$$\alpha = \frac{I(y,x)}{I(x)} \tag{31}$$

где I(y, x) определенно формулой (30), а I(x) формулой (9).

Выводы

Результаты исследования информационных преобразований сигнала при его прохождении через линейные инерционные системы совместно с помехой типа гауссового белого шума, позволяющее количественно оценить величину погрешности преобразования и достоверность информации линейных инерциальных систем таких как СЗИ.

Полученные аналитические зависимости отличаются общностью и могут быть использованы для расчета характеристик широкого класса линейных инерционных систем с постоянными параметрами.

Список литературы

1. Советов Б.Я. – Теория информации. Теоретические основы передачи информации в АСУ /Советов Б.Я. – Л. : изд. Ленинградского Университета, 1977. – 184 ст.

2. Евланов Л.Г. – Контроль динамических систем / Евланов Л.Г. – М. : Наука, 1999. – 432 ст.

3. Игнатов В.А. – Метод ранжирования и цензурирования показателей качества функционирования сложных систем / Игнатов В.А., Гузий Н.Н. // Защита Информации, №3 2004. – 83 – 94.ст.

4. Левин Б.Р. – Теоретические основы статистической радиотехники. Том.1 / Левин Б.Р. – М. : Сов. Радио, 1974. – 550 ст.

5. Зернов Н.В. – Теория Радиотехнических цепей / Зернов Н.В., Карпов В.Г.- Л. : Энергия, 1972. – 816 ст.

Рецензент: Ленков С.В.
Надійшла 12.08.2010

УДК 004.621.381 **Берназ Н.М., Браіловський М.М.** (ДУІКТ)

ОСОБЛИВОСТІ МОБІЛЬНИХ ЗАСОБІВ ЗАХИСТУ

Вступ

Системи захисту і особливо мобільні системи захисту інформації, представляють собою певний додаток або надбудову до функціональної системи, яку передбачається захищати. Таким чином, стає актуальним питання про те, щоб такі додатки не погіршували експлуатаційних параметрів функціональних систем. Одним з найважливіших параметрів цього типу являється параметр, котрий характеризує швидкодію системи. У випадку мобільних систем захисту цей параметр має особливе значення оскільки мобільні системи повинні бути, у відповідності зі змістовним значенням терміну "мобільність", переносимими, а це означає, що вони повинні надавати користувачу можливість оцінювати ступінь мобільності, оскільки на основі такої оцінки може бути прийнято рішення про можливості використання мобільної системи. Слід відмітити, що у випадку інших підходів до побудови систем захисту, таких як декларативні чи цільові, ця проблема розв'язується на стадії розробки відповідної системи захисту, оскільки в цих підходах система захисту, при розробці орієнтується на захищувану систему і цей параметр враховується з самого початку.

Основна частина

У зв'язку з цим, формальний опис засобів захисту у вигляді логічних послідовностей необхідно розширити компонентами, зв'язаними з параметрами, що характеризують час роботи відповідних складових [1]. Кожна логічна складова, що реалізує фрагмент мобільних засобів захисту, володіє деяким часовим параметром τ_i. Цей часовий параметр означає інтервал часу, котрий є необхідним для її реалізації. Одним з принципових питань в цьому випадку є питання про вимірювання такого параметру, оскільки мова йде про мобільні системи. Будемо ці параметри визначати кількістю циклів роботи відповідних фрагментів. В цьому випадку, в залежності від базових технічних засобів, котрі забезпечують фізичну швидкодію і базового системного програмного забезпечення, котре забезпечує програмну швидкодію, можна достатньо легко в кожному конкретному випадку перейти до абсолютних часових значень відповідних параметрів системи захисту і окремих компонент цієї системи. Розглянемо наступне визначення.

Визначення 1. Одиниця часового масштабу параметра τ_{ij} компоненти λ_j послідовності ϑ_j відповідає одному циклу виконання λ_i, що будемо записувати у вигляді:

$$\xi_{ij} = t[\vartheta_i(\lambda_j)],$$

якщо ξ_{ij} визначається компонентою λ_j. Можна використовувати як одиницю вимірювань τ_i, якщо в процесі використання $\vartheta_i = \lambda_1 * ... * \lambda_n$, по умовах застосування ϑ_i в системі захисту Z_i використовується ϑ_i по максимальних циклах. В загальному випадку формальний запис засобів захисту описується наступним чином:

$$A_i = \{\vartheta_1[\lambda_1^1 t_1^1 * ... * \lambda_m^1 t_m^1] * ... * \vartheta_n[\lambda_1^n t_1^n * ... * \lambda_k^n t_k^n]\}.$$

В цьому виразі не для всіх λ_j^i або ϑ_i може приписуватись параметр t_i. Розглянемо наступне визначення.

Визначення 2. Якщо для λ_j^i з ϑ_i $t_i = const$, то відповідна компонента втрачає часовий параметр t_i.

По суті це означає, що коли λ_j^i у всіх випадках її використання в процесі роботи системи захисту займає фіксований проміжок часу, то цей проміжок в кількості циклів виноситься в склад узагальнених часових характеристик системи захисту. Це дозволяє спростити формальний опис системи захисту та аналіз часових параметрів, при переносі засобів з одного середовища в інше.

Розглянемо питання про часову виконуваність і невиконуваність компоненти A_i системи захисту Z_i.

Часова виконуваність приводить до уявлень про часове протиріччя, яке є більш складним і менш очевидним з точки зору уявлень про протиріччя в класичній математичній логіці. Тому розглянемо наступне визначення.

Визначення 3. Часовою виконуваністю логічних функцій називається здатність здійснювати обчислення значень λ_i не більш ніж за τ_i елементарних операцій.

В даному випадку, під елементарною операцією розуміється деяка кількість перетворень, яка в даному підході декларується як елементарне перетворення. Прикладом такої сукупності можуть служити перетворення типу генценовських [2]. Для більшої визначеності, приймемо їх як частину задекларованої множини елементарних перетворень і позначимо цю множину буквою S.

$$\begin{gathered}S = \{G \mid G; U \mid G \Rightarrow U; D \mid G; (U, G \mid D) \,\&\, (U \mid G) \Rightarrow U \mid D; \\ U \mid U \vee G; (U \mid G) \,\&\, (T \mid G) \Rightarrow (U \vee T \mid G); (U, D \mid (U \,\&\, D); \\ ((U, G \mid D) \,\&\, (U, G \mid \neg D)) \Rightarrow (U \mid \neg D); \neg\neg U \mid U; (U_1, ..., U_n \mid G_i) \,\& \\ (G_1, ..., G_k \mid D) \Rightarrow U_1, ..., U_n \mid D; U \mid G(x) \Rightarrow U \mid \forall x G(x); \\ \forall x U(x) \mid U(y); U(y) \mid \exists x U(x); \exists x U(x) \mid G; (U_1, ..., U_n \mid U) \,\& \\ \mid (U \sim G) \Rightarrow U_1, ..., U_n \mid G; U(y/x) \Rightarrow U(y)\}.\end{gathered}$$

В приведеній системі під одиничною операцією розуміється реалізація описаного перетворення по відношенню до одного елемента в співвідношенні. В будь якому правилі системи S в реальному випадку можлива скінчена множина компонент в правій частині співвідношення. При необхідності здійснювати перетворення, котре в загальному вигляді може записуватись у вигляді:

$$U_1,...,U_n \Rightarrow F_1,...,F_m \text{ при } m < n,$$

навіть якщо n скінчене, то у зв'язку з проблемою часової виконуваності, необхідно розглянути уявлення про інтерпретаційні узагальнення. На змістовному рівні це означає наступне. Будь яка інтерпретація представляє собою засіб звуження області загальнозначущості тієї або іншої формули. Отже можна записати операцію інтерпретаційного звуження логічної формули у наступному вигляді:

$$I[\lambda_i(x_1^i,...,x_n^i)] = \lambda_i[x_1^i,...,x_k^i,(n-k=q \neq 0)].$$

Інтерпретаційне звуження може приводити не тільки до зменшення кількості змінних у формулах, а й до звуження області їх інтерпретації, котра описується предикатами:

де X - множина значень, котрі можуть приймати x_j^i. В цьому випадку можна записати співвідношення:

$$I[\lambda_i(x_1^i,...,x_n^i)] = \lambda_i^*(x_1^{*i},...,x_n^{*i}), \text{де } x_j^{*i} \in \{x_j^{*i} : x_j^* \in X' \subset X\}.$$

Інтерпретуюче звуження, яке буде приводити до зменшення змінних в формулі, будемо називати інтерпретуючим звуженням першого роду, що будемо записувати у вигляді:

$$\lambda_i' = Ip(\lambda_i).$$

Інтерпретуюче звуження, що приводить до зменшення області визначення змінних, які фігурують у формулах і описуються предикатами $P_i(x_i)$ будемо називати інтерпретуючим звуженням другого роду і будемо записувати у вигляді:

$$\lambda_i^* = I\nu(\lambda_i).$$

Розглянемо більш конструктивно Ip, оскільки безпосередня або груба елімінація змінних x_i з логічних формул $\lambda_i(x_i)$ може привести до порушення синтаксису написання формули λ_i або до змін, при яких λ_i виявиться невиконуваною внаслідок порушення логіки опису ситуації або об'єкту, до якого відноситься формула $\lambda_i(x_i)$. У зв'язку з введенням уявлень про Ip необхідно розглянути правила допустимих виключень змінних x_i з λ_i. Для цього розглянемо синтаксично можливі фрагменти формул в λ_i, при використанні логічних функцій вузького обчислення висловлювань.

Твердження 1. Якщо x_i, x_j, x_k розміщені підряд і об'єднуються функціями "*" = $\{\&, \vee\}$, то $Ip(\lambda_i(x_i))$ допустима, що формально можна записати у вигляді:

$$(x_i * x_j * x_k) \Rightarrow (x_i * x_k).$$

Доведення цього твердження випливає з інтерпретації протиріччя формул класичної логіки, в яких використовуються логічні функції $\&$ і $\vee$.

Твердження 2. Якщо має місце:

$$x_i \to (x_j \to x_k) \vee (x_i \to x_j) x_k,$$

то допустиме $Ip(\lambda_i(x_i))$, що формально записується у вигляді:

$$Ip\ [x_i \to (x_j \to x_k) \vee (x_i \to x_j) \to x_k].$$

Доведемо допустимість $Ip(\lambda_i)$, для кожного члена диз'юнкції окремо. Здійснимо еквівалентні перетворення кожного члена диз'юнкції, котрі можна записати у вигляді наступних перетворень:

$$x_i \to (x_j \to x_k) \Rightarrow x_i \to (\neg x_j \vee x_k) \Rightarrow \neg x_i \vee \neg x_j \vee x_k;$$

$$(x_i \to x_j) \to x_k \Rightarrow (\neg x_i \vee x_j) \to x_k \Rightarrow \neg(\neg x_i \vee x_j) \vee x_k \Rightarrow x_i \& \neg x_j \vee x_k;$$

Об'єднаємо результати двох перетворень знаком диз'юнкції так, як це записано в умові твердження.

$$\neg x_i \vee \neg x_j \vee x_k \vee (x_i \& \neg x_j) \vee x_k \Rightarrow \neg x_i \vee \neg x_j \vee x_k \vee \neg x_i \vee x_j \vee x_k \Rightarrow$$

$$\Rightarrow \neg x_i \vee \neg x_j \vee x_j \vee x_k \Rightarrow \neg x_i \vee x_k \Rightarrow x_i \to x_k .$$

Отже, при елімінації x_j значення початкової формули не стане заперечним, оскільки при об'єднанні двох варіантів використання імплікації, такі перетворення приведуть до синтаксично допустимих зображень фрагментів формули.

Твердження 3. $Ip(\lambda_i(x_i))$ допустиме у фрагментах формул, які записуються у вигляді:

a) $(..., x_i) \& x_j \& x_k, ...;$

b) $(..., x_i) \vee x_j \& x_k, ...;$

c) $(..., x_i) \vee x_j \vee x_k, ...;$

d) $x_i \vee (x_j \& x_k, ...);$

e) $x_i \vee (x_j * x_k, ...).$

Доведення. У випадку а) частину фрагменту $(...,x_i)$ можна замінити новою змінною y_i. Тоді можна записати:

$$(...x_i) \& x_j \& x_k, ... \Rightarrow y_i \& x_i \& x_k, ... ,$$

де права частина у відповідності з твердженням 2.1 допускає перетворення $Ip(\lambda_i(x_i))$.

Для випадку с) можемо поступити аналогічно.

$$(...x_i) = y_i \Rightarrow y_i \vee x_j \vee x_k, ... ,$$

де права частина допускає перетворення $Ip(\lambda_i(x_i))$ у відповідності з твердженням 2.1.

Для випадку b) проводимо заміну $(...x_i) = y_i$ і $(...x_k) = y_k$, тоді можна записати, що $(...x_i) \vee x_j \& x_k, ... \Rightarrow y_i \vee x_j \& y_k \Rightarrow (y_i \vee x_j) \& (y_i \vee y_k)$. Оскільки елімінуючий елемент x_j зв'язаний диз'юнктивно з y_i і цей диз'юнкт окремо зв'язаний кон'юнктивно з рештою формули λ_i, то можна розглядати тільки $(y_i \vee x_j)$. Елімінація x_j в $(y_i \vee x_j)$ не приведе до протиріччя в формулі λ_i у відповідності з твердженням 1.

Аналогічно можна провести доведення допустимості елімінації x_j для випадку d) і e).

Розглянемо конструктивні правила елімінації x_j^i в λ_i при $Ip(\lambda_i)$, які будуть передбачати всі синтаксично допустимі конфігурації x_i, x_j і x_k в λ_i.

Правило 1. $...x_i \& x_j \& x_k, ... \Rightarrow ...x_i \& x_k, ...$

Правило 2. $...x_i \vee x_j \vee x_k, ... \Rightarrow ...x_i \& x_k, ...$

Правило 3. $...,(x_i \to x_j) * x_k, ... \Rightarrow ..., \neg x_i * x_k, ...$

Правило 4. $...x_i * (x_j \to x_k), ... \Rightarrow ...x_i * x_k, ...$

Правило 5. $...x_i) * x_j * x_k, ... \Rightarrow ...x_i) * x_k, ...$

Правило 6. $...x_i * (x_j * x_k, ... \Rightarrow ...x_i * (x_k, ...$

Приведені правила ґрунтуються на твердженнях 1, 2, 3.

Твердження 4. Інтерпретаційне звуження Ip поглинає інтерпретаційне звуження Iv, при проведенні елімінації x_j в

$$Iv(Ip(\lambda_i(x_j^i))) \Rightarrow Ip(\lambda_i(x_j^i)).$$

При цьому, протилежне твердження не вірне.

Доведення. По визначенню $Iv(Ip(\lambda_i) \Rightarrow \lambda_i(x_j^i)$, де $x_j^i \in X' \subset X$, а $Ip(\lambda_i) \Rightarrow \lambda_i'(...,x_{j-1},x_{j+1},...)$. Таким чином, після використання звуження $Ip(\lambda_i(x_j))$, змінна для Iv з λ_i вилучається, що приводить до зникнення необхідності виконання Iv (λ_i).

Твердження 5. Якщо інтерпретація *I* системи *A* допускає звуження будь-якого типу, то в $\vartheta \subset A$ існує хоча би одна λ_i, для якої $p(\lambda_i)$ або Iv (λ_i)не приводить до протиріччя відповідної ϑ або має місце $A\,|\,\vartheta\{\lambda_1,...,I(\lambda_i),...,\lambda_n\}$.

Доведення. Будь яка інтерпретація *I(A)* здійснює співставлення кожній змінній x_i елемента з області інтерпретації d_i, котрий визначається співвідношенням $d_i = I(x_i)$ і кожній константі a_j базиса - деякий елемент $d_j=I(a_j)$ з області інтерпретації *D*. Таким чином, процедура занурення кожної λ_i з *A* може бути зведена до процедури відповідної заміни. Може статися, що всі x_i з ϑ і відповідно з λ_i, виявились заміненими. В цьому випадку, при зануренні *A* в область інтерпретації *D* за допомогою *I(A)*, інтерпретаційного звуження не відбулося. Це заперечує допущенню твердження. Якщо при зануренні *A* в *D* або при виконанні інтерпретації *I* над *A* *I(A, D)=> A'(I)* виявилось, що залишились деякі x_i, або a_i з λ_i, то *I(A)* здійснює інтерпретаційне звуження *Ip* або Iv тих формул λ_i з ϑ, в котрі входять відповідні x_i або a_i. Елімінація a_i реалізується перш за все з допомогою Iv, але a_i може бути позначена як x_j з предикатом, що визначає область визначення для x_j у вигляді $P_j(x_j)=a_i$. В цьому сенсі можна говорити про приведення Iv до *Ip*. Тому будемо розглядати елімінацію $Ip(x_i)$, а всі випадки елімінації a_i з λ_i будемо вважати елімінаціями приведених інтерпретаційних звужень $Ip(x_j)$. Припустимо, що в деякій формулі λ_i існує x_j, для якої відсутній елемент $d_j=I(x_j)$. Це значить, що відповідний предикат $P_i(x_i)=0$, оскільки відсутня така x_i з *X*, для якої x_i в $I(x_i)$ мало би місце. Звідси витікає, що відсутність відповідної x_i в λ_i не приведе до протиріччя в λ_i, і відповідно, в ϑ і в *A* в цілому. Тепер необхідно так виключити x_i з λ_i, щоб не порушити синтаксис відповідної формули λ_i, інакше формула виявиться неправильно побудованою, а це призведе до її невиконаності навіть в області визначення змінних, що залишилися і визначаються як x_i з X. Якщо елімінацію x_i, які не одержали відповідних d_i при зануренні *I(A,D)=> A'(I)*, здійснювати у відповідності з правилами 2.1 - 2.6, допустимість котрих грунтується на твердженнях 2.1-2.3, то синтаксис λ_i не буде порушеним. Таким чином, відповідні λ_i не будуть заперечними, оскільки залишаться правильно побудованими після елімінації відповідних змінних чи констант. Внаслідок цього буде мати місце співвідношення, яке доводить твердження: $A\,|\,\vartheta\{\lambda_1,...,I(\lambda_i),...,\lambda_n\}$.

Введені уявлення про інтерпретаційну звужуваність логічних формул λ_i з ϑ являються основою для одного з можливих механізмів розв'язання задачі забезпечення часової виконуваності логічних формул, котрі в певній мірі описують мобільну систему захисту і характеризують її можливості при переносі системи на конкретну систему, що підлягає захисту. Іншим механізмом забезпечення необхідної часової виконуваності системи *A* і, відповідно, $\vartheta\{\lambda_1,...,\lambda_n\}$ являються правила обчислення логічних функцій, які описують, у випадку систем захисту, залежність параметрів засобів захисту, які необхідно використовувати для захисту в залежності від параметрів розпізнаних на даний момент загроз.

По суті, механізми інтерпретаційного звуження окремих λ_i, і ϑ реалізуються один раз, при переносі системи захисту в нове середовище, котре необхідно захищати. В подальшому цей механізм може використовуватись у випадках змін, які відбуваються в самій системі, що захищається. Завдяки формалізації уявлень про інтерпретаційне звуження, можна реалізовувати автоматичні процедури його здійснення.

При незмінному функціонуванні захищуваної системи, для забезпечення часової виконуваності, необхідно використовувати процедури вибору правил перетворення логічних формул, котрі доцільно проводити перед безпосереднім обчисленням їх значень. Ці перетворення можна інтерпретувати як сам процес обчислення значень формул, якщо не притримуватись класичних уявлень про процедуру їх обчислень [2]. Найчастіше класична процедура обчислення значень логічних формул зводиться до підстановки поточних значень змінних, що використовуються в логічних формулах, і в обчисленні значення всієї логічної формули. Прикладом такого підходу може служити метод резолюцій Робінсона [3] з різними його модифікаціями [4] або обернений метод Маслова [5]. В цих методах, котрі грунтуються на теоремі Ербрана [6], розв'язується задача визначення заперечності досліджуваної системи формул, для чого здійснюється перетворення логічних формул до деякого їх канонічного представлення. В даному випадку мова йде про таку оперативну зміну логічних формул, котра не приводить до тієї чи іншої канонічної форми, а змінює їх у зв'язку зі зміною текучої ситуації, котра складається в системі в кожний текучий момент часу у зв'язку з виявленням в останній зовнішніх дій на систему, що підлягає захисту.

Висновки

В цьому контексті уявлення про часове протиріччя на змістовному рівні полягає в наступному. Нехай в текучий момент часу засоби захисту описуються системою логічних формул A. В певний момент часу, по кількості змінних, констант, існуючих елементарних і виділених фрагментів логічних формул і на основі вихідних, для даного моменту, даних про необхідні часові ресурси здійснюється перевірка окремих формул λ_i з ϑ і окремих ϑ з A на часове протиріччя. Це протиріччя має місце, якщо для обчислення значення окремої A або ϑ необхідно затратити більше часу ніж час, що потрібен загрозі, для повної реалізації своєї дії на захищувану систему.

Для розв'язку задачі забезпечення часової виконуваності A в цілому, необхідно вживати заходи по скороченню часу необхідного для обчислення значень λ_i чи ϑ. Для цього, крім механізмів елімінації окремих елементів x_i з λ_i чи зменшення областей їх визначення, необхідно розглядати задачі елімінації окремих λ_i з ϑ.

Список літератури

1. Перегудов Д.А. – Программные средства защиты информации / Перегудов Д.А., Берназ Н.М., Гришин С.П., Ленков Е.С. // Сб. науч. трудов ВНУ им. В.Даля. – Луганск, №6(136), 2009. –С.214-218.

2. Девис М. – Упрощение лишнего из механических доказательств / Девис М. // Кибернетический сборник. –М.: Наука, №7, 1998. –С.180-189.

3. Робинсон Дж. – Машинно-ориентированная логика, основанная на принципе резолюции / Робинсон Дж. // Кибернетический сборник. –М.: Наука, №7, 1998. –С.160-179.

4. Чень Ч. – Математическая логика и автоматическое доказательство теорем / Чень Ч., Ли Р. – М.: Наука, 1983. – 324 с.

5. Чень Ч. – Проблемы математической логики / Чень Ч., Ли Р. – М.: Мир, 1970. – 283 с.

6. Маслов С.Ю. – Обратный метод установления выводимости в классическом исчислении / Маслов С.Ю. // ДАН СССР. – М., №1, 1964. – С.17-20.

В статті розглядається оперативна зміна логічних формул, котра не приводить до тієї чи іншої канонічної форми, а змінює їх у зв'язку зі зміною текучої ситуації.

В статье рассматривается оперативная замена логических формул, которая не приводит к той или иной каноничной форме, а меняет их зависимо от текущей ситуации.

The article discusses the operational replacement of logical formulas. This replacement does not lead to some canonical form, but changes them depending on the current situation.

Рецензент: Корнійчук М.Т.
Надійшла 03.09.2010