# Formalizing and Verifying Authenticity over Assertion Changes for An Interaction Protocol

Xiaolie Ye and Lejian Liao

School of Computer Science and Technology, Beijing Institute of Technology,
5 South Zhongguancun Street, Haidian District, Beijing, China

**Abstract.** The Semantic Web techniques, like OWL[1], bring more semantic to the static information about functionalities and non-functionalities of Web services. However, it is not smooth to faithfully describe some dynamic aspects and support reasoning tasks. When discussing the security of interactions of Web services, we should solve such problems like how to describe interactive behaviors, static information, and the security properties required in the ontological layer, and how to validate those properties by a reasonable reduction method. As well-known, a knowledge base (e.g. that contains assertive axioms in OWL), can be used to represent the possible states of a world. Then, using a set of the assertions(assertion changes)that describe the update and erasure in instance level for a knowledge base, we propose an approach to conceptualize transitions of states for modeling interactions of Web services. Furthermore, we present an OWL-based Past Linear Temporal Logic (Past-LTL)[2] to describe temporal properties within a finite sequence of interactions and refine some algorithms to reduce the validity of an OWL-based Past-LTL formula into the entailment relationship in OWL.

**Keywords:** Ontology Change, Interaction Protocol, Temporal Logic, Authenticity

## 1 Introduction

Due to the importance of security for Web services, the dynamic aspects of interactive services should be formalized and verified for the satisfaction of some security requirement, such as the compliance of authentication, authorization and privacy policy. In particular, if a cryptographic protocol is designated to perform the authentication in the composition of services, we should abstract the relevant interactions and verify it. Respecting *authenticity*, the intuitional explanation is that an event $e$ authenticates an agent $a$ such that $e$ can occurs only if a previous message was send by $a$ [23]. For example, given the Needham-Schroeder Public Key protocol [19] as follows, when *Server* authenticates *Alice*

[1] Web Ontology Language , at http://www.w3.org/TR/owl-guide/

[2] It is the variant of LTL that only concern the temporal relations in the past time, such as *yesterday* and *until in history*.

with $Nonce_s$, $Server$ should detect whether a *correspondence assertion*[23] is true: once $Server$ accepts $Nonce_s$ encrypted by $K_s$ , it should ensure the event corresponding has occurred in the past, namely, that $Server$ created $Nonce_s$ and sent $Nonce_s$ encrypted by $K_a$.

$$\begin{aligned}
Alice \rightarrow Server &: (a, Nonce_a)_{K_s}\\
Server \rightarrow Alice &: (Nonce_s, Nonce_a)_{K_a}\\
Alice \rightarrow Server &: (Nonce_s)_{K_s}
\end{aligned}$$

So that, one agent should become sure of the identity of the other. Usually, the authenticity is represented as a temporal relationship of events occurring in an interaction protocol of Web services. In the relevant studies [20, 6, 24], authors mainly concern using the grounding messages and operators for the security protocol analysis in the SOAP-based layer. Meanwhile, the relevant techniques of Semantic Web bring more semantics to the functionality and non-functionality of Web services and composition, and perform reasoning tasks for semantic matchmaking. The Web Ontology Language(OWL) and OWL-S [3] have been widely accepted in practice. Respecting OWL-S, to describe their functionality, services are viewed as processes that have pre-conditions and effects. Further, it leads to the consideration about representing interactions of Web services in the OWL and reasoning for the satisfaction of requirement.

However, towards faithfully unrevealing the dynamic aspects of services, it is beyond the expressiveness and reasoning capability of the OWL. Even if we obtain the conversational interactions of processes described in the OWL-S, none of the approaches in [20, 6], is adoptable for us to verify security properties in the semantic layer. That is because that, after mapping the ontological representation into the SOAP-base encapsulation, the implicit and hidden information in the semantic layer will not be preserved completely. Perhaps, it will cause ignoring potential flaws. On the other hand, the formalism and reasoning mechanism in [20, 6] are based on the *Closed World Assumption*(the unknown is false by default), but, the basic logics of the OWL, like the Description Logics(DLs), is on the *Open World Assumption*. Generally speaking, we should consider how to describe interactive behaviors, changes of information, and the security properties required in the ontology-based semantic layer, and how to validate those properties by a reasonable reduction method.

Moreover, our issue is relevant to the well-known *frame problem* [22](how to handle the consequence of actions and those facts that remain unaffected by actions), and the reasoning task for inconsistency has to be performed under incomplete knowledge of the world. In recent years, *Ontology Evolution*, as the generalized case of inconsistent problems, has been classified as one subfield of the relevant research about *Ontology Change* [9]. In essence, it addresses how to represent the reaction for changing an ontology in order to reflect a change in the domain of interest. As mentioned in [11], there is a pair of changing operations,

[3] Ontology Web Language for Services to provide the building blocks for encoding rich semantic service descriptions, http://www.w3.org/Submission/OWL-S.

*update* and *erasure*, which revise the intensional level of the ontology or the extensional, or both, e.g. making effect on both *ABox* and *TBox* of a knowledge base in Description Logics(DL)[2]. There, the special case that changes only occurs in the extensional level of ontology is so-called *assertion change*, which is similar as other notations, like *ABox update* in [18], and *instance level update and erasure* in [11]. As we know, while the intension level of ontology is stable and is defined to conceptualize the domain of intense, the extension level, frequently changing, can be used to represent possible models. And also, towards designating a set of *assert changes* as a semantic transition, some studies related to *assertion change* in [18, 11, 1], are compliant with the strategy of minimal change(the change should be as little as possible on a possible model)[22]. Respecting the application related to interactions of services, as mentioned in [21] and [17], the situation calculus and GOLOG are applied to formalize the dynamic aspects of Web services and describe their composition. In particular, Franz Baader, et. al. [1], integrate the *action* theory[21] with DLs to model invocations of services and present an approach to reasoning for composition. In [1], an atomic service is defined as an *action* that has a pre-condition and post-condition (a set of effects), described using the assertions of ontology changes. And, the common knowledge base is a set of possible states for the world. As a result, the *composability* of Web services is reduced into the consistency of a knowledge base in DLs. Furthermore, Franz Baader, et. al. [3], integrate action formalisms into a linear temporal description logics and discuss the computational complexity of satisfiability of executability and projection under unconditional or conditional actions, with or without occlusions. Therefore, following the vein above, we propose to use an *assert change*-based formalism to model interactions of Web services and reason for the verification of temporal properties, such as *authenticity*, in the ontological layer.

For convenience, we only concern the case interactions of atomic services and simplify an *action* with removing pre-conditions and occlusions. In this paper, we propose an OWL-based Past-Linear Temporal Logic (Past-LTL) to formulate temporal properties along a sequence of ontology changes (caused by a sequence of the execution of atomic services), and present the refined method reasoning for the validity of the formulae in an interaction protocol from the semantic layer. As a result, we present a Past-LTL formulae to formally describe *authenticity* in an interaction protocol of Web services.

In the paper, the rest is organized as follows: Section 2 presents Past-LTL and a skeleton of the reduction approach. In Section 3, we express the authenticity in an interacting protocol as a Past-LTL formula. Finally, we present the related works in Section 4 and give some conclusions in Section 5.

## 2 OWL Ontology based Past-LTL and Reasoning

### 2.1 The $\mathcal{ALCQIO}$ *fragment* of OWL

With the consideration on the decidability for ontology-based context reasoning, it is necessary to limit the expressive capability of OWL and use a fragment of that to implement context reasoning. In DLs, $\mathcal{ALCQIO}$(that is based on $\mathcal{ALC}$[4]), allows for these constructors including Negation, Conjunction, Disjunction, Existential and Universal restrictions, Qualified number restriction($\mathcal{Q}$), Inverse role($\mathcal{I}$), and Nominal($\mathcal{O}$)[2]. For conveniens, the subset of the OWL corresponding to $\mathcal{ALCQIO}$ is so-called the $\mathcal{ALCQIO}$ $fragment$ ($fragment$) in this paper. Furthermore, for presenting semantics in the $fragment$, we take the direct model-theoretic semantics in OWL 2[5] and simplify those for the $fragment$. Namely, given a 4-tuple $< \Delta_I, \cdot^C, \cdot^{OP}, \cdot^I >$ as an interpretation $I$ , in which $\Delta_I$ is a non-empty set of object domains and $\cdot^C$ is a mapping to assign a subset $C^C$ of $\Delta_I$ to each class $C$, $\cdot^{OP}$ is a mapping to assign a subset $r^{OP}$ of $\Delta_I \times \Delta_I$ to each object property $r$, and $\cdot^I$ is a mapping to assign a subset $a^I$ of $\Delta_I$ to each individual $a$. Without confusion, an atomic class $A$, or a class $C$, or an object property $r$, or an individual $a$ with a superscript $I$ is as the abbreviation of the result set $A^I$, or $C^I$, or $r^I$, or $a^I$ through the corresponding mappings in the model $I$. And also, we call an interpretation $I$ as a model such that $I$ satisfies an ontology $O$ if all of conditions resulted from each axiom in $O$ are satisfied by $I$, noted with $I \models O$($I$ possibly with subscription to indicate a time point.). One of the most important relationships between two ontologies is the entailment. Namely, let $O_1$ and $O_2$ be two ontologies, $O_1$ entails $O_2$, noted with $O_1 \models O_2$, such that for every interpretation $I$, $I \models O_1$ implies $I \models O_2$ . Likewise, let $\varphi$ be an $fragment$ axiom, then $O_1 \models O_2$ if and only if for every $\varphi \in O_2$, $O_1 \models \varphi$. In a $fragment$ ontology, every class expression is restricted to contain only a simple object property. So that, the inference, e.g. the ontology entailment, is decidable.

## 2.2 Conceptualizing Assertion Change

For formalizing an interaction protocol, we present a concept $assertion\ change(AC)$ that describes a change from a source $fragment$ ontology into another.

**Definition 1.** *(Assertion Change) The assertion change is a set $\alpha$ of atomic assertions (e.g. class assertion, object property assertion, and negative object property assertion axioms) that describe a change on a $fragment$ ontology.*

Supposed that we follow the constant domain assumption, (namely, all interpretations share the same set of individuals within a common domain, let $I_1$ and $I_2$ be the different models for a $fragment$ ontology, then $domain((\cdot^I)_{I_1}) = domain((\cdot^I)_{I_2})$.), we present Def.2 to express a transition from one model to another.

**Definition 2.** *(AC-Labelled Transition) Let $\alpha$ be AC that puts effect on a model $I_1$ w.r.t a $fragment$ ontology $O$, and products another model $I_2$, and $A$ be an atomic class, and $r$ be an object property. We call that an $AC-labelled$*

[4] The prototypical Description Logics Attributive Concept Language with Complements is the basis of many expressive Description Logics.

[5] http://www.w3.org/TR/2009/REC-owl2-direct-semantics-20091027/

*transition(ALT) noted with $I_1 {\rightarrow}_{\alpha} I_2$, such that the semantic of $I_1 {\rightarrow}_{\alpha} I_2$ is inductively defined through (1) and (2) for classes and object properties in $O$.*

$$A^{I_2} = (A^{I_1} \cup \{a^{I_1} | a : A \in \alpha\} \backslash \{b^{I_1} | b : \neg A \in \alpha\}) \tag{1}$$

$$r^{I_2} = (r^{I_1} \cup \{(a^{I_1}, b^{I_1}) | (a, b) : r \in \alpha\} \backslash \{(c^{I_1}, d^{I_1}) | (c, d) : \neg r \in \alpha\}) \tag{2}$$

And, according to Def.2 above, we propose another definition *ALT path* as the following:

**Definition 3.** *(ALT Path) The ALT Path(path) is defined as a sequence $\rho$ of $AC-labelled$ transitions, noted with follows: ( Note that a subscription $i$ indicates the order in $\rho$.)*

$$\rho = \begin{cases} I_0, i = 0, \\ I_0 \rightarrow_{\alpha_1} I_1 \rightarrow_{\alpha_2} \ldots \rightarrow_{\alpha_i} I_i, i \geq 0. \end{cases} \tag{3}$$

*Given a path $\rho$ and $0 \leq i \leq \#\rho$, let $\alpha = f_{AC}(\rho, i)$ be a function to obtain an AC $\alpha$ at the position $i$ in $\rho$.*

Furthermore, through combining some past temporal operators with assertions in a *fragment* ontology, we could obtain Past-LTL formulae as defined in Def.4. And, each of the past temporal operators, such as $Y$(Yesterday), and $U^-$( until in history), only appears in front of an assertion.

**Definition 4.** *(Past-LTL Formula) Given a $fragment$ ontology $O$, a Past-LTL formula is inductively defined as follows:*

1. *$Forevery \varphi \in O$, $\varphi$ is a Past-LTL formula.*
2. *If either of $\varphi$ and $\psi$ is a Past-LTL formula, then $\varphi \wedge \psi$,$\varphi \vee \psi$, $Y\varphi$, and $\varphi U^- \psi$, are also Past-LTL formulae.*

Then, as to a Past-LTL formula, back along a *path*, the validity is defined as follows:

**Definition 5.** *(Validity along a path) Given a Past-LTL formula $\varphi$ and a path $\rho$ from an initial $fragment$ ontology $O$, the validity of a Past-LTL formula $\varphi$, back from a time point $i$ along $\rho$, noted with $(\rho, i) \models \varphi$, is inductively defined as follows:*
*$(\rho, i) \models \varphi$, iff for the interpretation $I_i$, $I_i \models \varphi$ and $\varphi$ is an assertion axiom;*
*$(\rho, i) \models \varphi \wedge \psi$, iff $(\rho, i) \models \varphi$ and $(\rho, i) \models \psi$;*
*$(\rho, i) \models \varphi \vee \psi$, iff $(\rho, i) \models \varphi$ or $(\rho, i) \models \psi$;*
*$(\rho, i) \models \neg\varphi$, iff $(\rho, i) \not\models \varphi$;*
*$(\rho, i) \models Y\varphi$, iff $(\rho, i-1) \models \varphi, i > 0$; Otherwise, false;*
*$(\rho, i) \models \varphi U^- \psi$, iff $\exists k\ 0 \leq k \leq i, (\rho, k) \models \psi$, implies $\forall j\ k \leq j \leq i$, $(\rho, j) \models \varphi$;*

Each interpretation in a *path* can be one of the possible worlds as similar as in first order logics. So, a Past-LTL formula can be used to express some temporal properties for a sequence of behaviors that change the possible world.

### 2.3 Reducing

We refine the reducing method in [4, 3] and propose an OWL-based approach for validating a Past-LTL formula $\varphi$ along a *path* $\rho$ from a $fragment$ ontology $O$. Supposed that each Past-LTL formula $\varphi$ has been the Negative Normal Form, $\Xi$ stands for a triple $< O,\ \rho,\ \varphi >$ as an input that consists of a $fragment$ ontology $O$ , a *path* $\rho$, and a Past-LTL formula $\varphi$. Let $Sub$ be a set of all class expressions occurring in $\Xi$, and $\Lambda$ a set of assertion axioms in $O$. And, $A$, $r$, and $T$ is an atomic class expression (an named class), an object property or a negative object property expression, and a class expression for an $AC$, respectively. Syntactically, either of names and expressions is possibly with a subscript that indicates a time point $i$ or $k$ with $0 \leq k \leq i$ in a *path*; and, it is also with a superscript that indicates which constructor the conceptualization is related to. For example, given the classes $C$ and $D$, $T_k^{C \sqcup D}$ stands for the reduced class from the class $C \sqcup D$.

Following the strategy in [22], changes between two interpretations should be little as possible while still satisfying all post-conditions. Intuitively, respecting the time point $i$, the minimization of changes on named elements can be described in a direct way through $\Lambda_i^{red}$, while the minimization of changes on unnamed elements is achieved through a suitable encoding of $T$ in $\Gamma_i^{red}$. As mentioned in [1], since the interpretation of a defined class is uniquely determined by the interpretation of an atomic class and role names, it is sufficient to impose this minimization of change condition on named classes and roles.

Given a time point $i$ in a *path* for the input $\Xi$, the reducing skeleton is as the following steps:

1. Due to the meaning of $ALT$ in Def.2, we can define a set $\Gamma_i^{red}$ of some equivalent class axioms to conceptualize the minimization of changes on individuals, classes, and axioms at each transition in $\rho$ from $O$.
2. In a *path* $\rho$, the changes on the named objects will be guaranteed by a set $\Lambda_i^{red}$ of the reduced assertions that consists of the initial assertions, the $AC$ assertions in $\rho$ , and the preserving assertions;
3. The Past-LTL formula $\varphi$ will be transformed into a set $\partial$ of sets of assertion axioms by a set of reducing tableaux rules;
4. Finally, $\varphi$ is valid such that $\exists \Lambda_i^{\varphi}, \Lambda_i^{\varphi} \in \partial, \Gamma_i^{red} \sqcup \Lambda_i^{red} \models \Lambda_i^{\varphi}$;

As shown in (4)[4], $\Gamma_i^N$ is defined as a set that contains a single equivalence class axiom for a named class $N$ and a conjunction of all nominal classes, in which, $n$ stands for the size of the set of nominal classes $a_j$ for an input $\Xi$. Furthermore, $T_k^A$ in (5) stands for the equivalent class to the interception of the atomic class $A$ after the $k^{th}$ transition. As shown in the right side of the formula (5)[4], the $unionOf$ $\sqcup$ constructor connects two parts: the first, expressing named elements and the second, expressing the unnamed elements. For same reason, the equivalent class to the interception of each named class, such as $T_k^{C \sqcup D}$, $T_k^{C \sqcap D}$, $T_k^{\neg C}$, $T_k^{\exists r.C}$, $T_k^{\forall r.C}$,$T_k^{\geq nr.C}$, and $T_k^{\leq nr.C}$ in $Sub$ can be inductively defined by the semantics of constructors(details in [1]). Finally, we can get a set $\Gamma_k^{Sub}$ of equivalent class axioms. In addition, as shown in (6), besides the axioms reduced from nominal and $AC$, $\mathit{\Gamma}_i^{red}$ also contains others axioms reduced from initial equivalent class axioms in $O$, and the object property domain and range axioms w.r.t $\mathit{\Xi}$.

$$\mathit{\Gamma}_i^N = \{N \equiv \bigsqcup_{0 \le j \le n} \{a_j\}\} \tag{4}$$

$$T_k^A \equiv (N \sqcap A_k) \sqcup (\neg N \sqcap A_0), A \in Sub, \tag{5}$$

$$\begin{aligned} \mathit{\Gamma}_i^{red} = \mathit{\Gamma}_i^N \sqcup ( \bigsqcup_{0 \le k \le i} (&\mathit{\Gamma}_k^{Sub} \sqcup \{T_k^A \equiv T_k^E | (A \equiv E) \in O\} \\ &\sqcup \{Domain(r_k, T_k^C) | Domain(r, C) \in O\} \\ &\sqcup \{Range(r_k, T_k^C) | Range(r, C) \in O\})) \end{aligned} \tag{6}$$

In this paper, we only discuss the case adding new assertions(possibly a negative object property). And also, with the addition of domain and range axioms, our approach avoids producing too many reduced assertions to affect the availability.

Given an input $\mathit{\Xi}$, with reducing each of class expressions, we also need to reduce the assertions related. For all assertions w.r.t $\mathit{\Xi}$, at a time point $i$ or after a transition, each class expression occurring within a class assertion or object property axiom should be replaced with the reduced one. Let $\varphi$ be a class assertion $a : C$, or an object property assertion $a, b : r$, or a negative object property assertion $a, b : \neg r$ , then the reduced one, as shown in (7), be $\varphi_i$, or $a, b : r_i$ , or $a, b : \neg r_i$ at time point $i$, respectively.

$$\varphi_i = \begin{cases} a : T_i^C), & \text{if } \varphi = a : C \\ (a, b) : r_i, & \text{if } \varphi = a, b : r \\ (a, b) : \neg r_i, & \text{if } \varphi = a, b : \neg r \end{cases} \tag{7}$$

Given $\mathit{\Lambda}$ as an initial set of all assertions w.r.t $\mathit{\Xi}$, $\mathit{\Lambda}^{ini}$ is a set of the results through (8).

$$\mathit{\Lambda}^{init} = \{\varphi_0 | \varphi \in \mathit{\Lambda}\} \tag{8}$$

So, the set $\mathit{\Lambda}_i^{red}$ of reduced assertions is defined inductively as follows(9 - 14):

$$\mathit{\Lambda}_0^A = \mathit{\Lambda}_0^{\neg A} = \mathit{\Lambda}_0^r = \mathit{\Lambda}_0^{\neg r} = \mathit{\Lambda}^{init} \tag{9}$$

$$\begin{aligned} \mathit{\Lambda}_k^A = &\mathit{\Lambda}_{k-1}^A \cup \{a : A_{k-1} \rightarrow A_k | a \in N_I, \text{ and } a : A_{k-1} \in \mathit{\Lambda}_{k-1}^A\} \\ &\cup \{a : A_k | a : A \in f_{AC}(\rho, k)\}, \text{ if } 1 \le k \le i. \end{aligned} \tag{10}$$

$$\begin{aligned} \mathit{\Lambda}_k^{\neg A} = &\mathit{\Lambda}_{k-1}^{\neg A} \cup \{a : \neg A_{k-1} \rightarrow \neg A_k | a \in N_I, \text{ and} \\ &a : \neg A_{k-1} \in \mathit{\Lambda}_{k-1}^{\neg A}\} \cup \{a : \neg A_k | a : \neg A \in f_{AC}(\rho, k)\}, \text{ if } 1 \le k \le i. \end{aligned} \tag{11}$$

$$\begin{aligned}\varLambda_k^r =&\varLambda_{k-1}^r \cup \{a : (\exists r_{k-1}\{b\} \rightarrow \exists r_k.\{b\})|a, b \in N_I, \text{ and } (a, b : r_{k-1}) \in \varLambda_{k-1}^r\} \\ &\cup \{a, b : r_k|a, b : r \in f_{AC}(\rho, k)\}, \text{ if } 1 \leq k \leq i.\end{aligned} \tag{12}$$

$$\begin{aligned}\varLambda_k^{\neg r} =&\varLambda_{k-1}^{\neg r} \cup \{a : (\forall r_{k-1}\neg\{b\} \rightarrow \forall r_k.\neg\{b\})|a, b \in N_I, \text{ and } (a, b : \neg r_{k-1}) \in \varLambda_{k-1}^{\neg r}\} \\ &\cup \{a, b : \neg r_k|a, b : \neg r \in f_{AC}(\rho, k)\}, \text{ if } 1 \leq k \leq i.\end{aligned} \tag{13}$$

$$\varLambda_{red} = \varLambda_i^A \cup \varLambda_i^{\neg A} \cup \varLambda_i^r \cup \varLambda_i^{\neg r} \tag{14}$$

As to a Past-LTL formula $\varphi$, through a tableaux approach refereing to that in [3], $\varphi$ is unfolded into a set $\varLambda_i^\varphi$ of assertions w.r.t $\varXi$. In the tableaux rules (15-18), $\partial$ is a set of sets of Past-LTL formulae with an initial status $\partial = \{\{\varphi_i\}\}, \varphi_0 = \varphi$. In $\vee Rule$, the set $\beta'$ and $\beta''$ is defined in (19-20) And, in $U^- Rule$, $\varOmega_k$ is defined as (21).

$$\frac{\varLambda \in \partial \wedge (\varphi \wedge \phi)_i \in \varLambda}{\varLambda := (\varLambda \backslash \{(\varphi \wedge \phi)_i\}) \cup \{\varphi_i, \phi_i\}} \wedge Rule \tag{15}$$

$$\frac{\varLambda \in \partial \wedge (\varphi \vee \phi)_i \in \varLambda}{\partial := (\partial \backslash \{\varLambda\}) \cup \{\varOmega', \varOmega''\}} \vee Rule \tag{16}$$

$$\frac{\varLambda \in \partial \wedge (Y\varphi)_i \in \varLambda,\ 0 \leq i \leq \#\rho}{\varLambda := (\varLambda \backslash \{(Y\varphi)_i\}) \cup \{\varphi_{i-1}\}} YRule \tag{17}$$

$$\frac{\varLambda \in \partial \wedge (\varphi U^- \phi)_i \in \varLambda,\ 0 \leq i \leq \#\rho}{\partial := (\partial \backslash \{\varLambda\}) \cup \{\varOmega_i, \varOmega_{i-1}, \ldots, \varOmega_0\}} U^- Rule \tag{18}$$

$$\varOmega^{'} = (\varLambda \backslash \{(\varphi \vee \phi)_i\}) \cup \{\varphi_i\} \tag{19}$$

$$\varOmega^{''} = (\varLambda \backslash \{(\varphi \vee \phi)_i\}) \cup \{\phi_i\} \tag{20}$$

$$\varOmega_k = (\varLambda \backslash \{(\varphi U^- \phi)_i\}) \cup \{\varphi_i, \varphi_{i-1}, \ldots, \phi_{i-k},\ 0 \leq k \leq\ i\} \tag{21}$$

Finally, The rules above are applied exhaustively on $\partial$ to get rid of any temporal operator in $\varphi$. And, we can take a set $\varLambda_i^\varphi$ from $\partial$, which should be as candidates to check the entailment relationship with the reduced ontology $\varGamma_i^{red} \cup \varLambda_i^{red}$.

**Theorem 1.** *Let $\varXi$ be an input as a triple ($O$, $\rho$, $\varphi$) and $O$, $\rho$, and $\varphi$, be an initial fragment ontology, a path, and a Past-LTL formula, respectively. Then, given a time point $i$ in $\rho$, through (4-5), $\varGamma_i^{red}$ is obtained as a set of reduced defining axioms; and through (9-14), $\varLambda_i^{red}$ as a set of reduced asserting axioms. Likewise, through (15-18) w.r.t $\varXi$, $\partial$ is obtained as a set of sets of assertions for $\varphi$. Then, $(\rho, i) \models \varphi$ if and only if $\varGamma_i^{red} \cup \varLambda_i^{red}$ is consistent and $\exists \varLambda_i^\varphi \in \partial$, $\varGamma_i^{red} \cup \varLambda_i^{red} \models \varLambda_i^\varphi$.*

**Table 1.** Conceptualizing Authentication Events in *Fragment*

| *Fragment* | Abbreviation | Statement |
|---|---|---|
| :Role | $C^R$ | a participant. |
| :Session | $C^S$ | a session. |
| :Nonce | $C^N$ | random value. |
| :Begin(End)Init | $C^{BI}$ | begin or end in an initiator. |
| :RunInit | $C^{RI}$ | run an authentication in an initiator. |
| :Begin(End)Response | $C^{BR}$ | begin or end in a responser. |
| :RunResponse | $C^{RR}$ | run an authentication in a responser. |
| :who | $r^w$ | range over participants. |
| :session | $r^s$ | range over sessions. |
| :nonce | $r^n$ | range over random value. |
| :parter | $r^p$ | range over participants. |

In summary, the validity of a Past-LTL formula w.r.t the input is transformed into the problem checking the entailment relationship between two OWL ontologies (two sets of axioms). Since our approach is based on the $\mathcal{ALCQIO}$ fragment of OWL and is approximatively the $\mathcal{ALCQIO}$-case under unconditional actions without occlusions in [3], the whole commotional complexity is NExpTime for the Lemma.12 in [3].

## 3 Authenticity in Past-LTL

The authenticity is an essential property for interacting protocols always as a temporal property [23, 5, 8]. So, we represent the property related to the authenticity in Past-LTL. Usually, the correspondence or non-injection in the authentication is expressed in a temporal logic based on such events, e.g. beginning an initial request, ending an initial request, etc[8]. So, we follow it but express them as a Past-LTL formula in a *fragment*, so as to conceptualize each event occurring in an authentication procedure. There are six events $C^{BI}$, $C^{RI}$, $C^{EI}$, $C^{BR}$, $C^{RR}$, and $C^{ER}$ in Tab.1 with other classes and object properties related. And, as to (22), we can obtain the concrete event assertion only if each $E$ is substituted by one of $C^{BI}$, $C^{RI}$, $C^{EI}$, $C^{BR}$, $C^{RR}$, and $C^{ER}$.

$$\begin{aligned} e : E(i, p, s, n) \doteq &((e : E) \wedge (e, i : r^w) \wedge (p : r^p) \cdot \wedge (s : r^s) \wedge (e, n : r^n) \cdot \\ &\wedge (i : C^R) \wedge (p : C^R) \cdot \wedge (s : C^S) \wedge (n : C^N) \end{aligned} \tag{22}$$

Given a collection of individual variables $a$, $b$, $s$, and $n$ and two event individuals $e_0$, $e_1$, a Past-LTL formula (23) with a universal quantification $\forall(a : C^R, b : C^R, s : C^S, n : C^N)$, represents the authenticity within an interacting protocol.

(Note that $\odot$ is the 'Once' operator and $\odot\varphi$ is as $(\top U^{-}\varphi)$, and $\phi \rightarrow \varphi$ is as $\neg\phi \vee \varphi$.)

$$\begin{aligned}&\forall(a : C^R, b : C^R, s : C^S, n : C^N) \cdot (e_0 : C^{ER}(b, a, s, n) \rightarrow \\ &\quad \odot\, (e_1 : C^{RI}(a, b, s, n)))\end{aligned} \tag{23}$$

As a result, given an abbreviated Past-LTL formula $\forall\nu\delta$ as (23) and an *input* $\Xi$, the authenticity is hold in $\rho$ such that for every instantiation of the individual variables $a$, $b$, $s$, and $n$, $\rho \models \delta$ w.r.t $\Xi$. (Note that $\rho \models$ is the abbreviation of $(\rho, \#\rho) \models$.)

## 4 Related Works

As the foundation of reasoning under a dynamic and open environment(with incomplete knowledge of the world), the research about *Ontology Change* has widely carried out[10] in recent years. Specially, many works fucus on update of assertive axioms, or update in the instance level of ontology. In [13], the authors present an algorithm for updating completion graphs under both the addition and removal of ABox assertions. On the contrary, both [12] and [18] adopt a semantic notion of update and erasure. In [12], erasure is studied for RDF, under the same semantics we use in the present paper, namely the Katsuno-Mendelson semantics [15]. In [4, 18], the authors propose a formal semantics for updates in DLs, and present interesting results on various aspects related to computing updates. In [11], authors introduce DL-$Lite_{\mathcal{FS}}$ that minimally extends DL-$Lite_{\mathcal{F}}$ and is closed with respect to instance-level update, and also present a polynomial algorithm for computing instance-level update in this logic. In this paper, we are inspired mainly by the reducing method in [4, 18] and refine it for the validation of the Past-LTL formulae.

Respecting the security verification for Web services, in [6], authors propose a specification language $TulaFale$ for writing machine-checkable descriptions of SOAP-based security protocols and their properties, which can be complied into the applied pi calculus, and be verified using Blanchet's resolution-based protocol verifier. Moreover, authors in [16] propose a method for mapping interacting messages to abstract symbols in the style of Dolev-Yao, and Casper notation and formally analyze WS-Security and WS-Secure Conversation. While these approaches mainly consider how to specify, model and verify security of SOAP-based interactions between Web services, our approach is such a solution in an ontology-based semantic layer that be more suitable for open environment.

For the security aspects of composing services, Barbara Carminati et al put efforts on security constraint-based Web services composition [7]. Moreover, Lalana Kagal et al present some ontology of policy language and a distributed solution for policy management to enhance the traditional identification and access control framework so as to realize the dynamic and non-center management[14]. Although these works discuss the enforcement of ontology-based security policies within a dynamic context, such as the composition of services, the reasoning mechanism is limited to check the satisfaction of static security properties since the absence of semantics of interactions (actions).

## 5 Conclusions and Future Works

With the help of the action theory and OWL, we can formalize a sequence of *state changes* caused by the invocations of atomic Semantic Web services and check the salification of temporal properties under incomplete knowledge of world. In particular, Authenticity as a concrete temporal property, has been expressed as an OWL-base Past-LTL formula. According to the approach, the validity of temporal properties in an interaction protocol has been reduced into obtaining an entailment relationship, namely, detecting whether a set of the axioms reduced from a *path* entails the one unfolded from the Past-LTL formula for the temporal properties. For more clarity, some algorithms has been proposed for reducing a *path* and unfolding a Past-LTL based on the result of the former. As a concrete application, we have represented the mechanism marking events in a $fragment$ for checking the non-injective agreement and reduce the authenticating procedure into a *path*. As a result, verifying the authenticity in an interacting protocol has been reduced into the validity of a Past-LTL formula in a *path*.

Since the result is archived on only concerning atomic services, we will extend the approach into the application of complex services. In this case, more control constructors, such as choice and iteration, will be considered and need to enhance the reducing method. Moreover, we plan to use more simple fragment of OWL to semantically describe the interactions of Web services, such as OWL-Lite, so as to promote the performance of checking the entailment relationship of reduced ontologies.

## References

1. Baader, F., Lutz, C., Milicic, M., Sattler, U., Wolter, F.: A description logic based approach to reasoning about web services. In: The WWW 2005 Workshop on Web Service Semantics (WSS2005). Chiba City, Japan (2005)
2. Baader, F.: Description logics. In: 5th International Summer School on Reasoning Web: Semantic Technologies for Information Systems, August 30, 2009 - September 4, 2009. vol. 5689 LNCS, pp. 1–39. Theoretical Computer Science, TU Dresden, Germany, Springer Verlag, Brixen-Bressanone, Italy (2009)
3. Baader, F., Liu, H., ul Mehdi, A.: Integrate Action Formalisms into Linear Temporal Description Logics. LTCS-Report LTCS-09-03, Chair for Automata Theory, Institute for Theoretical Computer Science, Dresden University of Technology, Germany (2009), see http://lat.inf.tu-dresden.de/research/reports.html.
4. Baader, F., Lutz, C., Milicic, M., Sattler, U., Wolter, F.: Integrating description logics and action formalisms: First results. In: 20th National Conference on Artificial Intelligence and the 17th Innovative Applications of Artificial Intelligence Conference, AAAI-05/IAAI-05, July 9, 2005 - July 13, 2005. vol. 2, pp. 572–577. American Association for Artificial Intelligence (2005)

5. Bhargavan, K., Fournet, C., Gordon, A.D.: A semantics for web services authentication. In: POPL 2004: 31st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, 14-16 Jan. 2004. vol. 39, pp. 198–209. Microsoft Res., Cambridge, UK, ACM, USA (01 2004)
6. Bhargavan, K., Fournet, C., Gordon, A.D., Pucella, R.: Tulafale: A security tool for web services. In: International Symposium on Formal Methods for Components and Objects (FMCO' 03), Volume 3188 of LNCS. pp. 197–222. Springer (2004)
7. Carminati, B., Ferrari, E., Bishop, R., Hung, P.C.K.: Security conscious web service composition. In: 4th IEEE International Conference on Web Services (ICWS. pp. 489–496. IEEE Computer Society (2006)
8. Corin, R., Saptawijaya, A.: A logic for constraint-based security protocol analysis. In: 2006 IEEE Symposium on Security and Privacy, 21-24 May 2006. p. 14. Twente Univ., Netherlands, IEEE Comput. Soc, Los Alamitos, CA, USA (2006)
9. FLOURIS, G., MANAKANATAS, D., KONDYLAKIS, H., PLEXOUSAKIS, D., ANTONIOU, G.: Ontology change: classification and survey. The Knowledge Engineering Review 23, 2 pp. 117–152 (2008)
10. Flouris, G., Plexousakis, D., Antoniou, G.: A classification of ontology change. In: In Proc. of the 3rd Italian Semantic Web Workshop: Semantic Web Applications and Perspectives (SWAP 2006) (2006)
11. Giacomo, G.D., Lenzerini, M., Poggi, A., Rosati, R.: On instance-level update and erasure in description logic ontologies. Journal of Logic and Computation 19(5), 745–770 (2009)
12. Gutierrez, C., Hurtado, C., Vaisman, A.: The meaning of erasing in rdf under the katsuno-mendelzon approach. In: In Proc. of the 9th Int. Workshop on the Web and Databases (WebDB 2006) (2006)
13. Halaschek-Wiener, C., Parsia, B., Sirin, E., Kalyanpur, A.: Description logic reasoning for dynamic aboxes. In: In Proc. of the 2006 Description Logic Workshop (DL 2006). vol. 189 (2006)
14. Kagal, L., Finin, T., Joshi, A.: A policy based approach to security for the semantic web. In: The SemanticWeb - ISWC 2003. pp. 402–418. Springer Berlin (2003)
15. Katsuno, H., Mendelzon, A.O.: On the difference between updating a knowledge base and revising it. pp. 387–394. Morgan Kaufmann
16. Kleiner, E., Roscoe, A.W.: On the relationship between web services security and traditional protocols. In: Mathematical Foundations of Programming Semantics (MFPS XXI (2005)
17. Levesque, H., Reiter, R., Lesperance, Y., Lin, F., Scherl, R.: Golog: a logic programming language for dynamic domains. Journal of Logic Programming 31(1-3), 59 – 83 (1997/04/)
18. Liu, H., Lutz, C., Milicic, M., Wolter, F.: Updating description logic aboxes. In: In International Conference of Principles of Knowledge Representation and Reasoning(KR. pp. 46–56 (2006)
19. Lowe, G.: An attack on the needham-schroeder public-key authentication protocol. Information Processing Letters 56(3), 131 – 3 (1995/11/10)
20. Meadows, C.A.: Formal verification of cryptographic protocols: A survey. pp. 133–150. Springer-Verlag (1995)
21. Reiter, R.: Knowledge in Action. MIT Press (2001)
22. Winslett, M.: Reasoning about action using a possible models approach UIUCDCS-R-88-1428, 17 – (1988/05/)
23. Woo, T.Y.C., Lam, S.S.: A semantic model for authentication protocols. In: IEEE Symposium on Research in Security and Privacy, 24-26 May 1993. pp. 178–194.

Dept. of Comput. Sci., Texas Univ., Austin, TX, USA, IEEE Comput. Soc. Press, Los Alamitos, CA, USA (1993)

24. Ye, X., Liao, L.: Security of composed interaction for web services. Journal of Software 4(10), 1160–1168 (2009)