Soft Comput (2018) 22:751–757
https://doi.org/10.1007/s00500-017-2497-7

FOUNDATIONS

Deontic STIT logic, from logical paradox to security policy

Lirong Qiu[1] · **Xin Sun**[2,3]

Published online: 24 January 2017

Abstract A deontic STIT logic is studied in this paper with the possible application of specifying security policies for intrude detection in the pervasive computing environment. Compared to the existing deontic STIT logics, an advantage of our logic is that it is capable of solving the miners paradox, a logical paradox which recently grabs attentions of logicians, philosophers, linguistists and computer scientists. A complete and sound axiomatization of our logic is developed.

Keywords Deontic logic · Miners paradox · Security policy

1 Introduction

Our ultimate goal in this article is to develop a logic to formalize security policies, especially for intrude detection in pervasive computing environments. Security is a high priority requirement for lots of information systems, and it is considered in practice as a more and more significant issue. In most systems, security requirements may already exist but usually remain informal, and starting from these requirements it is of growing interest to be able to define a rigorous security policy.

In pervasive computing environments, resources like information and services are accessible anywhere and anytime via any devices (Barolli and Takizawa 2010; Marcelloni et al. 2014; Ogiela et al. 2014; Ramos et al. 2014; Choi et al. 2014). There are different sorts of users and services, and some of them may be unknown or not predefined (Kagal et al. 2001). The distribution of resources in these environments forces us to leverage decentralized security management. In this setting, the environment is divided into a number of domains based on different factors. For each domain, there is a security agent with an administrator (we call it authority) who is responsible for preserving the security of resources that are under their protection.

Several authors have used *deontic logic* to specify security policies (Glasgow et al. 1992; Jones and Sergot 1992; Demolombe and Jones 1996; Cuppens-Boulahia and Cuppens 2008; Cuppens et al. 2013). These authors outlined the main features of this formalism to analyze further various aspects of security, to formalize previously informal security requirements and to provide a flexible and expressive language for specifying security properties. Deontic logic is a formal study of norms and deontic modalities (such as permission, forbidden and obligation). In 1951, the publication of von Wright (1951) indicates the birth of deontic logic. With the work of Meyer (1988), deontic logic became a part of computer science. Deontic logic has been a valuable tool in the specification and reasoning of security policies because key notions in security such as permission, authorization, prohibition and obligation are exactly the subjects of deontic logic. To apply deontic logic in the specification of security policies in pervasive computing environments,

Communicated by A. Di Nola.

This paper is a revision of Sun and Baniasadi (2014).

✉ Xin Sun
xin_sun_logic@sina.com

Lirong Qiu
qiu_lirong@126.com

[1] Information Engineering School, Minzu University of China, Beijing, China

[2] Department of Foundations of Computer Science, Faculty of Philosophy, The John Paul II Catholic University of Lublin, Lublin, Poland

[3] Institute of Logic and Cognition, Sun Yat-sen University, Guangzhou, China

we need a deontic logic in which different authorities are explicitly modeled. Deontic STIT logic offers one option for this purpose. Deontic STIT logic (Horty 2001; Kooi and Tamminga 2008; Sun 2011; Broersen 2011), grounded on STIT (see to it that) theory (Belnap et al. 2001), is a branch of deontic logic developed by philosophers, logicians and computer scientists in recent years. In Kooi and Tamminga (2008) and Sun (2011), the authors develop deontic logics which are capable of models commands from different authorities.

Another reason for choosing deontic STIT logic comes from the motivation of the specification of policies of intrusion detection. Cuppens-Boulahia and Cuppens (2008) investigate the specification of intrusion detection policies. They argue that it is appropriate to use the *bring it about* modality for specification. Since the difference between *bring it about* and *see to it that* is negligible, deontic STIT logic can be an appropriate tool to specify policies of intrusion detection.

From a logical perspective, one limitation of the existing deontic STIT logic is that they are suffered from some logical paradoxes. This paper develops a new multi-authority deontic STIT logic (MADL) to overcome this problem such that our logic is more suitable for the application to security than the existing deontic STIT logics.

In the rest of this paper, we recap the miners paradox in Sect. 2 as a trigger of our further study. We then present our deontic STIT logic in Sect. 3. In Sect. 4 we discuss some related work. Section 5 summarizes this article with future work.

2 The miners paradox

In recent years, many deontic logicians get interested in the miners paradox (Gabbay et al. 2014). The miners paradox presented in Kolodny and MacFarlane (2010) is described like this:

> There are 10 miners trapped in either shaft A or shaft B, but we don't know which one. Water threatens to flood the shafts. We have sandbags to block only one shaft. If one shaft is blocked, all water will flood into the other shaft, killing all miners inside. If we block neither shaft, both will be flooded partially, killing 1 miner.

Since we don't know the miners' location, it seems plausible that:

(1) We should block neither shaft A nor shaft B.
However, the following also seems acceptable.
(2) We should block shaft A if the miners are in shaft A.
(3) We should block shaft B if the miners are in shaft B.
(4) The miners are either in shaft A or in shaft B.
And (2), (3) together with (4) imply that
(5) Either we should block shaft A or we should block shaft B.

Which contradicts to (1).

The deontic STIT logic proposed in Horty (2001), Kooi and Tamminga (2008), Sun (2011) cannot solve this paradox: Although the inference from (2)–(4) to (5) is not valid in the logic introduced in Sun (2011), both Horty (2001) and Sun (2011) are not capable of predicting (1). In this paper, we develop MADL, which is able to block the inference from (2)–(4) to (5) meanwhile predicts (1)–(4).

3 Deontic STIT logic

In deontic STIT logic, the semantics of deontic operator is interpreted by best choices, which are defined via a preference relation over sets of possible worlds. Such a relation is characterized by a preference relation over possible worlds through *lifting*. In the literature, there are many methods of lifting preference, which are summarized by Lang and van der Torre (2008) as follows:

- **strong lifting**: Let U_1 and U_2 be two sets of worlds, U_1 is strongly at least as good as U_2 iff $\forall w \in U_1, \forall v \in U_2$, w is at least as good as v.
- **optimistic lifting**: U_1 is optimistically at least as good as U_2 iff $\exists w \in U_1, \forall v \in U_2$, w is at least as good as v.
- **pessimistic lifting**: U_1 pessimistically at least as good as U_2 iff $\forall w \in U_1, \exists v \in U_2$, w is at least as good as v.

In utilitarian deontic logic (UDL) of Horty (2001), Kooi and Tamminga (2008), Sun (2011), strong lifting is used. According to strong lifting, the best choices in the miners paradox are *block_A*, *block_B* and *block_neither*. Therefore, "we ought to block neither" is false. To have a more precise understanding of such reasoning, we now formally review the UDL introduced in Sun (2011).

The language of utilitarian deontic logic, $\mathfrak{L}_{udl}$, is defined by the following BNF: Let $\Psi = \{p, q, r, \ldots\}$ be a set of propositional atoms and $Agent = \{1, \ldots, n\}$ be a set of agents,

$$\psi ::= p \mid \neg\psi \mid \psi \wedge \psi \mid \bigcirc_G \psi \mid \bigcirc_G(\psi/\psi) \mid [G]\psi$$

where $p \in \Psi, G \subseteq Agent$. Intuitively, $[G]\psi$ says that "group G sees to it that ψ." $\bigcirc_G \psi$ says that "G ought to see to it that ψ." $\bigcirc_G(\psi/\phi)$ says that "G ought to see to it that ψ under the condition ϕ." The semantics of UDL is defined via the notion of utilitarian models.

Definition 1 A utilitarian model $(W, V, Choice, \preceq)$ is a tuple where W is a set of possible worlds, V is a valuation function that maps every atom to a set of worlds, $\preceq$ is a transitive and reflexive relation over W, $Choice$ is a choice function. The function $Choice : 2^{Agent} \mapsto 2^{2^W}$ is based on the individual choice function $IndChoice$: $Agent \mapsto 2^{2^W}$. $IndChoice$ is required to satisfy the following conditions:

(1) $IndChoice(i)$ forms a partition of W, for every $i \in Agent$;
(2) given arbitrary $x_1 \in IndChoice(1), \ldots, x_n \in IndChoice(n)$ and $Agent = \{1, \ldots, n\}$, it holds that $x_1 \cap \cdots \cap x_n \neq \emptyset$;

A selection function τ: $Agent \mapsto 2^W$ is a function such that for all $i \in Agent$, it holds that $\tau(i) \in IndChoice(i)$. For $H \subseteq Agent$, if $H \neq \emptyset$, then we let $Choice(H) = \{\bigcap_{j \in H} \tau(j) : \tau \text{ is a selection function}\}$. If $H = \emptyset$, then $Choice(H) = \{W\}$.

We use $w \preceq v$ to represent that w is no better than v and $w \approx v$ as an abbreviation of $w \preceq v$ and $v \preceq w$.

Definition 2 (Sun (2011)) For $X, Y \subseteq W$, $X \preceq^s Y$ iff

(1) there are $u \in X$ and $u' \in Y$ such that $u \preceq u'$.
(2) for every $u \in X$, for every $u' \in Y$, $u \preceq u'$.

$X \prec^s Y$ is used to denote $X \preceq^s Y$ meanwhile $Y \not\preceq^s X$.

Definition 3 (Horty (2001)) Let $H \subseteq Agent$ and $T, T' \in Choice(H)$. $T \preceq^s_H T'$ iff for all $S \in Choice(Agent - H)$, $T \cap S \preceq^s T' \cap S$.

$T \preceq^s_H T'$ means that "T' weakly dominates T." From a perspective of decision theory, $T \preceq^s_H T'$ says that whatever other agents do, the result obtained by choosing T' is no worse than that of choosing T. $T \prec^s_H T'$ is short for $T \preceq^s_H T'$ and $T' \not\preceq^s_H T$. If $T \prec^s_H T'$, then we say T' strongly dominates T.

Definition 4 (Horty (2001)) Let H be a set of agents and Y a set of worlds.

$$Choice(H/Y) = \{T : T \in Choice(H) \text{ and } T \cap Y \neq \emptyset\}$$

Intuitively, $Choice(H/Y)$ are those choices made by group H which are consistent with Y.

Definition 5 (Sun (2011)) Let $T, T' \in Choice(H/Y)$.

$T \preceq^s_{H/Y} T'$ *iff for every* $S \in Choice((Agent - H)/(Y \cap (T \cup T')))$, $T \cap Y \cap S \preceq^s T' \cap Y \cap S$.

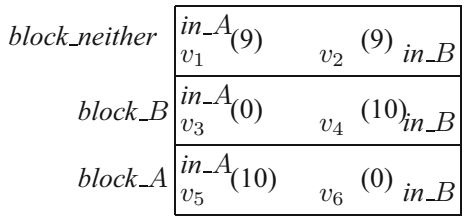

Fig. 1 $W = \{v_1, \ldots, v_6\}$, $v_3 \approx v_6 \preceq v_1 \approx v_2 \preceq v_4 \approx v_5$

$T \preceq^s_{H/Y} T'$ means that "T' weakly dominates T under the condition of Y." $T \prec^s_{H/Y} T'$, read as "T' strongly dominates T under the condition of Y," is short for $T \preceq^s_{H/Y} T'$ and $T' \not\preceq^s_{H/Y} T$.

Definition 6 (Horty (2001)) Let H be a set of agents,

- $Optimal^s_H = \{T \in Choice(H)$: there is no $T' \in Choice(H)$ such that $T \prec^s_H T'\}$.
- $Optimal^s_{H/Y} = \{T \in Choice(H/Y)$: there's no $T' \in Choice(H/Y)$ such that $T \prec^s_{H/Y} T'\}$.

Definition 7 (*Semantics of UDL*). Given a utilitarian model $M = (W, V, choice, \preceq)$ and $v \in W$,

$M, v \vDash p$	*iff* $v \in V(p)$;
$M, v \vDash \neg\psi$	*iff it does not hold that* $M, v \vDash \psi$;
$M, v \vDash \psi \wedge \phi$	*iff* $M, v \vDash \psi$ *and* $M, v \vDash \phi$;
$M, v \vDash [H]\psi$	*iff* $M, v' \vDash \psi$, *for all* $v' \in W$ *satisfying that there is* $T \in Choice(H)$ *such that* $\{v, v'\} \subseteq T$;
$M, v \vDash \bigcirc_H \psi$	*iff* $T \subseteq \|\|\psi\|\|$ *for every* $T \in Optimal^s_H$;
$M, v \vDash \bigcirc_H(\psi/\phi)$	*iff* $T \subseteq \|\|\psi\|\|$ *for every* $T \in Optimal^s_{H/\phi}$.

Here $\|\psi\| = \{v \in W : M, v \vDash \psi\}$.

The miners paradox is characterized by a model $Miners = (W, V, Choice, \preceq)$, $W = \{v_1, \ldots, v_6\}$, $Choice(H) = \{\{v_1, v_2\}, \{v_3, v_4\}, \{v_5, v_6\}\}$, $Choice(Agent - H) = \{W\}$, $v_3 \approx v_6 \preceq v_1 \approx v_2 \preceq v_4 \approx v_5$, $V(in\_A) = \{v_1, v_3, v_5\}$, $V(in\_B) = \{v_2, v_4, v_6\}$, $V(block\_A) = \{v_5, v_6\}$, $V(block\_B) = \{v_3, v_4\}$, $V(block\_neither) = \{v_1, v_2\}$ (Fig. 1).

Group H can choose *block_A*, *block_B* or *block_neither*, while other agents can only choose W. All the three choices of group H are optimal by the strong lifting. Therefore, $Miners, v_1 \nvDash \bigcirc_H(block\_neither)$. Therefore, UDL cannot solve the miners paradox.

3.1 Utilitarian deontic logic via pessimistic lifting

With the motivation of solving the miners paradox, we introduce a new logic called pessimistic utilitarian deontic logic

(PUDL), in which pessimistic lifting is used instead of strong lifting. We will show that PUDL not only solves the miners paradox but also solves Ross's paradox and the contrary to duty paradox. We then present an axiomatization for PUDL and generalize PUDL to MADL in the next subsection.

Informally, *block_neither* in the miners scenario is the only optimal choice according to the pessimistic lifting. Hence, "we ought to block neither" holds. Moreover, in PUDL both (2) and (3) are true, whereas the inference from (2)-(4) to (5) is invalid. Therefore, PUDL is capable of solving the miners paradox. Now, we present these arguments formally.

3.1.1 Language

The language $\mathfrak{L}_{pudl}$ is generated by the following BNF:

$$\psi ::= p \mid \neg\psi \mid \psi \wedge \psi \mid [i]\psi \mid [\preceq]\psi \mid [\prec]\psi \mid [\succeq]\psi \mid \Box\psi$$

Intuitively, $[i]\psi$ means that "agent i sees to it that ψ." $\Box\psi$ says that "ψ is true everywhere." $[\preceq]\psi$ express "ψ is weakly preferable" while $[\prec]\psi$ states that "ψ is strictly preferable." $[\succeq]\psi$ means that "ψ is unpreferable." $\langle\preceq\rangle$, $\langle\prec\rangle$ and $\Diamond$ are dual for $[\preceq]$, $[\prec]$ and $\Box$, respectively. The relation $\preceq$ must be reflexive, transitive and total, while $\prec$ must satisfy that $v \prec w$ iff $v \preceq w$ and $w \npreceq v$. Pessimistic lifting is defined in $\mathfrak{L}_{pudl}$ as follows:

- pessimistic lifting: $\psi \preceq^p \phi ::= \Box(\phi \Rightarrow \langle\succeq\rangle\psi)$. Informally, the formula $\Box(\phi \Rightarrow \langle\succeq\rangle\phi)$ says that every ϕ-world is weakly better than some ψ-world.

We use $\psi \prec^p \phi$ to denote $\neg(\phi \preceq^p \psi) \wedge (\psi \preceq^p \phi)$. Obligation in $\mathfrak{L}_{pudl}$ is characterized as follows:

- $\bigcirc_i\psi ::= (\neg\psi \prec^p [i]\psi) \wedge \Diamond[i]\psi$. That is to say, agent i ought to STIT ψ if and only if in the pessimistic sense STIT ψ is strictly better than $\neg\psi$ and it is possible for i to STIT ψ.
- $\bigcirc_i(\psi/\phi) ::= \Diamond[i]\psi \wedge ((\neg\psi \wedge \phi) \prec^p ([i]\phi \wedge \psi))$.

3.1.2 Semantics

We now introduce the semantics of PUDL.

Definition 8 A tuple $M = (W, \preceq, \prec, IndChoice, V)$ is a pessimistic utilitarian model if W and $IndChoice$ are the same as in the utilitarian model, $\preceq$ is a relation over W that represents the social welfare of all agents, $\preceq$ is reflexive, transitive and connected.[1] $\prec$ is a relation over W such that for every $v, v' \in W$, $v \prec v'$ iff $v' \npreceq v$ meanwhile $v \preceq v'$.

[1] $\preceq$ is connected if for all $v, v' \in W$, either $v \preceq v'$, or $v' \preceq v$.

Let R_i be a relation such that $(v, v') \in R_i$ if and only if there exists a $T \in IndChoice(i)$ with $\{v, v'\} \subseteq T$. The semantics of $\mathfrak{L}_{pudl}$ is defined as follows:

Definition 9 Given a pessimistic utilitarian model M and $v \in W$,

$M, v \vDash_{pudl} [i]\psi$ *iff* $M, u \vDash \psi$ *for every* u *with* $(v, u) \in R_i$;
$M, v \vDash_{pudl} [\preceq]\psi$ *iff* $M, u \vDash \psi$ *for every* u *with* $v \preceq u$;
$M, v \vDash_{pudl} [\succeq]\psi$ *iff* $M, u \vDash \psi$ *for every* u *with* $u \preceq v$;
$M, v \vDash_{pudl} [\prec]\psi$ *iff* $M, u \vDash \psi$ *for every* u *with* $v \prec u$;
$M, v \vDash_{pudl} \Box\psi$ *iff* $M, u \vDash \psi$ *for every* $u \in W$.

3.1.3 Solving the miners paradox

We formally describe the miners scenario by a pessimistic utilitarian model. Let $Miners^p = (W, IndChoice, \preceq, \prec, V)$ such that $W = \{v_1, \ldots, v_6\}$, $IndChoice(i) = \{\{v_1, v_2\}, \{v_3, v_4\}, \{v_5, v_6\}\}$, $IndChoice(j) = \{W\}$ for all $j \neq i$, $v_3 \approx v_6 \prec v_1 \approx v_2 \prec v_4 \approx v_5$, $V(in\_A) = \{v_1, v_3, v_5\}$, $V(in\_B) = \{v_2, v_4, v_6\}$, $V(block\_A) = \{v_5, v_6\}$, $V(block\_B) = \{v_3, v_4\}$, $V(block\_neither) = \{v_1, v_2\}$.

We know that $\neg block\_neither$ is strictly worse than $[i]block\_neither$ according to the pessimistic semantics. Therefore, $Miners^p, v_1 \vDash \bigcirc_i(block\_neither)$. Moreover, we have "if the miners are in A, then i ought to block A" because $\neg block\_A$ is worse than $[i]block\_A$, given the condition of miners being in A. Therefore, $Miners^p, v_1 \vDash \bigcirc_i(block\_A/in\_A)$. Similarly $Miners^p, v_1 \vDash \bigcirc_i(block\_B/in\_B)$. It remains to prove that even if "if the miners are in A, then we ought to block A" and "if the miners are in B, then we ought to block B" are both true, we do not infer that "we ought to block either A or B." The following proposition justifies such reasoning.

Proposition 1 $\nvDash_{pudl} \bigcirc_i(\phi/\psi) \wedge \bigcirc_i(\phi/\chi) \Rightarrow \bigcirc_i(\phi/(\psi \vee \chi))$.

3.1.4 Bonus 1: solving the contrary to duty paradox

The contrary to duty paradox is one of the most serious paradoxes in deontic logic. The best known example of this paradox is give by Chisholm (1963):

(1a) It ought to be that you go to the party;
(2a) It ought to be that if you go, then you tell them you are going;
(3a) If you don't go, you ought not to tell them you are going;
(4a) You do not go.

Intuitively, these four statements are consistent and independent of each other. But either the consistency or the independency is lost after they are translated to standard

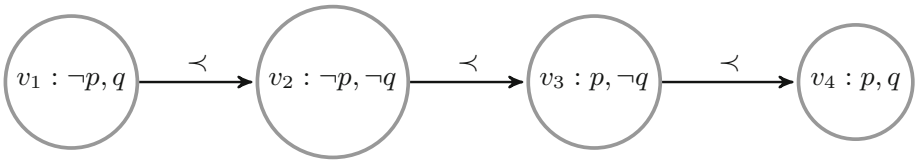

Fig. 2 Contrary to duty paradox

deontic logic. In our logic, fortunately, we survive form such predicament.

Let p represent "go to the party." Let q represent "tell them you are going." Then, we can formalize the four statements using our logic in the following way:

(a) $\bigcirc_i p$
(b) $\bigcirc_i (p \Rightarrow q)$
(c) $\bigcirc_i (\neg q / \neg p)$
(d) $\neg p$

It's not hard to see that the above four formulas are independent of each other. For consistency, consult the following example.

Example 1 Let $M = (W, V, IndChoice, \preceq, \prec)$, $W = \{v_1, \ldots, v_4\}$, $IndChoice(i) = \{\{v_1\}, \{v_2\}, \{v_3\}, \{v_4\}\}$, $v_1 \prec v_2 \prec v_3 \prec v_4$. $V(p) = \{v_3, v_4\}$, $V(q) = \{v_1, v_4\}$. See Fig. 2. In this model, we have all the four formulas $(a) - (d)$ are all true in v_1.

3.1.5 Bonus 2: solving Ross' paradox

Another well-known paradox in deontic logic is Ross' paradox Alfred (1941):

> Suppose John should send a letter. Since sending the letter implies sending it or burning it, John should send the letter or burn it.

In UDL, the formula $\bigcirc_H \phi \Rightarrow \bigcirc_H (\phi \vee \psi)$ is valid, which means UDL cannot solve Ross' paradox. On the other hand, PUDL solves Ross' paradox, as the following proposition shows.

Proposition 2 $\nvDash_{pudl} \bigcirc_i \phi \Rightarrow \bigcirc_i (\phi \vee \psi)$.

3.1.6 Axiomatization of PUDL

The axiomatic system of PUDL contains the rules *necessitation* for $\Box$, $[\preceq]$, $[\succeq]$, $[\prec]$, $[1], \ldots, [n]$, *modus pones*, and the following axioms:

1. Mutual converse for $[\preceq]$ and $[\succeq]$:
   $(\psi \Rightarrow [\succeq]\langle\preceq\rangle\psi) \wedge (\psi \Rightarrow [\preceq]\langle\succeq\rangle\psi)$.
2. S4.3 for $[\preceq]$:
   (a) $[\preceq](\psi \Rightarrow \phi) \Rightarrow ([\preceq]\psi \Rightarrow [\preceq]\phi)$;
   (b) $[\preceq]\psi \Rightarrow [\preceq][\preceq]\psi$;
   (c) $[\preceq]\psi \Rightarrow \psi$;
   (d) $\langle\preceq\rangle\phi \wedge \langle\preceq\rangle\psi \Rightarrow (\langle\preceq\rangle(\psi \wedge \langle\preceq\rangle\phi) \vee \langle\preceq\rangle(\phi \wedge \langle\preceq\rangle\psi) \vee \langle\preceq\rangle(\psi \wedge \phi))$.
3. K for $[\prec]$:
   $[\prec](\psi \Rightarrow \phi) \Rightarrow ([\prec]\psi \Rightarrow [\prec]\phi)$.
4. Interaction:
   (a) $[\prec]\psi \Rightarrow [\preceq][\prec]\psi$;
   (b) $[\prec]\psi \Rightarrow [\prec][\preceq]\psi$;
   (c) $[\preceq]([\preceq]\psi \vee \phi) \wedge [\prec]\phi \Rightarrow \psi \vee [\preceq]\phi$.
5. Inclusion:
   (a) $\Box\psi \Rightarrow [\preceq]\psi$;
   (b) $[\preceq]\psi \Rightarrow [\prec]\psi$;
   (c) for $i \in Agent$, $\Box\psi \Rightarrow [i]\psi$.
6. Agent independent: $(\Diamond[1]\psi_1 \wedge \cdots \wedge \Diamond[n]\psi_n) \Rightarrow \Diamond([1]\psi_1 \wedge \cdots \wedge [n]\psi_n)$.
7. S5 for $\Box$.
8. S5 for $[i]$, $i \in Agent$.

If ψ can be deduced from the above axiomatic system ($\vdash_{pudl} \psi$), then ψ is a theorem of PUDL. We say ψ is deducible from Γ ($\Gamma \vdash_{pudl} \psi$), where Γ is a set of formulas, if $\vdash_{pudl} \psi$ or there are formulas $\phi_1, \ldots, \phi_n \in \Gamma$ such that $\vdash_{pudl} (\phi_1 \wedge \cdots \wedge \phi_n) \Rightarrow \psi$.

Theorem 1 *$\Gamma \vdash_{pudl} \psi$ iff $\Gamma \vDash_{pudl} \psi$*

The completeness (right-to-left) can be proved by using a canonical model technique together with Bulldozing (Segerberg 1971), and both are standard technique in modal logic. The proof of soundness (left-to-right) is trivial.

3.2 Multi-authority deontic STIT logic

Now we generalize PUDL to MADL. The main difference between them is that in MADL, deontic modality is interpreted via multiple authorities.

3.2.1 Language

The language of MADL is constructed from $Agent$, Ψ, a set of authorities $Auth$, a set of objects Obj and a set of atomic action Act. For $i \in Agent$, $o \in Obj$ and $a \in Act$, $do(i, a, o)$ is an atomic formula, which means agent i execute action a on

object o. For atomic formulas $p, q, i \in Agent$ and $j \in Auth$, the language $\mathfrak{L}_{madl}$ is generated by the following BNF:

$$\psi ::= p \mid \neg\psi \mid \psi \wedge \psi \mid [i]\psi \mid \Box\psi \mid [\preceq_j]\psi \mid [\succeq_j]\psi \mid [\prec_j]\psi$$

Intuitively, $[\preceq_j]\psi$ means that "ψ is weakly preferable according to the normative standard of authority j," while $[\prec_j]\psi$ means "ψ is strictly preferable according to the normative standard of authority j." $[\succeq_j]\psi$ means "ψ is unpreferable according to the normative standard of authority j." We use $\psi \prec^j \phi$ as an abbreviation of $(\psi \preceq^j \phi) \wedge \neg(\phi \preceq^j \psi)$. Obligation is expressed in $\mathfrak{L}_{madl}$ as follows:

- $\bigcirc_i^j \psi ::= (\neg\psi \prec^j [i]\psi) \wedge \Diamond[i]\psi$. Intuitively, this formula means that agent i ought to see to it that ψ according to the normative value of authority j iff $\neg\psi$ is strictly worse than seeing to it that ψ according to the normative value of authority j and it is possible for i to see to it that ψ.
- $\bigcirc_i^j(\psi/\phi) ::= ((\neg\psi \wedge \phi) \prec^j ([i]\psi \wedge \phi)) \wedge \Diamond[i]\psi$.

To specify security policies, we further introduce (conditional) prohibition and (conditional) permission in $\mathfrak{L}_{madl}$:

- $F_i^j \psi ::= \bigcirc_i^j \neg\psi$. This means according to the normative value of authority j, agent i is forbidden to STIT ψ iff i is obliged to STIT $\neg\psi$.
- $F_i^j(\psi/\phi) ::= \bigcirc_i^j (\neg\psi/\phi)$.
- $P_i^j \psi ::= \neg F_i^j \psi$. This means according to the normative value of authority j, agent i is permitted to see to it that ψ iff i is not forbidden to see to it that ψ.
- $P_i^j(\psi/\phi) ::= \neg F_i^j(\psi/\phi)$.

3.2.2 Semantics

The semantics of MADL is based on multi-authority STIT model, which is a generalization of PUDL model.

Definition 10 (*Multi-authority STIT model*) A Multi-authority STIT model $M = (W, IndChoice, \preceq_1, \prec_1, \ldots, \preceq_m, \prec_m, V)$ is a tuple where W and $IndChoice$ are the same as in PUDL model, and $\preceq_j$ is a relation on W indicating the normative standard of authority j. $\preceq_j$ is required to be reflexive, transitive and connected. $\prec_j$ is a sub-relation of $\preceq_j$ such that for all $v, v' \in W$, $v \prec_j v'$ iff $v \preceq_j v'$ and $v' \not\preceq_j v$.

The semantics of $\mathfrak{L}_{mddl}$ is defined similarly to that of PUDL; here, we only give the crucial cases:

Definition 11 Let M be a multi-authority STIT model, $v \in W$.

$M, v \vDash_{madl} [\preceq^j]\psi$ *iff* $M, u \vDash_{madl} \psi$ *for all* w *such that* $v \preceq_j u$;
$M, v \vDash_{madl} [\succeq^j]\psi$ *iff* $M, u \vDash_{madl} \psi$ *for all* u *such that* $u \preceq_j v$;
$M, v \vDash_{madl} [\prec^j]\psi$ *iff* $M, u \vDash_{madl} \psi$ *for all* u *such that* $v \prec_j u$;

3.2.3 Axiomatization of MADL

The axiomatic system of MADL is obtained by a simply modification of the proof system of PUDL: Simply replace the occurrence of $[\preceq]$, $[\succeq]$ and $[\prec]$ by $[\preceq^j]$, $[\succeq^j]$ and $[\prec^j]$ for each $j \in Auth$.

Theorem 2 (Soundness and completeness) $\Gamma \vdash_{madl} \psi$ *iff* $\Gamma \vDash_{madl} \psi$.

4 Related work

Using logics to handle the problems of specifying and reasoning about the security of information systems started from 1988 by Glasgow and MacEwen (1988). Since then, various types of logic have been used to model inference abilities and specification of security policies. Van Hertum et al. (2016) have recently proposed a multi-agent variant of autoepistemic logic, called Distributed Autoepistemic Logic with Inductive Definitions (dAEL(ID)), to be used as a says-based access control logic. By applying the semantic principles of autoepistemic logic to characterize the says-modality, dAEL(ID) allows us to derive a statement of the form $says_{\neg k}\psi$ on the basis of the observation that k has not issued statements implying ψ. Supporting reasoning about such negated says-statements allows dAEL(ID) to straightforwardly model access denials, which can hardly be modeled by previous *says*-based access control logics.

5 Summary and future work

In this article, we have developed a deontic STIT logic with the possible application to the specification of security policy for intrude detection in the pervasive computing environment. Compared to the existing deontic STIT logics, an advantage of our logic is that it is capable of solving the miners paradox, a logical paradox which recently grabs attentions of logicians, philosophers, linguistists and computer scientists. A complete and sound axiomatization for our logic was developed. Concerning future works, we will study the computational complexity of our logic and perform some case study for the application of our logic to security policies.

Acknowledgements Lirong Qiu has been supported by the National Nature Science Foundation of China (Nos. 61672553, 61331013). Xin Sun has been supported by the National Science Centre of Poland (BEETHOVEN, UMO-2014/15/G/HS1/04514).

Compliance with ethical standards

Conflict of interest Both authors declare that they have no conflict of interest.

Human and animals participants This article does not contain any studies with human participants or animals performed by any of the authors.

References

Barolli L, Takizawa M (2010) Special issue on emerging trends in ubiquitous computing systems. J Ambient Intell Humaniz Comput 1(4):235–237

Belnap N, Perloff M, Xu M (2001) Facing the future: agents and choice in our indeterminist world. Oxford University Press, Oxford

Broersen JM (2011) Deontic epistemic stit logic distinguishing modes of mens rea. J Appl Logic 9(2):137–152

Chisholm R (1963) Contrary-to-duty imperatives and deontic logic. Analysis 24:33–36

Choi J, Choi C, Ko B-K, Kim P (2014) A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. Soft Comput 18(9):1697–1703

Cuppens F, Cuppens-Boulahia N, Elrakaiby Y (2013) Formal specification and management of security policies with collective group obligations. J Comput Secur 21(1):149–190

Cuppens-Boulahia N, Cuppens F (2008) Specifying intrusion detection and reaction policies: an application of deontic logic. In: van der Meyden R, van der Torre Leendert WN (eds) Deontic logic in computer science, 9th international conference, DEON 2008, Luxembourg, Luxembourg, July 15–18, 2008. Proceedings, volume 5076 of Lecture Notes in Computer Science, pp 65–80. Springer

Demolombe R, Jones AJI (1996) Integrity constraints revisited. Logic J IGPL 4(3):369–383

Gabbay Dov M, Robaldo L, Sun X, van der Torre L, Baniasadi Z (2014) Toward a linguistic interpretation of deontic paradoxes—beth-reichenbach semantics approach for a new analysis of the miners scenario. In: Deontic logic and normative systems—12th international conference, DEON 2014, Ghent, Belgium, July 12–15, 2014. Proceedings, pp 108–123

Glasgow JI, MacEwen GH (1988) Reasoning about knowledge in multilevel secure distributed systems. In: Proceedings of the 1988 IEEE symposium on security and privacy, Oakland, California, USA, April 18–21, 1988, pp 122–128. IEEE Computer Society

Glasgow JI, MacEwen GH, Panangaden P (1992) A logic for reasoning about security. ACM Trans Comput Syst 10(3):226–264

Horty J (2001) Agency and deontic logic. Oxford University Press, New York

Jones AJI, Sergot MJ (1992) Formal specification of security requirements using the theory of normative positions. In: Yves D, Gérard E, Jean-Jacques Q (eds) Computer security—ESORICS 92, second European symposium on research in computer security, Toulouse, France, November 23–25, 1992, Proceedings, volume 648 of Lecture Notes in Computer Science, pp 103–121. Springer

Kagal L, Finin TW, Joshi A (2001) Trust-based security in pervasive computing environments. IEEE Comput 34(12):154–157

Kolodny N, MacFarlane J (2010) Iffs and oughts. J Philos 107(3):115–143

Kooi B, Tamminga A (2008) Moral conflicts between groups of agents. J Philos Logic 37:1–21

Lang J, van der Torre L (2008) From belief change to preference change. In: Ghallab M, Spyropoulos CD, Fakotakis N, Avouris N (eds) Proceedings of the 2008 conference on ECAI 2008: 18th European conference on artificial intelligence, pp 351–355, Amsterdam, 2008. IOS Press

Marcelloni F, Puccinelli D, Vecchio A (2014) Special issue on sensing and mobility in pervasive computing. J Ambient Intell Humaniz Comput 5(3):263–264

Meyer JJ (1988) A different approach to deontic logic: deontic logic viewed as a variant of dynamic logic. Notre Dame J Formal Logic 109–136

Ogiela MR, Castiglione A, You I (2014) Soft computing for security services in smart and ubiquitous environments. Soft Comput 18(9):1655–1658

Ramos JLH, Cano MVM, Jara AJ, Skarmeta AF (2014) A soft computing based location-aware access control for smart buildings. Soft Comput 18(9):1659–1674

Ross A (1941) Imperatives and logic. Theoria 7(53)

Segerberg K (1971) An essay in classical modal logic, volume 13 of Filosofiska studier. Filosofiska foreningen och Filosofiska institutionen vid Uppsala universitet, Uppsala

Sun X (2011) Conditional ought, a game theoretical perspective. In: Lang J, van Ditmarsch H, Ju S (eds) Logic, rationality, and interaction: proceedings of the third international workshop, pp 356–369, Guangzhou, China, October 2011

Sun X, Baniasadi Z (2014) STIT based deontic logics for the miners puzzle. In: Nils B (ed) Multi-agent systems—12th European conference, EUMAS 2014, Prague, Czech Republic, December 18–19, 2014, revised selected papers, volume 8953 of Lecture Notes in Computer Science, pp 236–251. Springer

Van Hertum P, Cramer M, Bogaerts B, Denecker M (2016) Distributed autoepistemic logic and its application to access control. In: Kambhampati S (ed) Proceedings of the twenty-fifth international joint conference on artificial intelligence, IJCAI 2016, New York, NY, USA, 9–15 July 2016, pp 1286–1292. IJCAI/AAAI Press

von Wright G (1951) Deontic logic. Mind 60:1–15