol n_r is a nonce generated by R and the packet P_i is of the form

$$\{m_i\}_{k_s} \cdot f(k_{i+1}) \cdot k_{i-1} \cdot \mathrm{mac}\big(g(k_i), \quad \{m_i\}_{k_s} \cdot f(k_{i+1}).k_{i-1}\big)$$

for $i = 2, 3, \ldots$ where f and g are two one-way functions known to everyone, k_{i+1} is the fresh key S has chosen in the ith step of the protocol, and "mac" is a message authentication code used in the verification of messages sent through packets.

The message authentication code has two inputs separated by a camma notation. To authenticate $\{m_i\}_{k_s}$, R must wait for the next packet P_{i+1}. By receiving P_{i+1}, R extracts k_i and computes $f(k_i)$ and compares it with the commitment, i.e., $f(k_i)$, sent in packet P_{i-1}. If the two values are equal, R concludes that k_i is safe. Then, R computes $\mathrm{mac}\big(g(k_i), \{m_i\}_{k_s} \cdot f(k_{i+1}) \cdot k_{i-1}\big)$ and verifies the authenticity of $\{m_i\}_{k_s}$. The authenticity of the source of P_i is inductively established on the basis of the belief formed when R receives P_{01} carrying his own nonce n_r encrypted by the source's private key pr_s. This protocol can be used in outsourced databases whenever the receiver who keeps the sender's encrypted records in his database asks the sender to update the records or create new ones.

Stream authentication protocols may operate in different modes [34]. An operation mode is defined to be a pair $([u, v], d)$ where $u, v, d \in \mathbb{N}$ and $d \neq 0$. If the protocol operates in this mode, the arrival time of every packet sent at time t can be at an instant in $[t+u, t+v]$. If the packet is received outside this time interval it is not accepted as a valid packet—the clocks of the sender and the receiver are synchronized. Moreover, the time distance between the transmission of two consecutive packets is d. If $v \geq d$, the protocol in Fig. 1 may be vulnerable to attack and fail in providing authentication requirements. In fact, S may consecutively send two packets which are intercepted by the adversary C. The adversary then forges the first packet by the information he obtains from the second one and sends the resulting packets to R. If the time taken by the attacker to alter and send packets to R is small enough, R will accept the packets. In this way, R is deceived into accepting ungenuine packets. Indeed, the so-called agreement [27] may not be established between S and R. The following describes an example attack which exploits this vulnerability.

Let $C(S)$ and $C(R)$ stand for a principal C impersonating S and R and k_c be C's secret key. An execution is considered to be a sequence of messages sent or received by a principal. Assume that there are at least two executions h_1 and h_2 of this protocol shown in Fig. 2 and where we use snd and rcv to represent sending and receiving a message by a principal in a model, i.e., a semantic notation, and snt and rcvd are used as the syntactic representation of the same. As seen in h_2, principal C is an adversary that intercepts P_i and P_{i+1}. It infers k_i from P_{i+1} and uses this key to change the packet P_i in which $\{m_i\}_{k_s}$ is replaced by $\{m_i'\}_{k_c}$. After changing P_i, C impersonates S and sends the forged packet along with the original packet P_{i+1}, in order, to R. This attack is possible in the mode of operation $([1, 4], 2)$, for example. The sender sends P_i and P_{i+1} at t and $t+2$. The attacker receives these two packets at $t+1$ and $t+3$. If the packets the attacker sends to the receiver are received at $t+4$ and $t+6$, they are accepted by the receiver since they are received in time intervals $[t+1, t+4]$ and $[t+3, t+6]$ as expected. Thus, the protocol is vulnerable to the attack.

Suppose that we want to investigate whether the run of the protocol in Fig. 1 between S and R can assure R that the ith packet received has certainly been sent by S. This requirement may be specified in an epistemic logic by a formula like R knows S snt P_i. Now, assume that we employ an epistemic logic to verify this protocol against the property specified above, but the logic is not omniscience-free. In such a logic, A knows ϕ is true in a possible world w whenever ϕ is true in every world reachable from w. Such an interpretation of truth leads to omniscience. Moreover, assume that h_1 and h_2 in Fig. 2 are two possible worlds in the model of

$\mathbf{h_1}$:

$$\vdots$$

$$S\ snd\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac\big(g(k_{i-1}),\{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}\big),$$
$$R\ rcv\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac\big(g(k_{i-1}),\{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}\big),$$
$$S\ snd\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i),\{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big),$$
$$R\ rcv\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i),\{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big),$$
$$S\ snd\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}),\{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$$
$$R\ rcv\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}),\{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$$

$$\vdots$$

$\mathbf{h_2}$:

$$\vdots$$

$$S\ snd\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac\big(g(k_{i-1}),\{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}\big),$$
$$R\ rcv\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac\big(g(k_{i-1}),\{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}\big),$$
$$S\ snd\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i),\{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big),$$
$$C(R)\ rcv\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i),\{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big),$$
$$S\ snd\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}),\{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$$
$$C(R)\ rcv\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}),\{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$$
$$C(S)\ snd\ \{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i),\{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1}\big),$$
$$R\ rcv\ \{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i).\{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1}\big),$$
$$C(S)\ snd\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}),\{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$$
$$R\ rcv\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}),\{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$$

$$\vdots$$

Fig. 2 Executions h_1 and h_2 of the protocol shown in Fig. 1

the protocol. Thus, to show that the formula is true in h_1, we should verify S snt P_i in every execution being indistinguishable from h_1 in R's view. Since R does not know k_s and k_c, he cannot distinguish between $\{m_i\}_{k_s}$ and $\{m'_i\}_{k_c}$, and consequently, h_1 is indistinguishable from h_2 in his view. As S snt P_i holds in h_2, these two possible worlds, i.e., h_1 and h_2, are not enough to refute the above property. At the same time, h_2 indicates an attack and is reasonable to take part in a counterexample for the property.

If we use an omniscience-free epistemic logic such as WS5 [11], then h_2 is enough to refute the property. In fact, WS5 requires a modified set of statements to be true in the worlds accessible from the world the truth of a given modal formula is being investigated. Recall that the possible worlds h_1 and h_2 are indistinguishable in R's

$$\mathbf{S_1} : A\ snt\ X \rightarrow (next^u\ B\ rcvd\ X) \vee \ldots \vee (next^v B\ rcvd\ X)$$
$$\mathbf{S_2} : next^0\ S\ snt\ \{f(k_1), n_r\}_{pr_s}$$
$$\mathbf{S_3} : next^d\ S\ snt\ \{m_1\}_{k_s}.f(k_2).mac\big(g(k_1), \{m_1\}_{k_s}.f(k_2)\big)$$
$$\mathbf{S_4} : next^{i\cdot d}\ S\ snt\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i), \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big) \quad (i \geq 2)$$
$$\mathbf{S_5} : S\ snt\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac(g(k_i), \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}) \leftrightarrow next^d\ S\ snt\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big) \quad (i \geq 2)$$

Fig. 3 The specification of the protocol shown in Fig. 1 using epistemic and temporal operators

view because he cannot differentiate between $\{m_i\}_{k_s}$ and $\{m'_i\}_{k_c}$. Now, consider the renaming function ρ that maps the message $\{m_i\}_{k_s}$ to $\{m'_i\}_{k_c}$ and keeps the other messages intact. The modified formula that must hold in h_2 is then

$$S\ \text{snt}\ \rho\big(\{m_i\}_{k_s}\big).f(k_{i+1}) \cdot k_{i-1} \cdot \text{mac}\big(g(k_i), \rho\big(\{m_i\}_{k_s}\big) \cdot f(k_{i+1}).k_{i-1}\big)$$

which is equal to

$$S\ \text{snt}\ \{m'_i\}_{k_c} \cdot f(k_{i+1}) \cdot k_{i-1} \cdot \text{mac}\big(g(k_i), \{m'_i\}_{k_c} \cdot f(k_{i+1}) \cdot k_{i-1}\big).$$

As this formula is not true in h_2, the property is refuted.

The receiver may receive the ith packet sent at time t at most v clock ticks later. As stated above, the security of the protocol depends on its mode of operation. Thus, an appropriate logic for the specification of the protocol and requirements should additionally have temporal operators like next and its derived form next^t representing the next clock tick and t clock ticks later, respectively. In Fig. 3, S_1 is an axiom scheme in which A and B can be any principal including the sender S, the receiver R, and an intruder C. Moreover, X can be a packet sent by a principal. For example, the consecutive packets sent and received in h_1 and h_2 (Fig. 2) can be represented as appropriate instances of S_1. The axiom scheme S5 represents the fact that the key k_i that is used in $g(k_i)$ of the ith packet is disclosed d time units later. The following formalizes the authentication requirement for the packet P_i with $i \geq 1$ as a modal formula using epistemic and temporal operators.

$$\text{next}^{(i+1)d+v}\ R\ \text{knows}\ S\ \text{snt}\ P_i.$$

3 WS5: An Omniscience-Free Epistemic Logic

The logic proposed in this paper builds on an epistemic logic for verifying authentication protocols [11]. We name it WS5 since it can be thought of as a variant of S5 in which there is a weak necessitation rule. In WS5, modal operators represent the knowledge of the agents identified by the set $\mathcal{A} = \{A_1, \ldots, A_n\}$. In this logic, propositions are about messages. A message may be atomic or be constructed from two messages m and m' by pairing or encryption, denoted $m.m'$ and $\{m\}_{m'}$, respectively. The sub-message relation '$\leq$' is defined as the smallest reflexive and transitive relation

on messages satisfying $m, m' \leq \{m\}_{m'}$ and $m, m' \leq m.m'$. The converse of '$\leq$' is noted '$\geq$' as well. The set of all messages is assumed to be a finite set τ, a subset of which is the set of keys.[1]

An atomic formula is a proposition $a(m)$ in which $m \in \tau$ and a is a keyword of the set $\mathcal{P} = \{A \text{ snt}, A \text{ rcvd}, A \text{ sen}, A \text{ rec}, \text{exists}, \text{unfresh} \mid A \in \mathcal{A}\}$. Atomic formulae can be interpreted as follows:

- A snt m: A has sent m.
- A rcvd m: A has received m.
- A sen m: A has sent m' and m is a sub-message of m'.
- A rec m: A has received m' and m is a sub-message of m'.
- exists m: An agent has sent or received m' and m is a sub-message of m'.
- unfresh m: m is not fresh.[2]

There is also an auxiliary keyword infers that is interpreted as follows:

- A infers m: m is among the initial knowledge of A or it can be computed on the basis of what A knows.

For a given set of atomic formulae Ω, a formula of the logic is defined inductively as follows:

- Every $p \in \Omega$ is a formula.
- If ϕ and ψ are formulae, then so are $\neg\phi$ and $\phi \rightarrow \psi$.
- If ϕ is a formula, then $K_i\phi$ is a formula for every $1 \leq i \leq n$, where the intended meaning of $K_i\ \phi$ is "Agent A_i knows ϕ."

The model of a protocol represents the set of all possible executions of that protocol. An execution can also be interpreted as a set of interactions between agents through the steps defined in the protocol. By such an interpretation, a protocol execution may comprise several interleaving runs of the protocol. In every possible execution of a protocol, agents in $\mathcal{A}$ interact with each other through the actions they take on messages and the knowledge of an agent is characterized by a finite set of atomic formulae which is called the local state for that agent. Each execution of a protocol is then represented by a global state which is the union of agents' local states. In the view of an agent, there may be a set of conceivable global states, as it does not know the local states of the others. This makes a basis for the access relation in the standard Kripke semantics. In this way, the set of all possible global states would be the set of possible worlds, W, of a Kripke model. In this model, there are also n equivalence relations $\{\sim_i\}_{1\leq i\leq n}$ on W. If two global states are in the same class induced by $\sim_i$, then they are indistinguishable in A_i's view in the sense that A_i has equal local states in the two global states. Notice that the idea of using an indistinguishability relation for modeling what an agent sees from a protocol execution has been applied in earlier works, e.g., [1,2,17].

A model also includes an interpretation function π from Ω to 2^W, where $\pi(p) = W' \subseteq W$ means that p holds in every possible world $w \in W'$. Thus, a model is a triple

[1] For technical reasons, we need to force τ to be finite using a finite set of atomic messages and restricting the number of interleaving concatenations and encryptions.

[2] A message is fresh if it has not been sent in any message previously [9]. If a message is unfresh, it is subject to replay attacks.

$\langle W, \{\sim_i\}, \pi\rangle$. As inspired by the motivating example, however, this model may lead to invalid judgments about protocols. In what follows, it is seen that the problem can be resolved by a modified interpretation of accessibility relation and truth definition.

In epistemic logics for cryptographic properties, encrypted parts in the scope of a modal operator are interpreted under *de re* interpretation [11]. Consider the statement $K_i\ A_i$ rcvd $\{m\}_k$ which states that A_i knows that he has received $\{m\}_k$. Under *de re* interpretation, A_i knows that he has received the message m encrypted by k as if he has an unlimited decryption power. Such a decryption power may cause logical omniscience. That is, if $\phi \rightarrow \phi'$ is a valid formula, then so is $K_i\phi \rightarrow K_i\phi'$. For example, the formula A_i rcvd $\{m\}_k \rightarrow$ exists m holds for every agent A_i, whereas $K_i\ A_i$ rcvd $\{m\}_k \rightarrow K_i$ exists m may not be true. In fact, the latter is true only if A_i knows the key k so that it can use this key to compute m. Therefore, logical omniscience may contradict resource-bounded knowledge and it may result in formulae that are not indeed valid.

To avid omniscience, the access relation in an agent's view is tagged with a message renaming function $\rho : \tau \rightarrow \tau$. The following concepts are required for defining the modified access relation. Note that although ρ is considered as an operation on messages, it can also be applied to statements. In doing so, it is applied to the messages in the given statement. The application of ρ to messages, however, is subject to the messages ρ is consistent with.

Definition 3.1 A message renaming function $\rho : \tau \rightarrow \tau$ is defined to be consistent with a set $\kappa \subseteq \tau$, written $\rho \lhd \kappa$, iff the following conditions are satisfied.

- $\rho(c) = c$ for any atomic message c.
- $\rho(\{m\}_k) = \{\rho(m)\}_{\rho(k)}$ for every $k \in \kappa$.
- $\rho(m.m') = \rho(m).\rho(m')$.

As agents can distinguish atomic (constant) messages, any consistent message renaming function maps an atomic message to itself. It is also worth noting that message renaming functions are total functions. As an example, assume that A_i infers a set of keys κ and $\rho \lhd \kappa$. If $k \in \kappa$, $\rho(\{m\}_k)$ is equal to $\{\rho(m)\}_{\rho(k)}$ in A_i's view. A_i can indeed expand ρ through the encrypted message because he infers the right decryption key k. If $k \notin \kappa$, A_i may just see $\rho(\{m\}_k)$, which is a message in the form of an atomic or an encrypted message or even the concatenation of two messages.

A WS5 model $\mathcal{M}$ is then defined to be a triple $\langle W, \{\rightsquigarrow_i^\rho\}, \pi\rangle$ in which W is the set of all possible executions of a protocol and π is the interpretation function. Moreover, when we say that the global state $s \in W$ has access to the global state $t \in W$ in A_i's view with respect to ρ, denoted by $s \rightsquigarrow_i^\rho t$, it means that the application of ρ to the local state of A_i in s is equal to its local state in t and ρ is consistent with the keys A_i infers from s. It is proven that if the global state s has access to the global state t in A_i's view with respect to ρ, then t has access to s in A_i's view with respect to ρ^{-1} [12]. Therefore, we use the notation $\rightsquigarrow_i^\rho$ to indicate that this relation is not symmetric.

The truth of a formula in a world w of a given model $\mathcal{M}$ can then be inductively defined. Figure 4 gives the definition. A formula ϕ is said to be valid, denoted by $\models \phi$, if $(\mathcal{M}, w) \models \phi$ holds for every model $\mathcal{M}$ and every possible world w of $\mathcal{M}$. A formula ϕ is satisfiable if there exists a model $\mathcal{M}$ and a possible world w of $\mathcal{M}$ such that $(\mathcal{M}, w) \models \phi$.

- $(\mathcal{M}, w) \models a(m)$ for any $a(m) \in \Omega$ iff $w \in \pi(a(m))$.
- $(\mathcal{M}, w) \models \neg\phi$ iff $(\mathcal{M}, w) \not\models \phi$.
- $(\mathcal{M}, w) \models \phi \to \psi$ iff $(\mathcal{M}, w) \models \phi$ implies $(\mathcal{M}, w) \models \psi$.
- $(\mathcal{M}, w) \models K_i\phi$ iff for all message renaming functions $\rho : \tau \to \tau$ and all $w' \in W$, if $w \rightsquigarrow_i^{\rho} w'$, then $(\mathcal{M}, w') \models \rho(\phi)$.

Fig. 4 Truth definition in WS5

All axioms of classical propositional logic.

$$\textbf{MP}: \ \frac{\phi,\ \phi \to \psi}{\psi}$$

$$\textbf{Nec}: \ \frac{\rho(\phi), \quad \forall \rho \lhd \kappa}{A_i\ infers\ \kappa \to K_i\phi}$$

$$\textbf{K}: \ K_i(\phi \to \phi') \to (K_i\phi \to K_i\phi')$$

$$\textbf{T}: \ K_i\phi \to \phi$$

$$\textbf{4}: \ K_i\phi \to K_iK_i\phi$$

$$\textbf{5}: \ \neg K_i\phi \to K_i\neg K_i\phi$$

$$\textbf{A1}: \ p_i(m) \to K_i\ p_i(m);\ p_i \in \{A_i\ snt, A_i\ rcvd\}$$

$$\textbf{A2}: \ A_i\ infers\ k \leftrightarrow K_i\ exists\ k$$

$$\textbf{A3}: \ unfresh\ m \to \exists m' \geq m \quad \bigvee_{A_i \in \mathcal{A}} \left(A_i\ snt\ m' \wedge\ K_i\ unfresh\ m'\right)$$

$$\textbf{A4}: p_i(m) \to p_i(m');\ m' \leq m, \quad p_i \in \{A_i\ rec, A_i\ sen, exists, unfresh\}$$

$$\textbf{A5}: \ A_i\ rcvd\ m \to A_i\ rec\ m$$

$$\textbf{A6}: \ A_i\ snt\ m \to A_i\ sen\ m$$

$$\textbf{A7}: \ p_i(m) \to exists\ m;\ \ p_i \in \{A_i\ rcvd, A_i\ snt\}$$

$$\textbf{A8}: \ A_i\ rec\ m \to \exists m' \geq m.\ A_i\ rcvd\ m'$$

$$\textbf{A9}: \ A_i\ sen\ m \to \exists m' \geq m.\ A_i\ snt\ m'$$

$$\textbf{A10}: \ exists\ m \to \exists m' \geq m.\ \bigvee_{A_i \in A}\ A_i\ infers\ m'$$

Fig. 5 Proof system of WS5

The proof system of WS5 is shown in Fig. 5 in which ϕ and ψ are formulae, m and m' are messages, and k is a key. Moreover, note that WS5 is a propositional logic and the symbol $\exists$ in axioms A8–A10 is a syntactic sugar for the disjunction of a finite number of statements. Moreover, the symbol $\forall$ in rule Nec is a syntactic sugar to represent all of the finite number of premises of the rule. It has been proven that WS5 is sound and complete with respect to the generalized Kripke semantics given in this section [11].

4 TWS5: A Temporal Epistemic Logic of Authentication Protocols

In this section, we propose a complete and omniscience-free temporal epistemic logic for the verification of authentication protocols. The underlying attacker model is also defined through the consistent message renaming functions involved in access relations. Our logic extends WS5 with temporal operators and is referred to as Temporal WS5, or TWS5 for short. The main challenging issue in developing this logic is finding intuitive models that reflect precedence among the actions taken by the agents in a protocol execution and the formation of knowledge with respect to performed actions. At the same time, the formulation of models should result in completeness. The reason for incorporating temporal operators in the logic is to provide the capacity for analyzing those protocols whose correctness largely depends on timely formation of agents' knowledge. Such protocols, e.g., stream authentication protocols, can only be verified by logics involving both knowledge and temporal operators [19]. As stated earlier, omniscience is a feature of epistemic logics that may result in misleading judgments about the protocols being analyzed. In this regard, the logic WS5 can serve as a candidate core for our logic as it is omniscience-free.

4.1 The Formulae and Models of TWS5

The formulae and models of TWS5 are defined on the basis of the set of agents $\mathcal{A}$, the set of keywords $\mathcal{P}$, the sub-message relation $\leq$, and the set of messages τ given in Sect. 3. The formulae of TWS5, however, may involve temporal operators and, in turn, the models should additionally reflect the meaning of these operators.

Definition 4.1 Given a set of atomic formulae Ω, the set $\mathcal{F}$ of TWS5 formulae is defined inductively by the following rules where $\bigcirc$ and $\mathcal{U}$ are symbols for next and until temporal operators.

- If $p \in \Omega$, then $p \in \mathcal{F}$.
- If $\phi, \psi \in \mathcal{F}$, then $\neg\phi, \phi \rightarrow \psi \in \mathcal{F}$.
- If $\phi \in \mathcal{F}$, then $K_i\phi \in \mathcal{F}$ for every $1 \leq i \leq n$.
- If $\phi, \psi \in \mathcal{F}$, then $\bigcirc \phi,\ \phi\, \mathcal{U}\, \psi \in \mathcal{F}$.

The meaning of a TWS5 formulae is given in terms of validity over possible worlds of a Kripke model generated by a message passing interpreted system (MPIS) [16], where agents send and receive messages. In what follows, we develop the semantics of TWS5.

Definition 4.2 For a given set of agents $\mathcal{A}$ and a set of messages τ, the initialization function is defined to be a function $\text{init}_{\mathcal{A},\tau} : \mathcal{A} \rightarrow 2^{\tau}$ that assigns every agent $A_i \in \mathcal{A}$ a set of messages. An action is also defined to be an element of the set $\Pi_{\mathcal{A},\tau} = \{A_i \text{ snd } m,\ A_i \text{ rcv } m \mid A_i \in \mathcal{A},\ m \in \tau\}$.

Definition 4.3 Given a set of agents $\mathcal{A}$ and a set of messages τ, an execution h until a time instant t is a finite multiset $h(t)$ such that $h(t-1) \subset h(t), h(t) \setminus h(t-1) \subset \Pi_{\mathcal{A},\tau}$, and $h(0) = \left\{A_i \text{ rcv } m \mid A_i \in \mathcal{A},\ m \in \text{init}_{\mathcal{A},\tau}(A_i)\right\}$. In fact, the messages that agents

receive in $h(0)$ are those messages that they initially infer. The finite multiset $h(t)$ is also called an execution history.

Definition 4.4 Let $A_i \in \mathcal{A}$. The execution history $h(t)$ in A_i's view, denoted by $h(t)|A_i$, is defined as $h(t)|A_i = h(t) \setminus \{A_j \text{ snd } m, A_j \text{ rcv } m \mid m \in \tau,\ A_j \neq A_i\}$.

Definition 4.5 Given a set of agents $\mathcal{A}$ and a set of messages τ, an MPIS, or a TWS5 model, is defined to be a triple $\mathcal{M} = \langle H, \{\rightsquigarrow_i^\rho\}, I\rangle$ such that

- $H = \bigcup_t H_t$ is the set of possible worlds where H_t is the set of all possible executions until t,
- for an agent $A_i \in \mathcal{A}$ and a message renaming function $\rho : \tau \to \tau$, $\rightsquigarrow_i^\rho \subseteq H \times H$ is the accessibility relation for A_i under ρ such that for every two possible worlds $h(t)$ and $h'(t')$, $h(t) \rightsquigarrow_i^\rho h'(t')$ iff ρ is consistent with the keys A_i infers from $h(t)$ and the application of ρ to $h(t)|A_i$ is equal to $h'(t')|A_i$, and
- I is an interpretation function from the set of atomic formulae to the power set of possible worlds, i.e., $I : \Omega \to 2^H$, defined by

$$
\begin{aligned}
&I(A_i \text{ snt } m) = \{h(t) \in H \mid A_i \text{ snd } m \in h(t)\},\\
&I(A_i \text{ rcvd } m) = \{h(t) \in H \mid A_i \text{ rcv } m \in h(t)\},\\
&I(A_i \text{ sen } m) = \{h(t) \in H \mid \exists m' \geq m.\ A_i \text{ snd } m' \in h(t)\},\\
&I(A_i \ rec\ m) = \{h(t) \in H \mid \exists m' \geq m.\ A_i \text{ rcv } m' \in h(t)\},\\
&I(\text{exists } m) = \{h(t) \in H \mid \exists A_i \in \mathcal{A}. \exists m' \geq m.\ A_i \text{ snd } m' \in h(t) \vee A_i \text{ rcv } m' \in h(t)\}, \text{ and}\\
&I(\text{unfresh } m) = \{h(t) \in H \mid \exists A_i \in \mathcal{A}.\ \exists t' < t_b.\ h(t') \in I(A_i \text{ sen } m)\}.
\end{aligned}
$$

  Here, t_b represents the start of the current epoch containing t. The details can be found in [2], but the interpretation of unfresh is not critical and other interpretations can also be used.

We also make use of an auxiliary keyword infers. The formula "$A\ infers\ m$" is meant to reflect the fact that m is among the initial knowledge of A or can be derived from what A knows. The formula "K_A exists m" reflects the same and can be regarded as the interpretation of "A infers m" [11].

Definition 4.6 Given a model $\mathcal{M} = \langle H, \{\rightsquigarrow_i^\rho\}, I\rangle$, for any $\phi, \psi \in \mathcal{F}$, any $a(m) \in \Omega$, and any $h(t) \in H$, the truth of a formula is defined as follows:

- $(\mathcal{M}, h(t)) \models a(m)$ iff $h(t) \in I(a(m))$.
- $(\mathcal{M}, h(t)) \models \neg\phi$ iff $(\mathcal{M}, h(t)) \not\models \phi$.
- $(\mathcal{M}, h(t)) \models \phi \to \psi$ iff $(\mathcal{M}, h(t)) \models \phi$ implies $(\mathcal{M}, h(t)) \models \psi$.
- $(\mathcal{M}, h(t)) \models \bigcirc\phi$ iff $(\mathcal{M}, h(t+1)) \models \phi$.
- $(\mathcal{M}, h(t)) \models \phi\ \mathcal{U}\ \psi$ iff for some $t' > t$, $(\mathcal{M}, h(l)) \models \phi$ for any $t \leq l < t'$ and $(\mathcal{M}, h(t')) \models \psi$.
- $(\mathcal{M}, h(t)) \models K_i\phi$ iff, for every $h'(t') \in H$ and every message renaming function $\rho : \tau \to \tau$, $h(t) \rightsquigarrow_i^\rho h'(t')$ implies that $(\mathcal{M}, h'(t')) \models \rho(\phi)$.

Notice that although at the first glance the definition of truth for the formula $K_i\phi$ involves arbitrary renaming functions ρ, the premise $h(t) \rightsquigarrow_i^\rho h'(t')$ limits them to those consistent with the keys inferred in $h(t)$.

Now, we give a proof system for TWS5 formulae.

4.2 Proof System of TWS5

Definition 4.7 Let $\phi, \phi', \psi \in \mathcal{F}$ and $a(m) \in \Omega$, the proof system of TWS5 consists of the following axioms and rules.

- A1-A10, K, T, 4, and 5: All axioms of WS5.
- A11: $\bigcirc\phi \wedge \bigcirc(\phi \rightarrow \psi) \rightarrow \bigcirc\psi$
- A12: $\bigcirc\neg\phi \leftrightarrow \neg \bigcirc \phi$.
- A13: $\phi \,\mathcal{U}\, \psi \leftrightarrow \psi \vee (\phi \wedge \bigcirc(\phi \,\mathcal{U}\, \psi))$
- A14: $a(m) \rightarrow \bigcirc a(m)$.
- R1: $\dfrac{\phi}{\bigcirc\phi}(TG)$
- R2: $\dfrac{\phi' \rightarrow (\neg\psi \wedge \bigcirc\phi')}{\phi' \rightarrow \neg(\phi \,\mathcal{U}\, \psi)}$(NU).
- R3: $\dfrac{\phi \;\; \phi \rightarrow \psi}{\psi}(MP)$
- R4: $\dfrac{\rho(\phi), \quad \forall \rho \lhd \kappa}{A_i \text{ infers } \kappa \rightarrow K_i\phi}$(Nec).

In the rules above, the names TG, NU, MP, and Nec are abbreviations for Temporal Generalization, Next-Until, Modus Ponens, and Necessitation, respectively.

A formula $\phi \in \mathcal{F}$ is true (or holds) in a TWS5 model $\mathcal{M} = \langle H, \{\rightsquigarrow_i^{\rho}\}, I\rangle$ if for any $h(t) \in H$ we have $(\mathcal{M}, h(t)) \models \phi$. A formula $\phi \in \mathcal{F}$ is valid if it is true in every TWS5 model. A TWS5 rule is valid if it preserves validity, that is, the validity of its premises results in the validity of its conclusion.

Theorem 4.8 *TWS5 is sound.*

Proof The validity of axioms A11, A12, A13, and rules TG and NU results from Definition 4.6. Axiom A14 is also valid due to Definition 4.3. The validity of those axioms of TWS5 that are inherited from the WS5 proof system as well as the rules MP and NEC are immediate.

5 Completeness

We prove that TWS5 is complete. To do so, we first give a short overview of the needed concepts, see [16]. Assume that $\mathcal{X}$ is an axiomatization system. A formula ϕ is $\mathcal{X}$-consistent if $\neg\phi$ is not provable in $\mathcal{X}$. A finite set $\{\phi_1, \ldots, \phi_k\}$ is $\mathcal{X}$-consistent if $\phi_1 \wedge \cdots \wedge \phi_k$ is $\mathcal{X}$-consistent. An infinite set of formulae is $\mathcal{X}$-consistent if its every finite subset is $\mathcal{X}$-consistent. A set Δ of formulae is maximal $\mathcal{X}$-consistent if Δ is $\mathcal{X}$-consistent and for any formula $\phi \notin \Delta$, $\Delta \cup \{\phi\}$ is not $\mathcal{X}$-consistent. It is known that any $\mathcal{X}$-consistent set Δ can be extended to a maximal $\mathcal{X}$-consistent set if $\mathcal{X}$ contains all of the tautologies of propositional calculus and the rule MP. Any maximal $\mathcal{X}$-consistent set Δ satisfies the properties shown in Fig. 6.

Let $\mathcal{M}_n$ be the class of all TWS5 models for n agents. To prove the completeness of TWS5, we should show that every formula $\phi \in \mathcal{F}$ that is valid with respect to $\mathcal{M}_n$

1. For any formula ϕ, either $\phi \in \Delta$ or $\neg\phi \in \Delta$.
2. $\phi \wedge \phi' \in \Delta$ iff $\phi \in \Delta$ and $\phi' \in \Delta$.
3. If $\phi \in \Delta$ and $\phi \rightarrow \phi' \in \Delta$, then $\phi' \in \Delta$.
4. If ϕ is provable in $\mathcal{X}$, then $\phi \in \Delta$.

Fig. 6 Properties of a maximal consistent set Δ

is provable in the proof system of TWS5. We can equivalently prove that the following property holds.

$$\text{Every TWS5-consistent formula is satisfiable with respect to } \mathcal{M}_n. \tag{5.1}$$

Suppose that we can prove (5.1) and ϕ is a valid formula. If ϕ is not provable in the TWS5 proof system, its double negation $\neg\neg\phi$ is not provable either. Therefore, $\neg\phi$ is a TWS5-consistent formula and consequently $\neg\phi$ is satisfiable with respect to $\mathcal{M}_n$. This contradicts the validity of ϕ. Hence, (5.1) implies completeness.

The sketch of the completeness proof is as follows: To prove completeness, we equivalently prove that every TWS5-consistent formula is satisfiable with respect to $\mathcal{M}_n$. To do so, we employ the general technique of building canonical models. Indeed, we build the canonical model $\mathcal{N}^c$ which has a state w corresponding to every maximal TWS5-consistent set w. We also show that a TWS5 formula ϕ belongs to w if it is satisfiable in a maximal TWS5-consistent set w of $\mathcal{N}^c$. Then, we prove that every TWS5-consistent formula is satisfiable with respect to $\mathcal{N}^c$. As $\mathcal{N}^c$ does not have the right shape of an MPIS, we extract a filtration model $\mathcal{M}^c \in \mathcal{M}_n$ from the canonical model. The possible worlds of $\mathcal{M}^c$ are execution histories that build on specific sequences of the possible worlds of $\mathcal{N}^c$. It is proven that if a TWS5 formula is satisfiable in a maximal TWS5-consistent set w of $\mathcal{N}^c$, then it is also satisfiable in the corresponding possible world of $\mathcal{M}^c$. Thus, we can prove that every TWS5-consistent formula is satisfiable with respect to $\mathcal{M}^c$. Since $\mathcal{M}^c \in \mathcal{M}_n$, it follows that TWS5 is complete.

We use the notion of counterpart models to build a canonical model. Counterpart models are used as a semantics for first order modal logics where new values are assigned to variables when we move along the accessibility relation [?]. In TWS5, we use a message renaming function to map a formula of a global state to another one and demand that the resulting formula should hold in the global state to which the current state has access. Intuitively, a message m at a possible world w corresponds to (is a counterpart of) m' at a possible world w' in A_i's view if A_i cannot distinguish between m and m'.

In the following arguments, by $\rho(\Delta)$ we mean the set $\{\rho(\phi) \mid \phi \in \Delta\}$ where Δ is a set of TWS5 formulae and ρ is a message renaming function.

Lemma 5.1 *Let $\mathcal{N}_n$ be the class of all counterpart Kripke models for n agents. There is a model $\mathcal{N}^c \in \mathcal{N}_n$, called a canonical model, where its possible worlds are maximal*

TWS5-consistent sets such that for any possible world w of $\mathcal{N}^c$ we have $(\mathcal{N}^c, w) \models \phi$ iff $\phi \in w$.

Proof For a given set of TWS5 formulae w, we define $w/K_i = \{\phi \mid K_i\phi \in w\}$ and $w/\bigcirc = \{\phi \mid \bigcirc\phi \in w\}$. Now, define the canonical model $\mathcal{N}^c = \langle W, \pi, \{\rightarrow_i^\rho\}, \prec\rangle$ as follows:

- $W = \{w \mid w$ is a maximal TWS5-consistent set$\}$.
- $\pi(w)(a(m)) =$ true if $a(m) \in w$, $\quad a(m) \in \Omega$.
- $\pi(w)(a(m)) =$ false if $a(m) \notin w$, $\quad a(m) \in \Omega$.
- $\rightarrow_i^\rho = \{(w, w') \mid \rho(w/K_i) \subseteq w'\}$ for any message renaming function $\rho : \tau \rightarrow \tau$ with $\rho \triangleleft \kappa$ where κ is the set of messages A_i infers from w, that is, A_i infers $\kappa \in w$.
- $\prec = \{(w, w') \mid w/\bigcirc \subseteq w'\}$.

The proof continues by induction on the number of the logical operators of TWS5 formulae. Assume that the property holds for all formulae with $n-1$ operators, we show that it also holds for any formula ϕ with n operators. The proof for atomic formulae and the ones constructed from atomic formulae using $\neg$ and $\rightarrow$ is immediate. Now, assume that ϕ is $K_i\psi$ for some ψ. For the 'if' part, we have $\phi \in w$. Therefore, $\psi \in w/K_i$. Now for every $(w, w') \in \rightarrow_i^\rho$, $\rho(\psi) \in w'$. Therefore, by the induction hypothesis, we have $(\mathcal{N}^c, w') \models \rho(\psi)$. Using Definition 4.6, we can conclude that $(\mathcal{N}^c, w) \models K_i\psi$.

For the 'only if' part, assume that $(\mathcal{N}^c, w) \models K_i\psi$. Now, for every message renaming function $\rho : \tau \rightarrow \tau$ such that $\rho \triangleleft \kappa$ and $A_i\ infers\ \kappa \in w$, consider the set $\rho(w/K_i) \cup \rho(\neg\psi)$. Any such set is not TWS5-consistent as otherwise there exists a maximal TWS5-consistent set w' such that $\rho(w/K_i) \cup \rho(\neg\psi) \subseteq w'$ and consequently $(w, w') \in \rightarrow_i^\rho$. Using the induction hypothesis we have $(\mathcal{N}^c, w') \models \rho(\neg\psi)$ and, in turn, $(\mathcal{N}^c, w) \models \neg K_i\psi$ which is a contradiction. Therefore, there exists a finite subset $\rho(\phi_1), \ldots, \rho(\phi_l), \rho(\neg\psi)$ of $\rho(w/K_i) \cup \rho(\neg\psi)$ which is not TWS5-consistent. We can show that $\vdash \rho(\phi_1) \rightarrow (\rho(\phi_2) \rightarrow (\cdots \rightarrow (\rho(\phi_l) \rightarrow \rho(\psi)) \cdots))$. Since ρ only applies to messages appearing in the formulae, we have $\vdash \rho(\phi_1 \rightarrow (\phi_2 \rightarrow (\cdots \rightarrow (\phi_l \rightarrow \psi)) \cdots))$. By the rule Nec, we conclude that $\vdash K_i(\phi_1 \rightarrow (\phi_2 \rightarrow (\cdots \rightarrow (\phi_l \rightarrow \psi) \cdots))$. By induction on l, axiom K and MP, we have $\vdash K_i\phi_1 \rightarrow (K_i\phi_2 \rightarrow (\cdots \rightarrow (K_i\phi_l \rightarrow K_i\psi) \ldots))$. Using Property 4 in Fig. 6, we have $K_i\phi_1 \rightarrow (K_i\phi_2 \rightarrow (\cdots \rightarrow (K_i\phi_l \rightarrow K_i\psi) \cdots)) \in w$. For any message renaming function $\rho : \tau \rightarrow \tau$ such that $\rho \triangleleft \kappa$ and $A_i\ infers\ \kappa \in w$, we have $\rho(\phi_1), \ldots, \rho(\phi_l) \in \rho(w/K_i)$. Thus, Nec implies $K_i\phi_1, \ldots, K_i\phi_l \in w$. Hence, from Property 3 in Fig. 6, we have $K_i\psi \in w$. The proof when ϕ is of the form $\bigcirc\psi$ or $\psi\ \mathcal{U}\ \psi'$ is standard using the definition of $\prec$ as well as the axiom NU. □

Theorem 5.2 *Every TWS5-consistent formula is satisfiable with respect to $\mathcal{N}_n$.*

Proof If ϕ is TWS5-consistent, then there exists a maximal TWS5-consistent set w such that $\phi \in w$. From Lemma 5.1, we have $(\mathcal{N}^c, w) \models \phi$ and consequently ϕ is satisfiable with respect to $\mathcal{N}_n$.

Given maximal $\mathcal{X}$-consistent sets $w_0, w_1, \ldots$, a sequence $\alpha = \langle w_0, w_1, \ldots\rangle$ is acceptable if $(w_k, w_{k+1}) \in \prec$ for any $k \geq 0$ and, for any $\psi_1\ \mathcal{U}\ \psi_2 \in w_k$, there exists

some $l \geq k$ such that $\psi_2 \in w_l$ and $\psi_1 \in w_{k'}$ with $k \leq k' < l$. It has been proven that for any maximal $\mathcal{X}$-consistent set w, there exists an acceptable sequence starting with it. Moreover, for any $\mathcal{X}$-consistent set w, there is an acceptable sequence containing w [16].

Lemma 5.3 *For any formula $\phi \in \mathcal{F}$ and mapping $\lambda : \tau \to \tau$, $\vdash \phi$ implies $\vdash \lambda(\phi)$.*

Proof The proof is by induction on the length of the proof of ϕ. Assume that for every mapping λ the above property holds for every proof of ϕ of length less than n. Now, we have to show that for every mapping λ, if ϕ is a theorem with a proof of length n, then $\lambda(\phi)$ is also a theorem. We should check that this property is preserved when applying the axioms and rules of TWS5. Assume that $\phi = K_j\psi$ and that we want to check Nec rule

$$\frac{\rho(\psi), \qquad \forall \rho \lhd \kappa}{A_j \text{ infers } \kappa \to K_j\psi}.$$

The proof for other axioms and rules is immediate.

Since the set of messages τ is finite, the set of message renaming functions that are consistent with the keys A_j infers is assumed to be $\{\rho_1, \ldots, \rho_l\}$. Evidently, $\rho_1(\psi), \ldots, \rho_l(\psi)$ are theorems with proof length less than n. Hence, if we define message renaming functions $\lambda' = \rho_i \circ \lambda \circ \rho_i^{-1}$, then $\rho_1 \circ \lambda \circ \rho_1^{-1}(\rho_1(\psi)), \ldots, \rho_l \circ \lambda \circ \rho_l^{-1}(\rho_l(\psi))$ are also theorems. Therefore, we have

$$\frac{\rho_1(\lambda(\psi)), \ldots, \rho_l(\lambda(\psi))}{K_j\lambda(\psi)}.$$

□

If we build an MPIS $\mathcal{M}^c$ from the canonical model $\mathcal{N}^c$, then we say that we can filter $\mathcal{N}^c$ to $\mathcal{M}^c$. For every acceptable sequence $\alpha = \langle w_0, \ldots, w_t, \ldots\rangle$ of the possible worlds of $\mathcal{N}^c$ and every w_t in α, we build a possible world of $\mathcal{M}^c$, noted $h^\alpha(t)$. To capture such a mapping, we use the notation $w_t, \alpha \mapsto h^\alpha(t)$. Let $int.act$ be an internal action on a given formula ϕ that returns all actions A_i snd m and A_i rcv m corresponding to the atomic formulae of the form A_i snt m and A_i rcvd m derivable from ϕ. The internal action is not interpreted in TWS5 and is only used in the proof of completeness. To build $h^\alpha(t)$ from α and w_t, we first extract all atomic formulae in w_t and add their corresponding actions to $h^\alpha(t)$. At the second step, for the formulae of the form $K_i\phi$, we take an internal action as described above. Figure 7 defines the filtration process.

We define H^c to be $\bigcup_{\alpha,t} h^\alpha(t)$. Assume that w_t and $w_{t'}$ are maximal TWS5-consistent sets that appear in the acceptable sequences α and α', respectively. Moreover, assume that w_{t_a} and $w_{t'_a}$ are their corresponding atomic formulae. We write $h^\alpha(t) \rightsquigarrow^\rho h^{\alpha'}(t')$ if $\rho(w_{t_a}) = w_{t'_a}$.

Lemma 5.4 *Let the TWS5 model $\mathcal{M}^c = \langle H^c, \{\rightsquigarrow_i^\rho\}, I^c\rangle$ be a filtration of the canonical model $\mathcal{N}^c = \langle W, \pi, \{\to_i^\rho\}, \prec\rangle$. Moreover, let $\alpha = \langle w_0, \ldots, w_t, \ldots\rangle$ and*

- $A_i\ rcv\ m \in h^\alpha(t)|A_i$ iff $K_i\ A_i\ rcvd\ m \in w_t$.
- $A_i\ snd\ m \in h^\alpha(t)|A_i$ iff $K_i\ A_i\ snt\ m \in w_t$.
- $A_i\ int.act\ \phi \in h^\alpha(t)|A_i$ iff $K_i\phi \in w_t$, $\quad for\ any\ \phi \in \mathcal{F} \setminus \Omega$.
- $h^\alpha(t) = \bigcup_i h^\alpha(t)|A_i$.

Fig. 7 The filtration $w_t, \alpha \mapsto h^\alpha(t)$

$\alpha' = \langle w_{0'}, \ldots, w_{t'}, \ldots\rangle$ be two acceptable sequences of the possible worlds of $\mathcal{N}^c$. Whenever $w_t, \alpha \mapsto h^\alpha(t)$, we have

(a) *$h^\alpha(t) \in I^c(a(m))$ iff $\pi(w_t)(a(m)) = true$ and $a(m) \in \Omega$.*
(b) *If $(w_t, w_{t'}) \in \rightarrow_i^\rho$, then there exists $w_{t''}$ in an acceptable sequence α'' of the possible worlds of $\mathcal{N}^c$ such that $w_{t'}, \alpha' \mapsto h^{\alpha''}(t'')$ and $h^\alpha(t) \rightsquigarrow_i^\rho h^{\alpha''}(t'')$.*
(c) *If $h^\alpha(t) \rightsquigarrow_i^\rho h^{\alpha'}(t')$, then there exists $w_{t''}$ in an acceptable sequence α'' of the possible worlds of $\mathcal{N}^c$ such that $w_{t''}, \alpha'' \mapsto h^{\alpha'}(t')$ and $(\mathcal{N}^c, w_t) \models K_i\phi \Rightarrow (\mathcal{N}^c, w_{t''}) \models \rho(\phi)$.*
(d) *If $(w_t, w_{t+1}) \in \prec$ with w_{t+1} in α, there exists an execution history $h^\alpha(t+1)$ such that $w_{t+1}, \alpha \mapsto h^\alpha(t+1)$ and $h^\alpha(t) \subset h^\alpha(t+1)$.*
(e) *If $h^\alpha(t) \subset h^\alpha(t+1)$, there exists an acceptable sequence α' equal to α up to w_t such that $w_{t+1}, \alpha' \mapsto h^\alpha(t+1)$. Moreover, $(\mathcal{N}^c, w_{t+1}) \models \phi \Rightarrow (\mathcal{N}^c, w_t) \models \bigcirc\phi$.*

Proof (a) We give the proof for the case $a(m) = A_i$ rcvd m.
$\pi(w_t)(A_i \text{ rcvd } m) = true$

$\Leftrightarrow A_i$ rcvd $m \in w_t$
$\Leftrightarrow K_i\ A_i$ rcvd $m \in w_t$ (Axioms A1 and T)
$\Leftrightarrow A_i$ rcv $m \in h^\alpha(t)|A_i$ $(w_t, \alpha \mapsto h^\alpha(t))$
$\Leftrightarrow h^\alpha(t) \in I^c(A_i \text{ rcvd } m)$.

(b) By $(w_t, w_{t'}) \in \rightarrow_i^\rho$ and the proof of Lemma 5.1 we have $\rho \lhd \kappa$ such that $A_i\ infers\ \kappa \in w_t$. We define $h^{\alpha''}(t'')|A_i$ to be $\rho(h^\alpha(t)|A_i)$ and give the proof for A_i snd $m \in h^\alpha(t)|A_i$.
A_i snd $m \in h^\alpha(t)|A_i$

$\Leftrightarrow K_i\ A_i$ snt $m \in w_t$ $(w_t, \alpha \mapsto h^\alpha(t))$
$\Leftrightarrow A_i$ snt $\rho(m) \in w_{t'}$ $((w_t, w_{t'}) \in \rightarrow_i^\rho)$
$\Leftrightarrow K_i\ A_i$ snt $\rho(m) \in w_{t'}$ (Axioms A1 and T)
$\Leftrightarrow A_i$ snd $\rho(m) \in h^{\alpha'}(t')|A_i$ $(w_{t'}, \alpha' \mapsto h^{\alpha'}(t'))$.

(c) Let w_{t_a} and $w_{t'_a}$ be the sets of the atomic formulae of the TWS5-consistent sets w_t and $w_{t'}$, respectively. Since $h^\alpha(t) \rightsquigarrow_i^\rho h^{\alpha'}(t')$, we have $\rho(w_{t_a}) = w_{t'_a}$. Now, we have to show that the set $h^{\alpha'}(t') \cup \{\rho(\phi) \mid K_i\phi \in w_t, \phi \in \mathcal{F}\}$ is TWS5-consistent. Let $h^{\alpha'}(t') = \{\rho(\theta_1), \ldots, \rho(\theta_k)\}$ and $\Delta = \{\rho(\phi_1), \ldots, \rho(\phi_l)\}$ be a finite subset of $\{\rho(\phi) \mid K_i\phi \in w_t, \phi \in \mathcal{F}\}$. Now, we have to show that $h^{\alpha'}(t') \cup \Delta$ is TWS5-consistent, as otherwise $\rho(\theta_1, \ldots, \theta_k) \vdash \neg\rho(\phi_1, \ldots, \phi_l)$. Since the message renaming function

ρ only applies to messages, we have $\vdash \rho((\theta_1 \wedge \cdots \wedge \theta_k) \rightarrow \neg(\phi_1 \wedge \cdots \wedge \phi_l))$. From Lemma 5.3, we can conclude that $\vdash \theta_1 \wedge \cdots \wedge \theta_k \rightarrow \neg(\phi_1 \wedge \cdots \wedge \phi_l)$. Hence, the set $\{\theta_1, \ldots, \theta_k, \phi_1, \ldots, \phi_l\}$ is TWS5-inconsistent which is a contradiction. Let $w_{t''}$ be the maximal TWS5-consistent set containing $h^{\alpha'}(t') \cup \Delta$. For any $m \in \tau$ and $A_j \in \mathcal{A}$, consider the following two cases. In the first case, we give the proof for $\phi = A_j$ rcvd m.

$(\mathcal{N}^c, w_t) \models K_i A_j$ rcvd m

$\Rightarrow K_i A_j$ rcvd $m \in w_t$ (Lemma 5.1)
$\Rightarrow A_j$ rcv $m \in h^{\alpha}(t)|A_i$ $(w_t, \alpha \mapsto h^{\alpha}(t))$
$\Rightarrow A_j$ rcv $\rho(m) \in h^{\alpha'}(t')|A_i$ $(h^{\alpha}(t) \rightsquigarrow_i^{\rho} h^{\alpha'}(t'))$
$\Rightarrow A_j$ rcvd $\rho(m) \in w_{t''}$ $(w_{t''}, \alpha'' \mapsto h^{\alpha'}(t'))$
$\Rightarrow (\mathcal{N}^c, w_{t''}) \models A_j$ rcvd $\rho(m)$ (Lemma 5.1).

Now, we prove the second case where ϕ is not an atomic formula.

$(\mathcal{N}^c, w_t) \models K_i \phi$
$\Rightarrow K_i \phi \in w_t$ (Lemma 5.1)
$\Rightarrow A_i\ int.act\ \phi \in h^{\alpha}(t)|A_i$ $(w_t, \alpha \mapsto h^{\alpha}(t))$
$\Rightarrow A_i\ int.act\ \rho(\phi) \in h^{\alpha'}(t')|A_i$ $(h^{\alpha}(t) \rightsquigarrow_i^{\rho} h^{\alpha'}(t'))$
$\Rightarrow K_i \rho(\phi) \in w_{t''}$ $(w_{t''}, \alpha'' \mapsto h^{\alpha'}(t'))$
$\Rightarrow (\mathcal{N}^c, w_{t''}) \models K_i \rho(\phi)$ (Lemma 5.1)

(d) From the way $\mathcal{M}^c$ is constructed from $\mathcal{N}^c$, we can conclude that there exists $h^{\alpha}(t+1)$ such that $w_{t+1}, \alpha \mapsto h^{\alpha}(t+1)$. We give the proof when A_i snd $m \in h^{\alpha}(t)|A_i$.

A_i snd $m \in h^{\alpha}(t)|A_i$

$\Rightarrow K_i\ A_i$ snt $m \in w_t$ $(w_t, \alpha \mapsto h^{\alpha}(t))$
$\Rightarrow A_i$ snt $m \in w_t$ (Axiom T)
$\Rightarrow \bigcirc A_i$ snt $m \in w_t$ (Axiom TG)
$\Rightarrow A_i$ snt $m \in w_{t+1}$ $((w_t, w_{t+1}) \in \prec)$.
$\Rightarrow A_i$ snd $m \in h^{\alpha}(t+1)|A_i$ $(w_{t+1}, \alpha \mapsto h^{\alpha}(t+1))$

(e) From the way $\mathcal{M}^c$ is constructed from $\mathcal{N}^c$, there exists a maximal TWS5-consistent set w_{t+1} in α such that $w_{t+1}, \alpha \mapsto h^{\alpha}(t+1)$.

$(\mathcal{N}^c, w_{t+1}) \models \phi$

$\Rightarrow \phi \in w_{t+1}$ (Lemma 5.1)
$\Rightarrow \bigcirc\phi \in w_t$ $((w_t, w_{t+1}) \in \prec)$
$\Rightarrow (\mathcal{N}^c, w_t) \models \bigcirc\phi$ (Lemma 5.1)

□

Now, we prove that a TWS5 formula is valid with respect to $\mathcal{N}^c$ iff it is valid with respect to $\mathcal{M}^c$, and hence, it is satisfiable with respect to $\mathcal{M}_n$.

Lemma 5.5 *Let the TWS5 model $\mathcal{M}^c = \langle H^c, \{\rightsquigarrow_i^{\rho}\}, I^c\rangle$ be a filtration of the canonical model $\mathcal{N}^c = \langle W, \pi, \{\rightarrow_i^{\rho}\}, \prec\rangle$. For any $\phi \in \mathcal{F}$ and every w_t in any acceptable sequence α of possible worlds of $\mathcal{N}^c$, the following property holds.*

$$(\mathcal{N}^c, w_t) \models \phi \text{ iff } (\mathcal{M}^c, h^{\alpha}(t)) \models \phi.$$

Proof The proof is by induction on the number of the logical operators in ϕ. Assume that the property holds for all formulae with $n-1$ operators. We show that it also holds for any formula with n operators. The proof for atomic formulae and the ones with only $\neg$ and $\wedge$ is trivial by Lemma 5.4a. Assume that $(\mathcal{M}^c, h^\alpha(t)) \models K_i\psi$. As demonstrated in the proof of Lemma 5.4b, $(w_t, w_{t'}) \in \rightarrow_i^\rho$ implies that there exists $w_{t''}$ in an acceptable sequence α'' of the possible worlds of $\mathcal{N}^c$ such that $w_{t'}, \alpha' \mapsto h^{\alpha''}(t'')$ and $h^\alpha(t) \rightsquigarrow_i^\rho h^{\alpha''}(t'')$ where $h^{\alpha''}(t'')$ can be taken $\rho(h^\alpha(t)|A_i)$. Therefore, for every $w_{t'} \in W$ in an acceptable sequence α' and any message renaming function $\rho : \tau \to \tau$, if $w_{t'}$ is an antecedent of w_t induced by ρ, we have $h^\alpha(t) \rightsquigarrow_i^\rho h^{\alpha'}(t')$. This implies that $(\mathcal{M}^c, h^{\alpha'}(t')) \models \rho(\psi)$. By induction hypothesis, we have $(\mathcal{N}^c, w_{t'}) \models \rho(\psi)$. From Definition 4.6, we conclude that $(\mathcal{N}^c, w_t) \models K_i\psi$. Conversely, assume that $(\mathcal{N}^c, w_t) \models K_i\psi$. Using Lemma 5.4.c, for every $h^{\alpha'}(t') \in H^c$ and any message renaming function $\rho : \tau \to \tau$, if $h^\alpha(t) \rightsquigarrow_i^\rho h^{\alpha'}(t')$, then there exists $w_{t''} \in W$ in an acceptable sequence α'' such that $w_{t''}, \alpha'' \mapsto h^{\alpha'}(t')$ and $(\mathcal{N}^c, w_t) \models K_i\psi \Rightarrow (\mathcal{N}^c, w_{t''}) \models \rho(\psi)$. Therefore, $(\mathcal{N}^c, w_{t''}) \models \rho(\psi)$. By induction hypothesis, we have $(\mathcal{M}^c, h^{\alpha'}(t')) \models \rho(\phi)$. From Definition 4.6, $(\mathcal{M}^c, h^\alpha(t)) \models K_i\psi$.

Assume that $(\mathcal{N}^c, w_t) \models \bigcirc\psi$. For any $w_{t'}$ that is an antecedent of w_t induced by $\prec$, $(w_t, w_{t+1}) \in \prec$, we have $(\mathcal{N}^c, w_{t+1}) \models \psi$. From Lemma 5.4.d, there exists $h^\alpha(t+1) \in H$ such that $w_{t+1}, \alpha \mapsto h^\alpha(t+1)$. Induction hypothesis implies $(\mathcal{M}^c, h^\alpha(t+1)) \models \psi$. From Definition 4.6, we have $(\mathcal{M}^c, h^\alpha(t)) \models \bigcirc\psi$. Conversely, assume that $(\mathcal{M}^c, h^\alpha(t)) \models \bigcirc\psi$. By Definition 4.6, we have $(\mathcal{M}^c, h^\alpha(t+1)) \models \psi$. From Lemma 5.4.e, there exists an acceptable sequence α' equal to α up to w_t such that $w_{t+1}, \alpha' \mapsto h^\alpha(t+1)$. By induction hypothesis, we conclude that $(\mathcal{N}^c, w_{t+1}) \models \psi$. Through applying Lemma 5.4.e another time, it can be concluded that $(\mathcal{N}^c, w_t) \models \bigcirc\psi$. □

Theorem 5.6 *TWS5 is complete.*

Proof According to Theorem 5.2 and since $\mathcal{N}^c \in \mathcal{N}_n$, we conclude that every TWS5-consistent formula is satisfiable with respect to $\mathcal{N}^c$. According to Lemma 5.5, if $\mathcal{M}^c$ is the filtration model resulting from the canonical model $\mathcal{N}^c$, every TWS5-consistent formula is satisfiable with respect to $\mathcal{M}^c$. From Property 5.1 (on p. 12), $\mathcal{M}^c \in \mathcal{M}_n$ implies that every TWS5-consistent formula is satisfiable with respect to $\mathcal{M}_n$. This is equivalent to the completeness of TWS5. □

6 Analyzing Some Example Protocols Using TWS5

In this section, we employ TWS5 to verify some authentication protocols. The first example is Lowe's modified Wide-Mouth Frog protocol [26] shown in Fig. 8. In this protocol, A and B are two agents and S is a trusted server. The timestamps t_a and t_s are generated by A and S, respectively. The symmetric key k_{as} is shared between A and S. Similarly, k_{bs} is a symmetric key only known to B and S. The symmetric key k_{ab} is generated by A and intended to serve as the session key between A and B. The random number n_b is a nonce generated by B and succ(n_b) is its successor. In

$$
\begin{aligned}
&A \rightarrow S: \ A.\{t_a.B.k_{ab}\}_{k_{as}} \\
&S \rightarrow B: \ \{t_s.A.k_{ab}\}_{k_{bs}} \\
&B \rightarrow A: \ \{n_b\}_{k_{ab}} \\
&A \rightarrow B: \ \{succ(n_b)\}_{k_{ab}}
\end{aligned}
$$

Fig. 8 Lowe's wide-mouth frog protocol

1. $\bigcirc^u \ K_B \ exists \ k_{ab}$: After u steps B knows that k_{ab} exists.
2. $\bigcirc^v \ K_A \ exists \ n_b$: After v steps A knows that n_b exists.
3. $K_A \ \bigcirc^{u+1} \ B \ snt \ \{n_b\}_{k_{ab}}$: A knows that after $u+1$ steps B has sent $\{n_b\}_{k_{ab}}$.

Fig. 9 The properties we prove for the protocol shown in Fig. 8

$$
\begin{aligned}
&\mathbf{S_1}.\ S \ rcvd \ A.\{t_a.B.k_{ab}\}_{k_{as}} \wedge K_S \neg unfresh \ t_a \leftrightarrow \bigcirc S \ snt \ \{t_s.A.k_{ab}\}_{k_{bs}} \\
&\mathbf{S_2}.\ B \ rcvd \ \{t_s.A.k_{ab}\}_{k_{bs}} \wedge K_B \neg unfresh \ t_s \leftrightarrow \bigcirc B \ snt \ \{n_b\}_{k_{ab}} \\
&\mathbf{S_3}.\ A \ rcvd \ \{n_b\}_{k_{ab}} \leftrightarrow \bigcirc A \ snt \ \{n_b+1\}_{k_{ab}}
\end{aligned}
$$

Fig. 10 The specification of the protocol shown in Fig. 8

this example, we assume that the roles of A and B can not be swapped as otherwise a message received by an agent could actually be sent by itself.

Now, we assume that the following set of statements hold for some $u, v \in \mathbb{N}$ where $u < v$.

$\Gamma = \{S \text{ rcvd } A \cdot \{t_a.B.k_{\text{ab}}\}_{k_{\text{as}}}, \ \bigcirc^u \ B \text{ rcvd } \{t_{\text{s}} \cdot A \cdot k_{ab}\}_{k_{bs}}, \ \bigcirc^v A \text{ rcvd } \{n_b\}_{k_{ab}}, A \text{ infers } k_{ab}, k_{as} \text{ secret of } \{A, S\}, \ k_{bs} \text{ secret of } \{B, S\}, K_{\text{s}} \ \neg\text{unfresh } t_a, \ \bigcirc^u K_B \neg\text{unfresh } t_{\text{s}}\}$.

These assumptions are based on what agents have received through the protocol steps shown in Fig. 8. In the set of assumptions, the formula $k \ secret \ of \ G$ is a syntactic sugar defined by

$$k \text{ secret of } G \leftrightarrow \Big(\Big(\bigwedge_{A \in G} A \text{ infers } k \Big) \wedge \Big(\bigwedge_{A \notin G} \neg \ A \text{ infers } k \Big) \Big).$$

Moreover, $\bigcirc^u \ B$ rcvd $\{t_{\text{s}} \cdot A \cdot k_{ab}\}_{k_{bs}}$ means that B rcvd $\{t_{\text{s}} \cdot A \cdot k_{ab}\}_{k_{bs}}$ holds after u steps from the start of the protocol execution.

We prove that Lowe's modified Wide-Mouth Frog protocol meets the properties in Fig. 9. These properties collectively make the belief that A will be certain that B is communicating with A using the key A has generated in the first step of the protocol. To verify the protocol against these properties (requirements), we should first build a trust theory [3,30,31] comprising the assumptions made and the protocol specification. Figure 10 shows the protocol specification in terms of TWS5 formulae.

1. $Tr \vdash \bigcirc^u\ B\ rcvd\ \{ts.A.k_{ab}\}_{k_{bs}}\quad(\Gamma)$
2. $Tr \vdash B\ rcvd\ \{ts.A.k_{ab}\}_{k_{bs}} \rightarrow K_B\ B\ rcvd\ \{ts.A.k_{ab}\}_{k_{bs}}\quad(A_1)$
3. $Tr \vdash \bigcirc^u\ B\ rcvd\ \{ts.A.k_{ab}\}_{k_{bs}} \rightarrow \bigcirc^u\ K_B\ B\ rcvd\ \{ts.A.k_{ab}\}_{k_{bs}}\quad(2, A_{11}, TG)$
4. $Tr \vdash \bigcirc^u\ K_B\ B\ rcvd\ \{ts.A.k_{ab}\}_{k_{bs}}\quad(1, 3, MP)$
5. $Tr \vdash B\ rcvd\ \{ts.A.k_{ab}\}_{k_{bs}} \rightarrow exists\ \{ts.A.k_{ab}\}_{k_{bs}}\quad(A_7)$
6. $Tr \vdash K_B\ B\ rcvd\ \{ts.A.k_{ab}\}_{k_{bs}} \rightarrow K_B\ exists\ \{ts.A.k_{ab}\}_{k_{bs}}\quad(5, K, Nec, \Gamma)$
7. $Tr \vdash \bigcirc^u\ K_B\ B\ rcvd\ \{ts.A.k_{ab}\}_{k_{bs}} \rightarrow \bigcirc^u\ K_B\ exists\ \{ts.A.k_{ab}\}_{k_{bs}}\quad(6, A_{11}, TG)$
8. $Tr \vdash \bigcirc^u\ K_B\ exists\ \{ts.A.k_{ab}\}_{k_{bs}}\quad(4, 7, MP)$
9. $Tr \vdash exists\ \{ts.A.k_{ab}\}_{k_{bs}} \rightarrow exists\ k_{ab}\quad(A_4)$
10. $Tr \vdash K_B\ exists\ \{ts.A.k_{ab}\}_{k_{bs}} \rightarrow K_B\ exists\ k_{ab}\quad(9, K, Nec, \Gamma)$
11. $Tr \vdash \bigcirc^u\ K_B\ exists\ \{ts.A.k_{ab}\}_{k_{bs}} \rightarrow \bigcirc^u\ K_B\ exists\ k_{ab}\quad(10, A_{11}, TG)$
12. $Tr \vdash \bigcirc^u\ K_B\ exists\ k_{ab}\quad(8, 11, MP)$

1. $Tr \vdash \bigcirc^v\ A\ rcvd\ \{n_b\}_{k_{ab}}\quad(\Gamma)$
2. $Tr \vdash A\ rcvd\ \{n_b\}_{k_{ab}} \rightarrow K_A\ A\ rcvd\ \{n_b\}_{k_{ab}}\quad(A_1)$
3. $Tr \vdash \bigcirc^v\ A\ rcvd\ \{n_b\}_{k_{ab}} \rightarrow \bigcirc^v\ K_A\ A\ rcvd\ \{n_b\}_{k_{ab}}\quad(2, A_{11}, TG)$
4. $Tr \vdash \bigcirc^v\ K_A\ A\ rcvd\ \{n_b\}_{k_{ab}}\quad(1, 3, MP)$
5. $Tr \vdash A\ rcvd\ \{n_b\}_{k_{ab}} \rightarrow exists\ \{n_b\}_{k_{ab}}\quad(A_7)$
6. $Tr \vdash K_A\ A\ rcvd\ \{n_b\}_{k_{ab}} \rightarrow K_A\ exists\ \{n_b\}_{k_{ab}}\quad(5, K, Nec, \Gamma)$
7. $Tr \vdash \bigcirc^v\ K_A\ A\ rcvd\ \{n_b\}_{k_{ab}} \rightarrow \bigcirc^v\ K_A\ exists\ \{n_b\}_{k_{ab}}\quad(6, A_{11}, TG)$
8. $Tr \vdash \bigcirc^v\ K_A\ exists\ \{n_b\}_{k_{ab}}\quad(4, 7, MP)$
9. $Tr \vdash exists\ \{n_b\}_{k_{ab}} \rightarrow exists\ n_b\quad(A_4)$
10. $Tr \vdash K_A\ exists\ \{n_b\}_{k_{ab}} \rightarrow K_A\ exists\ n_b\quad(9, K, Nec, \Gamma)$
11. $Tr \vdash \bigcirc^v\ K_A\ exists\ \{n_b\}_{k_{ab}} \rightarrow \bigcirc^v\ K_A\ exists\ n_b\quad(10, A_{11}, TG)$
12. $Tr \vdash \bigcirc^v\ K_A\ exists\ n_b\quad(8, 11, MP)$

1. $Tr \vdash \bigcirc^u\ B\ rcvd\ \{ts.A.k_{ab}\}_{k_{bs}}\quad(\Gamma)$
2. $Tr \vdash B\ rcvd\ \{t_s.A.k_{ab}\}_{k_{bs}} \wedge K_B \neg unfresh\ t_s \rightarrow \bigcirc\ B\ snt\ \{n_b\}_{k_{ab}}\quad(S_2)$
3. $Tr \vdash \bigcirc^u\ B\ rcvd\ \{t_s.A.k_{ab}\}_{k_{bs}} \wedge \bigcirc^u\ K_B \neg unfresh\ t_s \rightarrow \bigcirc^{u+1}\ B\ snt\ \{n_b\}_{k_{ab}}$
   $(2, A_{11}, TG)$
4. $Tr \vdash \bigcirc^{u+1}\ B\ snt\ \{n_b\}_{k_{ab}}\quad(1, 3, MP, \Gamma)$
5. $Tr \vdash K_A\ \bigcirc^{u+1}\ B\ snt\ \{n_b\}_{k_{ab}}\quad(4, Nec, \Gamma)$

Fig. 11 Lowe's wide-mouth frog protocol meets the properties in Fig. 9

In this specification A, B, and S range over $\mathcal{A}$ including attackers. The formula S_1 says that if a server S receives a packet of the form $A \cdot \{t_a \cdot B \cdot k_{ab}\}$ and it knows that the timestamp t_a is not unfresh by checking its own clock, then at the next step it will send a packet of the form $\{t_s \cdot A \cdot k_{ab}\}_{k_{bs}}$. The formulae S_2 and S_3 reflect similar facts. Let $Tr = \{S_1, S_2, S3\} \cup \Gamma$ be the trust theory of the protocol in Fig. 8. We should

$$
\begin{aligned}
h_1(t-2) &= h_1(t-3) \cup \{S\ snd\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac(g(k_{i-1}), \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2})\}\\
h_1(t-1) &= h_1(t-2) \cup \{R\ rcv\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac(g(k_{i-1}), \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2})\}\\
h_1(t) &= h_1(t-1) \cup \{S\ snd\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac(g(k_i), \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1})\}\\
h_1(t+1) &= h_1(t) \cup \{R\ rcv\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac(g(k_i), \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1})\}\\
h_1(t+2) &= h_1(t+1) \cup \{S\ snd\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i)\}\\
h_1(t+3) &= h_1(t+2) \cup \{R\ rcv\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i)\}
\end{aligned}
$$

$$
\begin{aligned}
h_2(t-2) &= h_2(t-3) \cup \{S\ snd\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac(g(k_{i-1}), \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2})\}\\
h_2(t-1) &= h_2(t-2) \cup \{R\ rcv\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac(g(k_{i-1}), \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2})\}\\
h_2(t) &= h_2(t-1) \cup \{S\ snd\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac(g(k_i), \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1})\}\\
h_2(t+1) &= h_2(t) \cup \{C(R)\ rcv\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac(g(k_i), \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1})\}\\
h_2(t+2) &= h_2(t+1) \cup \{S\ snd\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i)\}\\
h_2(t+3) &= h_2(t+2) \cup \{C(R)\ rcv\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i),\\
&\qquad C(S)\ snd\ \{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1}.mac(g(k_i), \{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1})\}\\
h_2(t+4) &= h_2(t+3) \cup \{R\ rcv\ \{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1}.mac(g(k_i), \{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1})\}\\
h_2(t+5) &= h_2(t+4) \cup \{S\ snd\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i)\}\\
h_2(t+6) &= h_2(t+5) \cup \{R\ rcv\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i)\}
\end{aligned}
$$

Fig. 12 Executions h_1 and h_2 of the protocol shown in Fig. 1 with mode m([1,4],2)

prove that the properties shown in Fig. 9 hold in each execution of the protocol under this trust theory. The proofs are given in Fig. 11.

The Second example is the protocol of Sect. 2 which operates in the mode $m([1, 4], 2)$. Two executions of this protocol are shown in Fig. 12 where it is assumed that $h_1(t-3) = h_2(t-3)$. Moreover, the model of the protocol is denoted by $\mathcal{M}$. Let ρ be a message renaming function such that $\rho(\{m_i\}_{k_s}) = \{m'_i\}_{k_c}$, $\rho(\{m'_i\}_{k_c}) = \{m_i\}_{k_s}$, and $\rho(m) = m$ for other messages. As R does not infer the keys k_s and k_c, this message renaming function is consistent with the keys R infers. Now, Since $h_1(t+1) \rightsquigarrow_R^{\rho} h_2(t+4)$, we have

$$
\begin{aligned}
(\mathcal{M}, h_1(t+1)) \not\models K_R\ & S\ \text{snt}\ \{m_i\}_{k_s} \cdot f(k_{i+1})\\
& \cdot k_{i-1} \cdot \text{mac}(g(k_i) \cdot \{m_i\}_{k_s} \cdot f(k_{i+1}).k_{i-1}) \cdot
\end{aligned} \tag{6.1}
$$

Since TWS5 is complete, (6.1) implies that the protocol does not fulfill the intended requirement. Note that in this example, we need to update the message algebra for specifying mac and the protocol.

7 Conclusion

We have presented an omniscience-free and complete temporal logic of knowledge for verifying authentication protocols. By this logic, in particular, one can analyze those protocols whose successful operation highly depends on timely actions by the principals involved in the protocol. The application of this logic to some example protocols evidences its capacity for verifying different kinds of authentication protocols. There is still much to be done. Developing an automated prover based on this logic is among the topics deserving future research.

Acknowledgements The authors would like to take this opportunity to thank Prof. Massoud Pourmahdian for his valuable comments in this research.

References

1. Abadi, M., Rogaway, P.: Reconciling two views of cryptography (the computational soundness of formal encryption). J. Cryptol. **15**(2), 103–127 (2002)
2. Abadi, M., Tuttle, M.R.: A semantics for a logic of authentication. In: Proceedings of the 10th Annual ACM Symposium on Principles of Distributed Computing, pp. 201–216 (1991)
3. Becker, M.Y., Russo, A., Sultana, N.: Foundations of logic-based trust management. In: Proceedings of the IEEE Symposium on Security and Privacy, pp. 161–175 (2012)
4. Belardinelli, F., Lomuscio, A: Interactions between time and knowledge in a first-order logic for multi-agent systems. In: Proceedings of the 12th International Conference on the Principles of Knowledge Representation and Reasoning, pp. 38–48 (2010)
5. Bonakdarpour, B., Hajisheykhi, R., Kulkarni, S.S.: Knowledge-based automated repair of authentication protocols. In: Proceedings of the 19th International Symposium on Formal Methods, pp. 132–147 (2014)
6. Boureanu, I., Cohen, M., Lomuscio, A.: Automatic verification of temporal-epistemic properties of cryptographic protocols. J. Appl. Non-Class. Logics **19**(4), 463–487 (2009)
7. Boureanu, I., Jones, A.V., Lomuscio, A.: Automatic verification of epistemic specifications under convergent equational theories. In: Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems, pp. 1141–1148 (2012)
8. Boureanu, I., Kouvaros, P., Lomuscio, A.: Verifying security properties in unbounded multiagent systems. In: Proceedings of the International Conference on Autonomous Agents and Multiagent Systems, pp. 1209–1217 (2016)
9. Burrows, M., Abadi, M., Needham, R.M.: A logic of authentication. ACM Trans. Comput. Syst. **8**(1), 18–36 (1990)
10. Chao, L., Hui, L., Jianfeng, M.: Analysis the properties of TLS based on temporal logic of knowledge. In: Proceedings of the 5th International Conference on Information Assurance and Security, pp. 19–22 (2009)
11. Cohen, M.: Logics of Knowledge and Cryptography: Completeness and Expressiveness. PhD Thesis, KTH, Stockholm, Sweden (2007)
12. Cohen, M., Dam, M.: Logical omniscience in the semantics of BAN logic. In: Proceedings of the Foundations of Computer Security Workshop, pp. 121–132 (2005)
13. Cohen, M., Dam, M.: A complete axiomatization of knowledge and cryptography. In: Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science, pp. 77–88 (2007)
14. Davis, E.: A proof-based approach to formalizing protocols in linear epistemic logic. PhD Thesis, Carnegie Mellon University, Pittsburgh (2014)
15. Dechesne, F., Wang, Y.: To know or not to know: epistemic approaches to security protocol verification. Synthese **177**(1), 51–76 (2010)
16. Fagin, R., Moses, Y., Halpern, J.Y., Vardi, M.Y.: Reasoning About Knowledge. The MIT Press, Cambridge, Massachusetts (2003)

17. Garcia, F.D., Hasuo, I., Pieters, W., Van Rossum, P.: Provable anonymity. In: Proceedings of the ACM Workshop on Formal Methods in Security Engineering, pp. 63–72 (2005)
18. Gong, L., Needham, R., Yahalom, R.: Reasoning about belief in cryptographic protocols. In: Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, pp. 234–248 (1990)
19. Governatori, G., Orgun, A.M., Liu, C.: Modal tableaux for verifying stream authentication protocols. J. Autonom. Agents Multi Agent Syst. **19**(1), 53–75 (2009)
20. J.Y. Halpern and R. Pucella, Modeling adversaries in a logic for security protocol analysis. In: Proceedings of the 1st International Conference on Formal Aspects of Security, pp. 115–132 (2003)
21. Halpern, J.Y., Pucella, R.: Dealing with logical omniscience: expressiveness and pragmatics. Artif. Intell. **175**(1), 220–235 (2011)
22. Hunter, A., Delgrande, J.P.: Belief change and cryptographic protocol verification. In: Proceedings of the 22th National Conference on Artificial Intelligence, pp. 427–433 (2007)
23. Lewis, D.K.: Counterpart theory and quantified modal logic. J. Philos. **65**(5), 113–126 (1968)
24. Liu, C.: Logical foundations for reasoning about trust in secure digital communication. In: Proceedings of the Australian Joint Conference on Artificial Intelligence, pp. 333–344 (2001)
25. Lomuscio, A., Woźna, B.: A complete and decidable security-specialised logic and its application to the TESLA protocol. In: Proceedings of the 5th International Joint Conference on Autonomous Agents and Multiagent Systems, pp. 145–152 (2006)
26. Lowe, G.: A family of attacks upon authentication protocols. Technical Report, Department of Mathematics and Computer Science, University of Leicester (1997)
27. Lowe, G.: A hierarchy of authentication specifications. In: Proceedings of 10th Computer Security Foundations Workshop, pp. 31–43 (1997)
28. Luo, X., Chen, Y., Gu, M., Wu, L.: Model checking Needham-Schroeder security protocol based on temporal logic of knowledge. In: Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 551–554 (2009)
29. Ma, J., Orgun, M., Adi, K.: An analytic tableau calculus for a temporalised belief logic. J. Appl. Logic **9**(4), 289–304 (2011)
30. Ma, J., Orgun, M.A.: Formalising theories of trust for authentication protocols. Inf. Syst. Front. **10**(1), 19–32 (2008)
31. Ma, J., Orgun, M.A., Sattar, A.: Analysis of authentication protocols in agent-based systems using labeled tableaux. IEEE Trans. Syst. Man Cybern. B Cybern. **39**(4), 889–900 (2009)
32. Ma, J., Schewe, K.: A temporalised belief logic for reasoning about authentication protocols. In: Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1721–1728 (2012)
33. Masalagiu, C., Alaib, V.: Logic engineering with applications to security. In: Proceedings of the Romanian Academy Series A-mathematics Physics Technical Sciences Information Science, pp. 141–148 (2012)
34. Orgun, M.A., Ma, J., Liu, C., Governatori, G.: Analysing stream authentication protocols in autonomous agent-based systems. In: Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp. 325–332 (2006)
35. Perrig, A., Canetti, R., Tygar, J.D., Song, D.: Efficient authentication and signing of multicast streams over lossy channels. In: Proceedings of the IEEE Symposium on Security and Privacy, pp. 56–73 (2000)
36. Syverson, P.F., Van Oorschot, P.C.: On unifying some cryptographic protocol logics. In: Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, pp. 14–28 (1994)
37. van Eijck, J., Gattinger, M.: Elements of epistemic crypto logic. In: Proceedings of the International Conference on Autonomous Agents and Multiagent Systems, pp. 1795–1796 (2015)
38. Yanjing, W.: Epistemic Modelling and Protocol Dynamics. PhD Thesis, Universiteit van Amsterdam (2010)