# Proofs of Theorems in "CoAChecker: Safety Analysis on Administrative Policies of Cyber-Oriented Access Control"

Mingjie Yu, Fenghua Li, Yunchuan Guo*, Zheng Yan, *Fellow, IEEE,* Xiao Wang, Liang Fang, Nenghai Yu

**Theorem 1.** *Let $q$ be a safety query, and $S = (U, A, UAV_0, P)$ and $S' = (U, A, UAV_0, P')$ be two ACoAC systems, where $P'$ is the policy obtained by removing all ineffective rules from $P$. Then, $S \models q$ if and only if $S' \models q$.*

*Proof:* $S \not\models q \implies S' \not\models q$: This conclusion is obvious, since $P'$ is a subset of $P$.

($S \models q \implies S' \models q$): Because of $S \models q$, there exists a state transition path $UAV_0 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_n} UAV_n$, where $UAV_n$ is a goal state and $\alpha_i = (u_{ai}, u_{ti}, a_{ti}, v_{ti})$ is authorized by rule $r_i = (\varphi_{ai}, \varphi_{ti}, a_{ti}, v_{ti}) \in P$. According to the definition ACoAC policy, we have $u_{ai} \models_{UAV} \varphi_{ai}$ and $u_{ti} \models_{UAV} \varphi_{ti}$, and hence $r_i$ is effective, i.e., $r_i \in P'$. Therefore, after removing ineffective rules, $\alpha_i$ is also authorized and $UAV_n$ remains reachable. ∎

**Theorem 2.** *An administrative rule $r = (\varphi_a, \varphi_t, a_t, v_t)$ is $\varphi_a$-ineffective if and only if there does not exist a user who satisfies $\varphi_a$ in the initial state $UAV_0$, that is,*

$$R_I = \{(\varphi_a, \varphi_t, a_t, v_t) \mid \forall u \in U, u \not\models_{UAV_0} \varphi_a\}.$$

*Proof:* If $r$ is $\varphi_a$-ineffective, according to the definition of $\varphi_a$-ineffective rules, we have $u \not\models_{UAV_0} \varphi_a$ for any user $u$, because the initial state $UAV_0$ is reachable.

If $u \not\models_{UAV_0} \varphi_a$ for all $u \in U$, due to the separate administration restriction, the value of an administrative attribute cannot be modified by any administrative action. Therefore, there does not exist any user who satisfies the condition $\varphi_a$ in any reachable state. As a result, rule $r$ is $\varphi_a$-ineffective. ∎

**Theorem 3.** *The rule $(true, \varphi_t, a_t, v_t) \in P$ is $\varphi_t$-ineffective if there exists an attribute $a \in A$ such that $UAV_0(u^*, a) \notin D_{\varphi_t}(a)$ and $D_P(a) \cap D_{\varphi_t}(a) = \emptyset$.*

*Proof:* Because $D_P(a) \cap D_{\varphi_t}(a) = \emptyset$, there does not exist a rule that can set attribute $a$ to a value in $D_{\varphi_t}(a)$. Furthermore, $UAV_0(u^*, a)$, the initial value of $a$, is also not in $D_{\varphi_t}(a)$. Therefore, condition $\varphi_t$ cannot be satisfied, which indicates that rule $(true, \varphi_t, a_t, v_t)$ is $\varphi_t$-ineffective. ∎

**Theorem 4.** *Let $S_1 = (\{u^*\}, A, UAV_0, P)$ and $S_2 = (\{u^*\}, A, UAV_0, P_{useful})$ be two ACoAC systems, and $q$ be a safety query. Then, $S_1 \models q$ if and only if $S_2 \models q$.*

*Proof:* ($S_2 \models q \implies S_1 \models q$): This conclusion is obvious, because $P_{useful} \subseteq P$, i.e., any sequence of actions authorized by $P_{useful}$ is also authorized by $P$.

($S_1 \models q \implies S_2 \models q$): Because of $S_1 \models q$, there exists at least one path from the initial state to a goal state. Let $\rho = UAV_0 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_n} UAV_n$ be the shortest one. Suppose that $\alpha_i$ is authorized by rule $r_i \in P$. We use mathematical induction to prove that $r_i \in P_{useful}$ for $1 \le i \le n$, which implies that $S_2 \models q$.

First, we prove that $r_n \in P_{useful}$. Because $\rho$ is the shortest path reaching a goal state, $UAV_n$ is a goal state but $UAV_{n-1}$ not. It follows that there exists an integer $1 \le i \le l$ such that $\alpha_n = (u^*, u^*, a_i^*, v_i^*)$. Therefore, rule $r_n$ is of the form $r_n = (true, \varphi_t, a_i^*, v_i^*)$. According to the definition of useful rules, $r_n$ is useful for reaching the goal states, so $r_n \in P_{useful}$.

Next, supposing that $r_i \in P_{useful}$ for all $k < i \le n$, where $1 \le k \le n$, we prove that $r_k \in P_{useful}$ by contradiction. Assume that $r_k \notin P_{useful}$, then $r_k$ is not useful for triggering $r_i$ for $k < i \le n$. It implies that $\alpha_{k+1}, \ldots, \alpha_n$ can be executed without $\alpha_k$. So, we can get another path ending to a goal state $UAV_0 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_{k-1}} UAV_{k-1} \xrightarrow{\alpha_{k+1}} UAV'_{k+1} \xrightarrow{\alpha_{k+2}} \cdots \xrightarrow{\alpha_n} UAV'_n$, which is shorter than $\rho$. It contradicts the assumption that $\rho$ is the shortest one. Therefore, $r_k \in P_{useful}$. ∎

**Theorem 5.** *The length of $\rho$ satisfies $n \le \prod_{a \in A} |D(a)| - 1$.*

*Proof:* For the sake of contradiction, assume that $n > \prod_{a \in A} |D(a)| - 1$. Because the number of distinct states is $\prod_{a \in A} |D(a)|$, there exist two same states in $\rho$. By removing the part between the two states from $\rho$, we obtain a shorter path from $UAV_0$ to a goal state, which leads to a contradiction. Therefore, $n$ is not greater than $\le \prod_{a \in A} |D(a)| - 1$. ∎

**Theorem 6.** *The length of $\rho$ satisfies*

$$n \le \prod_{a \in A_1} |D(a)| \sum_{k=0}^{m} \prod_{i=1}^{k} \big(|D(a_i)| - 1\big) - \prod_{a \in A_1 \setminus A_q} |D(a)| \prod_{a \in A_4 \setminus A_q} \big(|D(a)| - 1\big).$$

*Proof:* To obtain a tight upper bound of $n$, we divide path $\rho$ into several segments and evaluate an upper bound for each segment. Then, the theorem can be reached by accumulating these upper bounds.

Let $A_5$ be the set of attributes that are modified by the actions in $\rho$, i.e., $A_5 = \bigcup_{i=1}^{n} \{a_t(\alpha_i)\}$, where $a_t(\alpha)$ denotes the target attribute of the administrative action $\alpha$. According to the definition of $A_3$, we have $A_5 \subseteq A_3$.

Next, we introduce the division of $\rho$. Because $A_5 \subseteq A_3$ and $A_4 = A_3 \setminus A_1$, we can divide $A_5$ into two disjoint parts: $A_{51}$ and $A_{54}$, where $A_{51} = A_1 \cap A_5$ and $A_{54} = A_4 \cap A_5$. Let

$A_{54} = \{a'_1, a'_2, \ldots, a'_s\}$ and $\alpha_{j_i}$ be the first action in $\rho$ that modifies the value of attribute $a'_i$. Without loss of generality, assume that $0 = j_0 < j_1 < \cdots < j_s < j_{s+1} = n+1$. Then, the $s$ actions $\alpha_{j_1}, \ldots, \alpha_{j_s}$ divide the path $\rho$ into $s+1$ path segments, where the $k$-th segment is $\rho_k = UAV_{j_{k-1}} \xrightarrow{\alpha_{j_{k-1}+1}} \cdots \xrightarrow{\alpha_{j_k-1}} UAV_{j_k-1}$.

Now, we evaluate the upper bound of the $len(\rho_k)$. There are two cases: $1 \le k \le s$ and $k = s+1$.

***Case 1:* $1 \le k \le s$.** Let a be an attribute and $N_k(a)$ be the number of values that $a$ can take in the states of $\rho_k$. Because A can be divided into three disjoint parts: $A_{51}$, $A_{54}$, and $A \backslash A_5$, we have

$$len(\rho_k) + 1 \le \prod_{a \in A_{51}} N_k(a) \prod_{a \in A_{54}} N_k(a) \prod_{a \in A \backslash A_5} N_k(a). \quad (1)$$

For $a \in A \backslash A_5$, $N_k(a) = 1$ holds because only the values of attributes in $A_5$ are modified. For $a \in A_{51}$, $N_k(a) \le |D(a)|$ holds. For $a \in A_{54}$, there exists an integer $1 \le i \le s$ such that $a = a'_i \in A_4$. If $1 \le i < k$, according to the definition of $\alpha_{j_k}$, the value of $a'_i$ has been modified. Because $A_4 = A_3 \backslash A_1$, $a'_i$ is non-restorable, i.e., it can not be reset to its initial value. As a result, we have $N_k(a'_i) \le |D(a'_i)| - 1$. If $k \le i \le s$, according to the definition of $\alpha_{j_k}$, the value of $a'_i$ is not modified by any actions in $\rho_k$, so $N_k(a'_i) = 1$.

According to the above discussion and (1), we conclude that

$$len(\rho_k) + 1 \le \prod_{a \in A_{51}} |D(a)| \prod_{i=1}^{k-1} (|D(a'_i)| - 1). \quad (2)$$

Since $\{a'_1, \ldots, a'_{k-1}\}$ is a subset of $A_4 = \{a_1, a_2, \ldots, a_m\}$ and $D(a_1) \ge \cdots \ge D(a_m)$, we have

$$\prod_{i=1}^{k-1} (|D(a'_i)| - 1) \le \prod_{i=1}^{k-1} (|D(a_i)| - 1). \quad (3)$$

According to (2), (3), and $A_{51} \subseteq A_1$, we obtain the following conclusion.

$$len(\rho_k) + 1 \le \prod_{a \in A_1} |D(a)| \prod_{i=1}^{k-1} (|D(a_i)| - 1) \quad (4)$$

***Case 2:* $k = s+1$.** Let $UAV$ be a non-terminal state in $\rho_{s+1}$. Similar to the discussion in case 1, we can obtain two properties of $UAV$: $UAV(u^*, a) \ne UAV_0(u^*, a)$ for $a \in A_{54}$, and $UAV(u^*, a) = UAV_0(u^*, a)$ for $a \in A \backslash A_5$. Let $B$ be the set of all states satisfying the above two properties and $C$ be the set of goal states. It is obvious that $UAV \in B \backslash C$, which follows that

$$len(\rho_{s+1}) \le |B \backslash C| = |B| - |B \cap C| \quad (5)$$

Let $N_B(a)$ be the number of values that $a$ can take in the states in $B$. We have $N_B(a) \le |D(a)|$ for $a \in A_{51}$, $N_B(a) \le |D(a)| - 1$ for $a \in A_{54}$, and $N_B(a) = 1$ for $a \in A \backslash A_5$. As a result

$$\begin{aligned} |B| &= \prod_{a \in A_{51}} N_B(a) \prod_{a \in A_{54}} N_B(a) \prod_{a \in A \backslash A_5} N_B(a) \\ &= \prod_{a \in A_{51}} |D(a)| \prod_{a \in A_{54}} (|D(a)| - 1). \end{aligned} \quad (6)$$

Let $N_{B \cap C}(a)$ be the number of values that $a$ can take in the states in $B \cap C$. We have $N_{B \cap C}(a) \le |D(a)|$ for $a \in A_{51} \backslash A_q$, $N_{B \cap C}(a) \le |D(a)| - 1$ for $a \in A_{54} \backslash A_q$, and $N_{B \cap C}(a) = 1$ for $a \in (A \backslash A_5) \cup A_q$. It follows that

$$\begin{aligned} |B \cap C| &= \prod_{a \in A_{51} \backslash A_q} N_{B \cap C}(a) \prod_{a \in A_{54} \backslash A_q} N_{B \cap C}(a) \\ &\quad \prod_{a \in (A \backslash A_5) \cup A_q} N_{B \cap C}(a) \\ &= \prod_{a \in A_{51} \backslash A_q} |D(a)| \prod_{a \in A_{54} \backslash A_q} (|D(a)| - 1). \end{aligned} \quad (7)$$

Consider $A_5$ as a variable whose domain is $2^{A_3}$, then (6) and (7) can be regarded as two functions of $A_5$. For simplicty, let $|B| = f_1(A_5)$, $|B \cap C| = f_2(A_5)$, and $|B| - |B \cap C| = f(A_5)$. According to (5), (6), and (7), we have

$$\begin{aligned} len(\rho_{s+1}) \le & f(A_5) \\ = & \prod_{a \in A_5 \cap A_1} |D(a)| \prod_{a \in A_5 \cap A_4} (|D(a)| - 1) \\ & - \prod_{a \in (A_5 \cap A_1) \backslash A_q} |D(a)| \prod_{a \in (A_5 \cap A_4) \backslash A_q} (|D(a)| - 1). \end{aligned} \quad (8)$$

To evaluate the upper bound of $f(A_5)$, we show that $f$ is a monotonically increasing function, that is, for $E, F \subseteq A_3$, $f(E) \le f(F)$ if $E \subseteq F$. To achieve this goal, we only need to prove $f(E) \le f(E \cup \{a_0\})$, where $a_0 \in A_3 \backslash E$. For simplicity, let $E' = E \cup \{a_0\}$.

Since $A_3 = A_1 \cup A_4$ and $A_1$ is disjoint from $A_4$, $a_0$ is in either $A_1$ or $A_4$. If $a_0 \in A_1$, we have $A_4 \cap E' = A_4 \cap E$, and $A_1 \cap E' = (A_1 \cap E) \cup \{a_0\}$. As a result,

$$\begin{aligned} f_1(E') &= \prod_{a \in E' \cap A_1} |D(a)| \prod_{a \in E' \cap A_4} (|D(a)| - 1) \\ &= |D(a_0)| \prod_{a \in E \cap A_1} |D(a)| \prod_{a \in E \cap A_4} (|D(a)| - 1) \\ &= |D(a_0)| f_1(E) \end{aligned} \quad (9)$$

$$\begin{aligned} f_2(E') &= \prod_{a \in (E' \cap A_1) \backslash A_q} |D(a)| \prod_{a \in (E' \cap A_4) \backslash A_q} (|D(a)| - 1) \\ &= \begin{cases} |D(a_0)| f_2(E), & a_0 \notin A_q \\ f_2(E), & a_0 \in A_q \end{cases} \end{aligned} \quad (10)$$

$$\begin{aligned} f(E') - f(E) &= (f_1(E') - f_1(E)) - (f_2(E') - f_2(E)) \\ &= \begin{cases} (|D(a_0)| - 1) f(E), & a_0 \notin A_q \\ (|D(a_0)| - 1) f_1(E), & a_0 \in A_q \end{cases} \end{aligned} \quad (11)$$

Similarly, if $a_0 \in A_2$, we have

$$f(E') - f(E) = \begin{cases} (|D(a_0)| - 2) f(E), & a_0 \notin A_q \\ (|D(a_0)| - 2) f_1(E), & a_0 \in A_q \end{cases} \quad (12)$$

Because $a_0$ is modified in path $\rho$, $|D(a_0)|$ must be greater than 1. Moreover, it is obvious that both $f(E)$ and $f_1(E)$ are non-negative. According to (11) and (12), $f(E') \ge f(E)$ always holds, i.e., $f$ is monotonically increasing.

According to the monotonicity of $f$, we have

$$\begin{aligned} len(\rho_{s+1}) \leq & f(A_5) \\ \leq & f(A_3) \\ = & \prod_{a\in A_1} |D(a)| \prod_{a\in A_4} (|D(a)|-1) \\ & - \prod_{a\in A_1\backslash A_q} |D(a)| \prod_{a\in A_4\backslash A_q} (|D(a)|-1) \end{aligned} \quad (13)$$

As shown in (4) and (13), we have obtained an upper bound for each path segment of $\rho$. Because $len(\rho_k) = j_k - j_{k-1} - 1$ and $n = \sum_{k=1}^{s+1}(j_k - j_{k-1}) - 1$, we can obtain an upper bound of $n$ by accumulating the upper bounds of $len(\rho_k)$ for $1 \leq k \leq s+1$. The computation is as follows.

$$\begin{aligned} n = & \sum_{k=1}^{s+1}(j_k - j_{k-1}) - 1 \\ = & len(\rho_{s+1}) + \sum_{k=1}^{s}(len(\rho_k)+1) \\ \leq & \prod_{a\in A_1} |D(a)| \prod_{a\in A_4} (|D(a)|-1) \\ & - \prod_{a\in A_1\backslash A_q} |D(a)| \prod_{a\in A_4\backslash A_q} (|D(a)|-1) \\ & + \prod_{a\in A_1} |D(a)| \sum_{k=1}^{s}\prod_{i=1}^{k-1}(|D(a_i)|-1) \\ \leq & \prod_{a\in A_1} |D(a)| \prod_{i=1}^{m}(|D(a_i)|-1) \\ & - \prod_{a\in A_1\backslash A_q} |D(a)| \prod_{a\in A_4\backslash A_q} (|D(a)|-1) \\ & + \prod_{a\in A_1} |D(a)| \sum_{k=1}^{m}\prod_{i=1}^{k-1}(|D(a_i)|-1) \\ = & \prod_{a\in A_1} |D(a)| \sum_{k=0}^{m}\prod_{i=1}^{k}(|D(a_i)|-1) \\ & - \prod_{a\in A_1\backslash A_q} |D(a)| \prod_{a\in A_4\backslash A_q} (|D(a)|-1) \end{aligned} \quad (14)$$

■

**Theorem 7.** *Assume (i) the domain of each attribute has identical size, denoted by d, where $d \gg 1$, (ii) there is exactly one attribute in the query (i.e., $|A_q| = 1$), (iii) the target attributes of rules in $P$ are uniformly distributed over $A$, and (iv) the target values of rules with target attribute $a \in A$ are uniformly distributed over $D(a)$. Then*

$$\mathbb{E}[\tau] \;=\; \mathbb{E}\left[\frac{b_2}{b_1}\right] \;\approx\; \left(\frac{|P|}{|A|\,d^2}+1\right)^{|A|+1}. \quad (15)$$

*Proof:* Let $part_1$ and $part_2$ be the two parts of $b_2$. Then, we have that

$$\frac{part_1}{b_1} = \frac{\sum_{k=0}^{m}(c-1)^k}{c^{|A\backslash A_1|}} \approx \frac{(c-1)^{m+1}}{(c-2)c^{|A\backslash A_1|}} \quad (16)$$

$$\frac{part_2}{b_1} = \frac{\prod_{a\in A_4\backslash A_q}|D(a)|-1}{\prod_{a\in A_4\cup A_q}|D(a)|} = \frac{(c-1)^{|A_4\backslash A_q|}}{c^{|A_4\cup A_q|}} \quad (17)$$

According to the definition of $A_1$-$A_4$, the set $A$ can be divided into three disjoint parts: $A_1$, $A_4$ and $A_q\backslash A_3$. It follows that $m = |A_4| = |A\backslash A_1| - |A_q\backslash A_3|$, $|A_4\backslash A_q| = |A\backslash A_1| - |A_q\backslash A_1|$, and $|A_4 \cup A_q| = |A\backslash A_1| + |A_q \cap A_1|$. As a result, Formulae (16) and (17) can be rewritten as follows.

$$\frac{part_1}{b_1} \approx \frac{1}{(c-2)(c-1)^{|A_q\backslash A_3|-1}}\left(\frac{c-1}{c}\right)^{|A\backslash A_1|} \quad (18)$$

$$\frac{part_2}{b_1} \approx \frac{1}{(c-1)^{|A_q\backslash A_1|}c^{|A_q\cap A_1|}}\left(\frac{c-1}{c}\right)^{|A\backslash A_1|} \quad (19)$$

From (18) and (19), we can conclude that $b_2/b_1$ decreases as $|A_q|$ increases. Now, we estimate the expectation of $b_2/b_1$ when $|A_q| = 1$. Suppose that the target attributes of the rules in $P$ are uniformly distributed among $A$, and the target values of the rules with target attribute $a$ are uniformly distributed among $D(a)$. Then, for any attribute $a$, we have

$$P_{a\notin A_1} = \left(1 - \frac{1}{|A|c}\right)^{|P|} \quad (20)$$

$$P(a \notin A_3 \mid a \in A_q) = \frac{P_{a\notin A_1}}{c} \quad (21)$$

Thus,

$$\begin{aligned} E\left(\left(\frac{c-1}{c}\right)^{|A\backslash A_1|}\right) &= \sum_{k=0}^{|A|}\left(\frac{c-1}{c}\right)^k P(|A\backslash A_1| = k) \\ &= \sum_{k=0}^{|A|}\left(\frac{c-1}{c}\right)^k C_{|A|}^k {P_{a\notin A_1}}^k (1-P_{a\notin A_1})^{|A|-k} \\ &= \sum_{k=0}^{|A|} C_{|A|}^k \left(\frac{c-1}{c}P_{a\notin A_1}\right)^k (1-P_{a\notin A_1})^{|A|-k} \\ &= \left(\frac{c-1}{c}P_{a\notin A_1} + 1 - P_{a\notin A_1}\right)^{|A|} \\ &= \left(1 - \frac{P_{a\notin A_1}}{c}\right)^{|A|} \end{aligned} \quad (22)$$

From (21) and $|A_q| = 1$, we have

$$\begin{aligned} E\left(\frac{1}{(c-1)^{|A_q\backslash A_3|-1}}\right) =& (c-1)P\left(|A_q\backslash A_3| = 0\right) \\ & + P\left(|A_q\backslash A_3| = 1\right) \\ =& (c-1)P\left(a \in A_3 \mid a \in A_q\right) \\ & + P\left(a \notin A_1 \cup A_2 \mid a \in A_q\right) \\ =& (c-1)\left(1 - \frac{P_{a\notin A_1}}{c}\right) + \frac{P_{a\notin A_1}}{c} \\ =& c - 1 - \frac{c-2}{c}P_{a\notin A_1} \end{aligned} \quad (23)$$

$$\begin{aligned} E\left(\frac{1}{(c-1)^{|A_q\backslash A_1|}c^{|A_q\cap A_1|}}\right) =& \frac{1}{c-1}P\left(|A_q\backslash A_1| = 1\right) \\ & + \frac{1}{c}P\left(|A_q \cap A_1| = 1\right) \\ =& \frac{1}{c-1}P_{a\notin A_1} + \frac{1}{c}(1 - P_{a\notin A_1}) \\ =& \frac{1}{c} + \frac{1}{c(c-1)}P_{a\notin A_1} \end{aligned} \quad (24)$$

From (18), (19), (22), (23) and (24), we can compute the expectation of $b_2/b_1$ as follows.

$$\begin{aligned}
E\left(\frac{b_2}{b_1}\right) =& E\left(\frac{part_1}{b_1}\right) - E\left(\frac{part_2}{b_1}\right) \\
\approx& \left(\frac{c-1}{c-2} - \frac{1}{c}P_{a\notin A_1}\right)\left(1-\frac{1}{c}P_{a\notin A_1}\right)^{|A|} \\
&- \left(\frac{1}{c} + \frac{1}{c(c-1)}P_{a\notin A_1}\right)\left(1-\frac{1}{c}P_{a\notin A_1}\right)^{|A|} \\
=& \left(1-\frac{1}{c}P_{a\notin A_1}\right)^{|A|}\left(\frac{c^2-2c+2}{c^2-2c} - \frac{1}{c-1}P_{a\notin A_1}\right) \\
\approx& \left(1-\frac{1}{c}P_{a\notin A_1}\right)^{|A|+1}
\end{aligned}$$

Because $P_{a\notin A_1} = \left(1-\frac{1}{|A|c}\right)^{|P|} \approx 1 - \frac{|P|}{|A|c}$ when $|A|c \gg 1$, we have

$$E\left(\frac{b_2}{b_1}\right) \approx \left(\frac{c-1}{c} + \frac{|P|}{|A|c^2}\right)^{|A|+1} \tag{25}$$

■