Problem eliminowania fałszywych alarmów w komputerowych systemach ochrony peryferyjnej

G. KONOPACKI, K. WORWA
e-mail: gkonopacki@wat.edu.pl

Instytut Systemów Informatycznych
Wydział Cybernetyki Wojskowej Akademii Technicznej
ul. S. Kaliskiego 2, 00-908 Warszawa

W artykule rozpatruje się problem ochrony obiektów powierzchniowych za pomocą komputerowego systemu ochrony peryferyjnej, sterującego ochroną utworzoną w postaci barykady z wmontowanymi w nią czujkami naciągowymi. Analizuje się problem fałszywych alarmów w tego typu systemach ochrony, które mają charakter losowy oraz ciągły i zmienny w czasie. Opisuje się w sposób formalny za pomocą procesu stochastycznego zachowanie barykady podczas oddziaływania na nią czynników losowych i formułuje się i rozwiązuje zadanie określenia czułości czujek naciągowych minimalizujących powstawanie fałszywych alarmów.

Słowa kluczowe: ochrona obiektów, fałszywy alarm

1. Wprowadzenie

Na przestrzeni wieków człowiekowi zawsze towarzyszyło zagrożenie jego bytu. W miarę rozwoju cywilizacyjnego zaczęto zdawać sobie sprawę z tego, że zagrożenia mogą mieć charakter losowy, niezależny od człowieka, jak też mogą wynikać ze świadomej jego działalności. Te ostatnie, podlegające niezwykle szybkiemu rozwojowi i rozprzestrzenianiu się, wynikały pierwotnie głównie z atawistycznej walki o byt, a następnie z chęci posiadania, ukierunkowanej na zabór mienia połączony nierzadko z pozbawianiem zdrowia, a nawet życia jego właściciela.

Potrzeba poczucia bezpieczeństwa, będąca jedną z podstawowych potrzeb każdego człowieka, powoduje stały wzrost zainteresowania systemami ochrony. Ewolucja zagrożeń, spowodowana brutalizacją metod postępowania napastników, oraz wzrost ilości dóbr będących w indywidualnym posiadaniu stały się istotnymi czynnikami stymulującymi rozwój w dziedzinie zabezpieczeń. Z biegiem czasu pojedyncze elementy ochronne zaczęto łączyć w coraz bardziej przemyślne systemy ochrony. Budowano więc mury, palisady, otaczano się fosą, ustawiano warty.

Czasy nam współczesne nie przyniosły osłabienia zagrożeń, a wręcz przeciwnie, ich rozwój zarówno ilościowy, jak i jakościowy, zatem dotychczasowe metody i narzędzia ochrony przestały już wystarczać. Spowodowało to znaczący rozwój systemów ochrony, wykorzystujących najnowsze osiągnięcia nauki i techniki.

Pomimo takiego nasycenia techniką współczesnych systemów ochrony, należy jednak zdawać sobie sprawę z faktu, iż udział człowieka w funkcjonowaniu tych systemów jest nadal decydujący. Człowiek podejmuje decyzje i organizuje przedsięwzięcia związane z niedopuszczeniem intruza na teren chroniony, a także usuwaniem skutków jego działania, gdy – niestety – przedostał się na teren chroniony. Niejako część techniczna (system techniczny) systemu ochrony ma za zadanie przygotować dane do podjęcia decyzji i wspomagać proces decyzyjny.

W dzisiejszych czasach gwałtownemu rozwojowi podlega szczególnie system techniczny systemu ochrony. Elektronika i technika komputerowa, a właściwie informatyka, zawładnęły systemami ochrony. Obserwacja terenu prowadzona jest za pomocą kamer telewizji przemysłowej, a dostęp do obiektu sterowany jest za pomocą inteligentnych systemów komputerowych.

Zadania, które stoją przed technologią komputerową zastosowaną w systemach ochrony, są bardzo ważne. To technika komputerowa zapewnia efektywne sterowanie całym systemem ochrony. Szybka wymiana danych między jego elementami, usytuowanymi nieraz w odległych od siebie miejscach, odpowiednie i szybkie ich przetworzenie oraz dostarczenie we właściwej formie decydentom ma podstawowe znaczenie dla przydatności systemu ochrony.

Komputerowe systemy ochrony umożliwiają nieprzerwaną ochronę obiektu w różnych warunkach klimatycznych, o różnych porach doby i roku. Dzięki dobrze rozwiniętej technice multimedialnej istnieje możliwość wizualizacji danych i zdarzeń w systemie ochrony i ochranianym obiekcie.

Niezaprzeczalną zaletą takich systemów jest to, że mogą być również wyposażane w elementy sztucznej „inteligencji", wykorzystywane do wstępnego analizowania zbieranych danych o stanie ochranianego obiektu oraz, co jest najważniejsze, do wykrywania stanów tzw. „fałszywych alarmów" oraz tzw. „fałszywego spokoju".

Rozwój w dziedzinie komputerowych systemów ochrony daje osobom odpowiedzialnym za bezpieczeństwo obiektów nowe narzędzia. Umiejętne ich zastosowanie znacznie podnosi poziom bezpieczeństwa chronionych dóbr, wyręczając człowieka w wykonywaniu najbardziej uciążliwych i żmudnych czynności. Faktem jest, iż w fazie tworzenia komputerowych systemów ochrony obiektu nakłady finansowe ponoszone przez inwestora są znaczne, jednakże korzyści, jakie daje zastosowanie takiego systemu, szczególnie w ochronie obiektów skomplikowanych architektonicznie lub usytuowanych na rozległym terenie, powodują ich coraz częstsze stosowanie.

Spośród wielu przestępstw, stanowiących zagrożenie dla chronionych wartości, jedną z najpoważniejszych grup przestępstw stanowią przestępstwa przeciwko mieniu – zarówno społecznemu jak i prywatnemu. Grupą, w której odnotowuje się od pewnego czasu stały wzrost liczby popełnianych przestępstw, są kradzieże z włamaniem.

Wymagania stawiane współczesnym komputerowym systemom ochrony są niezwykle wysokie. Ich spełnienie mogą zagwarantować tylko systemy charakteryzujące się następującymi własnościami:

- wysoką niezawodnością w sensie technicznym
- wiarygodnością reakcji na wystąpienie realnego zagrożenia
- minimalnym poziomem występowania stanów fałszywego alarmu i fałszywego spokoju
- łatwością weryfikacji sygnałów generowanych przez system
- prostotą obsługi
- podwyższoną odpornością na sabotaż i zniszczenie.

Oprócz tych cech, komputerowe systemy ochrony coraz częściej oferują możliwość wypracowywania propozycji decyzji w przypadku wystąpienia określonych zagrożeń. Jest to o tyle istotne, iż wystąpienie realnego zagrożenia (szczególnie o dużym nasileniu) może powodować różne reakcje u osób obsługujących system. Dlatego system oferujący pomoc personelowi w postaci „podpowiedzi" działań wymusza ich określoną kolejność, dokumentuje ich podejmowanie oraz przypomina o działaniach koniecznych, ale jeszcze dotychczas niepodjętych. W przypadkach wystąpienia lokalnych zagrożeń o niewielkim nasileniu, ten aspekt działania systemu nie jest tak bardzo istotny. Natomiast wystąpienie zagrożeń na dużym obszarze, przy ich znacznym nasileniu, wymaga szybkiego podejmowania decyzji podczas koordynacji działań mających na celu przywrócenie porządku lub kierowanie akcją ratowniczą. W takich sytuacjach duże ilości danych napływających do stanowiska kierowania wymagają ich szybkiej interpretacji oraz przetworzenia na decyzje.

Równie istotnym czynnikiem jak sprawność i efektywność zabezpieczeń technicznych jest reakcja odpowiednich służb na wygenerowany przez system sygnał alarmu. Dlatego system, wspomagający proces podejmowania decyzji przez kierownictwo akcji, może wydatnie zwiększyć skuteczność działań np. ekip ratowniczych bezpośrednio na miejscu działań. Dopiero jednak system ochrony wyposażony w niezawodną i sprawną instalację powiadamiania oraz osoby kompetentne do reagowania na sygnały zagrożenia gwarantuje bezpieczeństwo chronionego obiektu.

Budowa komputerowych systemów ochrony obiektów musi uwzględniać następujące podstawowe zasady:

- każdy system ochrony obiektu musi być ściśle dostosowany do ochranianego obiektu. Oznacza to, że system ochrony musi uwzględniać specyfikę chronionego obiektu i chronionych w nim wartości. To zwykle decyduje o tym, że nie tworzy się identycznych systemów ochrony dla dwóch różnych chronionych obiektów, nawet gdyby charakteryzowały się bardzo zbliżonymi własnościami, gdyż identyczne rozwiązania szczegółowe systemów ochrony ułatwiałyby możliwość ich stosunkowo szybkiego pokonania, a co za tym idzie, brak możliwości dalszego ich stosowania
- system ochrony w zależności od własności obiektu chronionego i rodzajów możliwych zagrożeń, powinien obejmować odpowiedni zestaw urządzeń technicznych (czujki)

ukierunkowanych na rozpoznawanie sytuacji świadczących o realizacji zagrożeń. To sprawia, że konieczny staje się bardzo starannie przemyślany dobór takiego zestawu czujek, który jest charakterystyczny dla chronionego obiektu

- system ochrony obiektu musi być elastyczny, tzn. przystosowany do możliwie najłatwiejszego wprowadzania zmian technicznych, organizacyjnych i funkcjonalnych stymulowanych:
  - rozwojem technicznym urządzeń specjalistycznych (czujek, bramek, kamer telewizji przemysłowej itp.), wykorzystywanych w systemach ochrony,
  - rozwojem metod i urządzeń służących do pokonywania systemów ochrony obiektów,
  - zmianami przeznaczenia oraz właściwości chronionego obiektu i chronionych w nim wartości,
  - zmianami rodzajów zagrożeń dotyczących chronionego obiektu oraz prawdopodobieństwa ich realizacji
- system ochrony musi dawać pewność, w granicach przyjętego poziomu ufności, że z określonym prawdopodobieństwem zostaną wykryte objawy wystąpienia zagrożenia w takim nasileniu, iż może ono rodzić ujemne skutki dla chronionego obiektu. Zatem oczywiste jest, że jeżeli będzie ulegać zmianie stan bezpieczeństwa obiektu (chodzi tutaj szczególnie o obniżenie tego stanu), to musi się również zmieniać sam system ochrony. Najprostszym rozwiązaniem byłoby demontowanie istniejącego systemu ochrony i budowanie nowego, ale ze względu na duży koszt utworzenia systemu nowego, raczej ta wersja dopasowania systemu ochrony do nowej sytuacji nie będzie miała za często miejsca.

Kolejne oczekiwania kierowane pod adresem systemów ochrony wiążą się z ich „inteligencją". Współczesne komputerowe systemy ochrony muszą również zapewniać wypracowywanie propozycji decyzji dla obsługi w przypadku identyfikacji realizacji określonego typu zagrożenia. Taka sztuczna inteligencja byłaby wykorzystywana do rozpoznawania stanów „fałszywego alarmu" i „fałszywego spokoju", identyfikacji osób według ich cech somatycznych, linii papilarnych, kości czaszki, kodu DNA i innych indywidualizujących cech osobniczych oraz identyfikacji wystąpienia niepożądanych bądź pożądanych innych stanów i zdarzeń. Stosowanie sztucznej inteligencji, ze względu na jej koszt, powinno następować w takich przypadkach, gdy intensywność zdarzeń koniecznych do obserwacji jest na tyle duża, że ochrona fizyczna może nie gwarantować odpowiednio wysokiego prawdopodobieństwa zidentyfikowania pojawiających się nieprawidłowości lub zagrożeń.

Cele komputerowego systemu ochrony obiektu są następujące:

- niedopuszczenie intruza na teren ochranianego obiektu lub maksymalne utrudnienie jego wejścia na ten teren
- niedopuszczenie wyjścia intruza z obiektu poza teren podlegający ochronie
- skryta obserwacja intruza
- ciągła kontrola obszaru, na którym mieści się obiekt
- kontrola wnętrza obiektu
- maksymalne ułatwienie współpracy czynnika ludzkiego (ochrony fizycznej) z systemem.

Niezawodność funkcjonowania systemów ochrony obiektów wiąże się z odpornością systemu na wykrywanie „fałszywych alarmów" lub „fałszywego spokoju". Fałszywy alarm występuje wtedy, gdy chroniony obiekt nie jest przedmiotem działań intruza, a system ochrony sygnalizuje alarm. Taki stan może być spowodowany wadliwie funkcjonującymi elementami systemu technicznego albo − przy technicznie sprawnym systemie − zaistnieniem niesprzyjających warunków losowych (np. wichura, przypadkowe wejście w barierę ochronną człowieka, zwierzęcia lub ptaka). Fałszywy spokój, o wiele groźniejszy od fałszywego alarmu, ma miejsce wtedy, gdy występuje rzeczywiste zagrożenie obiektu, natomiast system jego ochrony z różnych przyczyn nie reaguje.

W dalszej części niniejszego opracowania zostanie rozpatrzony problem eliminowania fałszywych alarmów w przypadku komputerowych systemów ochrony peryferyjnej, przeznaczonych głównie do ochrony obiektów powierzchniowych, jak np. lotniska, ujęcia wody, podejścia do zakładów produkcji specjalnej, terenów, na których mieszczą się elektrownie, przede wszystkim atomowe itp.

2. Podstawowe zasady funkcjonowania systemu ochrony peryferyjnej

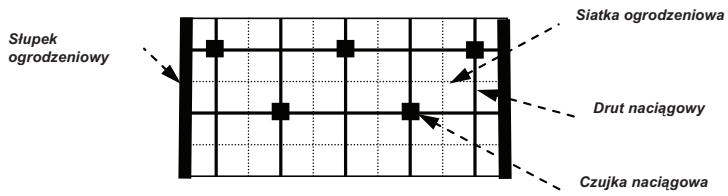
Ze względu na swoją specyfikę, komputerowe systemy ochrony peryferyjnej, oprócz innych urządzeń technicznych rozpoznawania zmian stanu ochranianego obszaru i znajdujących się na nim obiektów (klasyczne czujki ruchu, kamery telewizji przemysłowej itp.), wykorzystują specjalnie konstruowane czujki naciągowe, przeznaczone do montowania w ogrodzeniach (tzw. barierach ochronnych lub barykadach), wykorzystywanych jako specyficzne urządzenia ochrony [2]. Czujki takie montuje się w ogrodzeniu, łącząc przez nie kolejne fragmenty tzw. drutu naciągowego, rozciągniętego pomiędzy słupkami całego ogrodzenia bądź jego segmentu. Druty te stanowią fizyczną przeszkodę dla ewentualnego intruza, a jednocześnie są elementami przewodzącymi sygnały elektryczne od czujek naciągowych do centrali systemu ochrony. Czujka będzie generować sygnał alarmu w przypadku, gdy wskutek celowej działalności intruza lub przypadku (np. oparcie się o ogrodzenie, próba jego sforsowania) zostanie zmieniona siła naciągu związanych z nią drutów naciągowych.

Na zmianę siły naciągu drutów naciągowych wpływ ma wiele czynników, z których za najważniejsze najczęściej uznaje się następujące:

- działanie intruza − próba przejścia ponad ogrodzeniem, podniesienie ogrodzenia i przejścia pod ogrodzeniem, taranowanie ogrodzenia np. pojazdem mechanicznym itp.
- oddziaływanie czynników atmosferycznych − padający śnieg osiadający na ogrodzeniu, oblodzenie ogrodzenia, napór wiatru, zmiany temperatury
- przypadkowe potrącenie ogrodzenia przez np. zwierzęta − uderzenie w ogrodzenie przez duże zwierzę, nacisk wywołany przez siadające duże ptaki.

Oddziaływanie wszystkich wymienionej wyżej czynników jest przypadkowe i nie można z całą pewnością określić ani czasu ich wystąpienia, ani natężenia, ani czasu trwania.

Schemat elementu (segmentu) bariery ochronnej (barykady) przedstawia rysunek 1.



Rys. 1. Schemat elementu barykady z wmontowanymi czujkami naciągowymi

W uproszczeniu, funkcjonowanie czujki naciągowej polega na wysyłaniu sygnału alarmu po przekroczeniu pewnej, ustalanej indywidualnie dla każdej czujki, granicznej dopuszczalnej siły naciągu związanego z nią drutu naciągowego, nazywanej dalej wartością progową siły naciągu. Zatem funkcjonowanie takiej czujki można opisać następująco: jeżeli wskutek naciągnięcia siatki ogrodzeniowej, spowodowanego np. próbą przejścia przez nią intruza, wytworzy się tak duża siła naciągu w co najmniej jednym drucie naciągowym przytwierdzonym do czujki naciągowej, że będzie ona przewyższać ustaloną wartość progową, to czujka wyemituje sygnał alarmu. W przeciwnym przypadku sygnał alarmu nie będzie emitowany.

W zależności od rozwiązań technicznych, czujka może emitować sygnał alarmu natychmiast po przekroczeniu progowej wartości siły naciągu w przyłączonym do niej drucie naciągowym lub taki sygnał będzie emitowany dopiero wtedy, gdy przekroczenie progowej wartości siły naciągu będzie trwało ciągle co najmniej przez określony czas, a jeżeli siła naciągu przed upływem tego czasu ulegnie zmniejszeniu – sygnał alarmu nie zostanie wyemitowany. Najczęstszym rozwiązaniem jest rozwiązanie łączące te dwa omówione, a więc aby sygnał alarmu został wyemitowany, muszą być spełnione jednocześnie dwa następujące warunki:

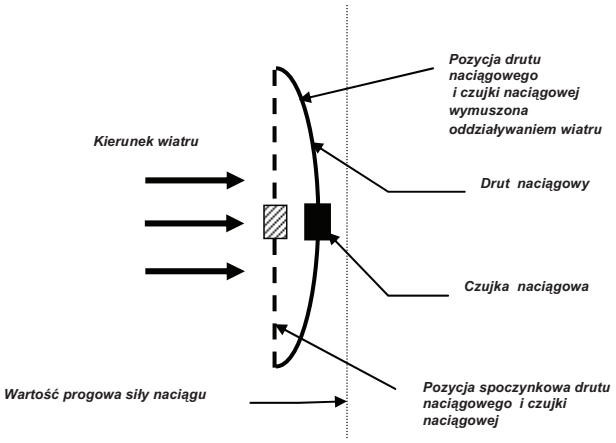
- siła naciągu drutu naciągowego musi przekroczyć wartość progową siły naciągu (**PN**), inaczej – przewyższyć wartość progową
- czas trwania tego przewyższenia nie może być krótszy od czasu progowego (**PC**), tj. ustalonego dopuszczalnego maksymalnego czasu trwania przewyższenia.

Zatem, dobierając dla każdego układu czujnik naciągowy – druty naciągowe (z nim związane) odpowiednie wartości PN oraz PC, można sterować czułością systemu ochrony, którą można interpretować jako odporność systemu na różnego rodzaju zakłócenia przypadkowe (losowe), w szczególności na

fałszywe alarmy, spowodowane przyczynami losowymi. Trzeba jednak wyraźnie stwierdzić, że zwiększając tak określaną czułość systemu ochrony, osiąga się małą odporność na fałszywe alarmy, gdyż nawet małe przypadkowe ugięcie barykady będzie powodowało wywołanie alarmu. Z drugiej jednak strony duża czułość systemu to gwarancja, iż system prawidłowo zareaguje na próbę celowego działania intruza, nawet przy zastosowaniu przez niego odpowiednio delikatnych metod pokonania barykady oraz będzie dobrze wykrywał stany fałszywego spokoju. Zmniejszając czułość systemu ochrony, powoduje się zwiększenie jego odporności na fałszywe alarmy, ale także, najczęściej, jednoczesne zmniejszenie odporności na celowe działanie intruza oraz stany fałszywego spokoju. Zatem właściwy dobór wielkości PN i PC ma istotne znaczenie dla poprawnego funkcjonowania systemu ochrony peryferyjnej.

Za najczęstszą przyczynę występowania fałszywych alarmów, związanych z funkcjonowaniem barykad, na ogół przyjmuje się oddziaływanie czynników, które mają charakter losowy oraz ciągły i zmienny w czasie; szczególnie dotyczy to parcia wiatru na ogrodzenie z czujnikami naciągowymi – barierę ochronną (barykadę).

Skutki oddziaływania wiatru na układ czujnik naciągowy – druty naciągowe, wmontowany do bariery ochronnej, przedstawiono schematycznie na poniższym rysunku 2.



Rys. 2. Schematyczny obraz odkształceń barykady pod wpływem oddziaływania na nią czynnika losowego (wiatru)

W praktyce wielkość **PN** jest wyrażana za pomocą wielkości dopuszczalnej amplitudy odchylenia (np. w milimetrach) bariery ochronnej i wmontowanego do niej układu czujnik naciągowy – druty naciągowe od stanu spoczynkowego, przy osiągnięciu której czujnik naciągowy może już wyemitować sygnał alarmu.

Zależność opisującą zmianę siły naciągu drutów ogrodzenia w funkcji czasu, w tym także zmianę siły naciągu drutów naciągowych, wywołaną czynnikami losowymi, można traktować jako proces stochastyczny (funkcję losową) klasy CC.

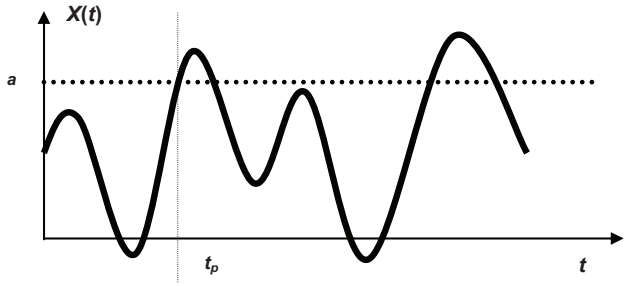
Po określeniu wartości **PN** na podstawie parametrów tego procesu, można będzie obliczyć prawdopodobieństwo przewyższenia tej wartości progowej przez omawiany proces oraz oczekiwaną długość przedziału czasu (oczekiwanego czasu) trwania takiego przewyższenia, tj. oczekiwanego czasu „przebywania" procesu ponad przyjętą wartością progową siły naciągu. Obliczone wartości tych wielkości mogą zostać wykorzystane do oceny poziomu czułości systemu ochrony, funkcjonującego w określonych warunkach i przy zadanych poziomach **PN** oraz **PC**, a więc również do oceny odporności systemu na mogące wystąpić sytuacje powodujące możliwość wytworzenia fałszywych alarmów.

3. Sformułowanie i rozwiązanie problemu [3, 5-7]

W dalszych rozważaniach przyjmuje się, że czynniki losowe mogące wpływać na powstawanie fałszywych alarmów powodują losowe w czasie zmiany naciągu drutów naciągowych, które będą opisywane za pomocą ciągłego w czasie procesu stochastycznego $X(t)$ klasy CC. O procesie $X(t)$ zakłada się, że jest to proces stacjonarny, ergodyczny, różniczkowalny średniokwadratowo ([1], ss. 94-96, [4], ss. 327--328). Niech a oznacza przyjętą wartość PN. Rozpatrywane dalej zadanie polega na wyznaczeniu dla wymienionego procesu stochastycznego $X(t)$:

- prawdopodobieństwa przewyższenia przez ten proces ustalonej wartości PN równej a
- wartości oczekiwanej czasu trwania takiego przewyższenia.

Przykładową realizację omawianego procesu stochastycznego $X(t)$, obrazującego zmianę naciągu drutu naciągowego w funkcji czasu, przedstawiono na rysunku 3, na którym przez t_p oznaczono chwilę osiągnięcia przez ten proces wartości progowej a:



Rys. 3. Przykładowa realizacja procesu stochastycznego opisującego zmianę naciągu drutu czujki naciągowej

Rozwiązanie sformułowanego wyżej zadnia będzie polegało na znalezieniu prawdopodobieństwa możliwości przyjęcia przez proces $X(t)$ wartości większych od ustalonej wartości progowej a oraz na wyznaczeniu rozkładu prawdopodobieństwa czasu przebywania rozpatrywanego procesu stochastycznego ponad tą ustaloną wartością progową, tj. rozkładu prawdopodobieństwa zmiennej losowej określającej długość odcinka czasu, w którym proces będzie miał przez cały czas wartości nie niższe niż ustalona wartość progowa. Tak sformułowane zadanie znane jest pod nazwą zagadnienia o przewyższeniu.

Rozwiązanie zagadnienia o przewyższeniu napotyka na istotne trudności obliczeniowe w przypadku określania rozkładu prawdopodobieństwa czasu przebywania rozpatrywanego procesu stochastycznego ponad ustaloną wartością progową. Na szczęście jednak w praktyce najczęściej wystarczająca jest znajomość oczekiwanej wartości czasu przebywania procesu stochastycznego ponad ustaloną wartością progową, co znacznie ułatwia osiągnięcie rozwiązania analitycznego.

Przedstawiane dalej ogólne zależności są prawdziwe dla dowolnych procesów stochastycznych klasy CC, natomiast końcowe, praktycznie przydatne formuły obliczeniowe można uzyskać stosunkowo prosto jedynie dla procesów stochastycznych normalnych.

Zgodnie z tym, co już powiedziano wcześniej, jako pierwsze zostanie rozpatrzone zagadnienie określenia prawdopodobieństwa $P(a,t)$ przewyższenia przez proces $X(t)$ wartości progowej a w przedziale czasu [0, t]. W celu rozwiązania tego zagadnienia rozważmy prawdopodobieństwo tego, że w nieskończenie małym przedziale czasu dt, następującym bezpośrednio po chwili t, proces $X(t)$ przewyższy wartość progową a. Aby takie zdarzenie nastąpiło, muszą być spełnione dwa następujące warunki:

- wartość procesu w chwili t musi być mniejsza od a, tj.
$$X(t) < a \tag{1}$$
- wartość procesu w chwili $t+dt$ musi być większa od a, tj.
$$X(t+dt) > a\,. \tag{2}$$

Zatem poszukiwane prawdopodobieństwo przewyższenia przez proces wartości progowej a w przedziale czasu dt jest równe
$$P\{X(t) < a \wedge X(t+dt) > a\} \tag{3}$$

Korzystając z założenia o ciągłości procesu $X(t)$ oraz uwzględniając prędkość zmian wartości tego procesu, wyżej podany układ nierówności można zastąpić z dowolnie dużą dokładnością dla dowolnie małego przedziału dt następującą równością
$$X(t+dt) = X(t) + V(t)dt\,,$$
gdzie $V(t)$ jest prędkością zmian wartości procesu $X(t)$ w chwili t, tj. zmian wartości amplitudy odchylania się bariery ochronnej od jej stanu spoczynkowego (normalnego).

Uwzględniając powyższą równość w wyrażeniu (1), otrzymuje się
$$P\{a - V(t)dt < X(t) < a\} \text{ dla } V(t) > 0\,. \tag{4}$$

Niech $f(X,V\,|\,t)$ oznacza funkcję gęstości dwuwymiarowego rozkładu procesu $X(t)$ i jego prędkości $V(t)$ w chwili t. Zatem prawdopodobieństwo (4) będzie równe
$$P\{a - V(t)dt < X(t) < a\} = \int_0^\infty \int_{a-vdt}^{a} f(x,v\,|\,t)dxdv\,, \tag{5}$$
gdzie granice całkowania obejmują wszystkie wartości $X(t)$ i $V(t)$ spełniające nierówność $a - V(t)dt < X(t) < a$ dla $V(t) > 0$.

Po przekształceniu zależności (5) z uwzględnieniem tego, że dt jest dowolnie małym przedziałem czasu, otrzymuje się
$$P\{a - V(t)dt < X(t) < a\} = \int_0^\infty f(a,v\,|\,t)vdv. \tag{6}$$

Ze względu na to, że prawdopodobieństwo przewyższenia wartości progowej a w nieskończenie małym przedziale czasu dt jest proporcjonalne do długości tego przedziału, celowe jest wprowadzenie funkcji gęstości $p(a|t)$, oznaczającej prawdopodobieństwo przewyższenia wartości progowej a przez proces $X(t)$ w jednostce czasu. Uwzględniając przyjęte założenie w wyrażeniu (4), otrzymuje się
$$P\{a - V(t)dt < X(t) < a\} = p(a\,|\,t)\,. \tag{7}$$

Z porównania zależności (6) i (7) wynika, że:

$$p(a \mid t) = \int_0^\infty f(a, v \mid t) v dv . \tag{8}$$

Prowadząc podobne rozważania, można wyznaczyć funkcję gęstości $p'(a|t)$, oznaczającą prawdopodobieństwo przekroczenia przez rozważany proces stochastyczny wartości progowej a z góry w dół w jednostce czasu:

$$p'(a \mid t) = -\int_{-\infty}^0 f(a, v \mid t) v dv .$$

Korzystając z zależności (8), można obliczyć dla dowolnego przedziału czasu o długości T oczekiwany czas przebywania procesu $X(t)$ nad wartością progową a.

Niech wymieniony wyżej przedział czasu zostanie podzielony na n równych podprzedziałów o długości dt każdy, tj. $[t_j, t_j+dt]$, $(j=1,2,...,n)$. Prawdopodobieństwo tego, że wartość procesu $X(t)$ przewyższy wartość progową a w przedziale czasu o numerze j, jest równe:

$$P\{X(t_j) \geq a\} = \int_a^\infty h(x \mid t_j) dx . \tag{9}$$

Jeżeli długość dt rozpatrywanych przedziałów będzie na tyle mała, że możliwe będzie zaniedbanie przypadków wielokrotnego (co najmniej dwukrotnego) przechodzenia w każdym z tych przedziałów przez proces $X(t)$ granicy określonej przez wartość progową a, zasadne będzie wprowadzenie zmiennych losowych Δj, z których każda przyjmuje wartość równą zeru lub dt, w zależności od tego, czy w j-tym przedziale proces $X(t)$, tj. $X(t_j)$, ma wartość mniejszą od a, czy nie. Stąd

$$\Delta_j = \begin{cases} dt, & \text{gdy } X(t_j) \geq 0, \\ 0, & \text{gdy } X(t_j) < 0. \end{cases} \tag{10}$$

Stąd sumaryczny czas przebywania procesu $X(t)$ w dowolnym przedziale czasu o długości T ponad wartością progową a jest zmienną losową postaci:

$$T_a = \sum_{j=1}^n \Delta_j . \tag{11}$$

Wartość oczekiwana tej zmiennej losowej wynosi:

$$E(T_a) = \sum_{j=1}^n E[\Delta_j] . \tag{12}$$

Ze względu na to, że, zgodnie z założeniem, zmienna losowa Δ_j może przyjmować tylko dwie wartości: dt lub 0, jej wartość oczekiwana jest równa iloczynowi dt przez prawdopodobieństwo $P\{X(t) \geq a\}$ i stąd:

$$E[\Delta_j] = dt \int_a^\infty h(x \mid t) dx .$$

Uwzględniając powyższe wyrażenie w zależności (12) i przechodząc do granicy dla $n \to \infty$, otrzymuje się

$$E(T_a) = \int_0^T \int_a^\infty h(x \mid t) dx dt . \tag{13}$$

W zastosowaniach praktycznych interesujący jest zazwyczaj oczekiwany czas przebywania procesu ponad wartością progową nie w dowolnym przedziale czasu, ale oczekiwany czas trwania tylko jednego takiego przewyższenia. Niech τ oznacza zmienną losową określającą czas trwania jednego przewyższenia procesu $X(t)$ nad wartością progową a. Wartość oczekiwana tej zmiennej losowej jest ilorazem wartości średniej $E(T_a)$ i oczekiwanej liczby przewyższeń $E(N_a)$ przez proces $X(t)$ wartości progowej a w rozważanym dowolnym przedziale czasu o długości T. W celu wyznaczenia poszukiwanej wartości oczekiwanej zmiennej losowej τ zostanie zastosowane takie samo podejście, jak przy wyznaczaniu wartości oczekiwanej $E(T_a)$. Zatem przedział czasu o długości T dzieli się na n równych podprzedziałów długości dt każdy, tj. $[t_j, t_j + dt]$, $(j = 1, 2,...,n)$. Jeżeli długość dt tak utworzonych przedziałów będzie na tyle mała, że możliwe będzie zaniedbanie przypadków wielokrotnego (co najmniej dwukrotnego) przechodzenia w każdym z tych przedziałów przez proces $X(t)$ granicy określonej przez wartość progową a, możliwe będzie wprowadzenie zmiennych losowych ξ_j, z których każda przyjmuje wartość równą jedności lub zeru, w zależności od tego, czy wewnątrz j-tego przedziału ma miejsce przewyższenie przez proces $X(t)$ wartości progowej a, czy nie. Stąd sumaryczna liczba przewyższeń N_a w rozpatrywanym przedziale czasu o długości T będzie równa

$$N_a = \sum_{j=1}^n \xi_j . \tag{14}$$

Wartość oczekiwana zmiennej losowej N_a będzie obliczana z następującej zależności:

$$\begin{aligned} E(N_a) &= \lim_{n \to \infty} \sum_{j=1}^n p(a \mid t_j) dt = \\ &= \int_0^T \int_a^\infty v \cdot f(a, v \mid t) dv dt. \end{aligned} \tag{15}$$

Wartość oczekiwana $E(\tau)$ czasu τ trwania jednego przewyższenia procesu $X(t)$ nad

wartością progową a przy uwzględnieniu zależności (13) i (15) jest obliczana z następującej zależności:

$$E(\tau)=\frac{\int_0^T\int_a^\infty h(x\mid t)dxdt}{\int_0^T\int_0^\infty v\cdot f(a,v\mid t)dvdt}. \tag{16}$$

Powyższe zależności znacznie się upraszczają dla procesów stacjonarnych, bowiem także funkcje gęstości $f(x|t)$ i $f(x,v|t)$ przestają zależeć od czasu i przyjmują, odpowiednio, postacie $f(x)$ oraz $f(x,v)$. Zatem dla procesów stacjonarnych będą obowiązywały następujące zależności:

$$E(T_a)=T\int_a^\infty h(x)dx, \tag{17}$$

$$E(N_a)=T\int_0^\infty v\cdot f(a,v)dv, \tag{18}$$

$$E(\tau)=\frac{\int_a^\infty h(x)dx}{\int_0^\infty v\cdot f(a,v)dv}. \tag{19}$$

Ponieważ, jak wynika z zależności (19), dla procesów stacjonarnych oczekiwana wartość $E(\tau)$ czasu τ trwania jednego przewyższenia procesu $X(t)$ nad wartością progową a nie zależy od długości przedziału czasu T, można dla tych procesów określić oczekiwaną liczbę n_a przewyższeń w jednostce czasu przez proces $X(t)$ wartości progowej a. Wyraża się ona następującą zależnością:

$$n_a=\frac{E(N_a)}{T}=\int_0^\infty v\cdot f(a,v)dv. \tag{20}$$

Uwzględniając zależność (20) w (18), otrzymuje się:

$$E(N_a)=n_a\cdot T. \tag{21}$$

Ponieważ w przytoczonych wyżej zależnościach występują funkcje gęstości prawdopodobieństw rozkładów różnych zmiennych losowych kształtujących rozpatrywany proces stochastyczny, do uzyskania przydatnych praktycznie formuł konieczna jest ich znajomość, co w ogólnym przypadku jest trudne. Natomiast stosunkowo łatwo można uzyskać zależności obliczeniowe w przypadku stacjonarnego normalnego procesu stochastycznego. Niestety, w praktyce procesy opisujące zachowanie się barier ochronnych pod wpływem oddziaływania czynników losowych nie zawsze są procesami stacjonarnymi i w dodatku – normalnymi. Zatem uzyskane zależności przy założeniu stacjonarności i normalności rozpatrywanego procesu stochastycznego $X(t)$ mają niewątpliwy walor poznawczy w odniesieniu do analizy rozpatrywanego zjawiska, ale uzyskane na ich podstawie wyniki należy traktować jako dane szacunkowe. Weryfikacja tych danych musi następować na gruncie statystyki. Pomimo tych zastrzeżeń jednak przyjęcie stacjonarności i normalności procesu jest nieraz jedynym wyjściem w sytuacji, gdy zachodzi konieczność dokonania a priori ilościowej oceny rozpatrywanego zjawiska, tzn. w warunkach, gdy nie ma jeszcze możliwości przeprowadzenia badań statystycznych na gotowej barierze ochronnej.

Stacjonarny normalny proces stochastyczny jest jednoznacznie określony, gdy znana jest jego wartość oczekiwana m_x i funkcja korelacji $K_x(\tau)$. Funkcja gęstości rozkładu prawdopodobieństwa tego procesu ma następującą postać:

$$f(x)=\frac{1}{\sigma_x\sqrt{2\pi}}\exp\left[-\frac{(x-m_x)^2}{2\sigma_x^2}\right], \tag{22}$$

przy czym wariancja jest równa

$$\sigma_x^2=K_x(0). \tag{23}$$

W przypadku stacjonarnego normalnego procesu stochastycznego jego wartość i prędkość zmian tej wartości dla ustalonej chwili są niezależnymi zmiennymi losowymi. Dlatego dwuwymiarowa gęstość rozkładu prawdo-podobieństwa f(x,v) jest w tym przypadku prosta do wyliczenia i równa:

$$f(x,v)=\frac{1}{\sigma_x\sqrt{2\pi}}\exp\left[-\frac{(x-m_x)^2}{2\sigma_x^2}\right]\cdot \cdot\frac{1}{\sigma_x\sqrt{2\pi}}ex\left[-\frac{v^2}{2\sigma_v^2}\right], \tag{24}$$

gdzie wariancja σ_v^2 procesu $V(t)$ jest obliczana z następującej zależności:

$$\sigma_v^2=-\left.\frac{d^2K_x(\tau)}{d\tau^2}\right|_{\tau=0}, \tag{25}$$

a wartość oczekiwana tego procesu jest równa zeru ze względu na stacjonarność procesu $X(t)$.

Uwzględniając wyrażenie (24) w (20), otrzymuje się:

$$n_a=p(a)=\frac{\sigma_v}{2\pi\sigma_x}\exp\left[-\frac{(a-m_x)^2}{2\sigma_x^2}\right]= =n_0\cdot\exp\left[-\frac{(a-m_x)^2}{2\sigma_x^2}\right], \tag{26}$$

przy czym n_0 oznacza oczekiwaną liczbę przewyższeń przez proces $X(t)$ swojej wartości oczekiwanej w jednostce czasu.

Uwzględniając (26) w (19), otrzymuje się:

$$E(\tau) = \pi \frac{\sigma_x}{\sigma_v} \cdot \exp\left[-\frac{(a-m_x)^2}{2\sigma_x^2} \right] \cdot \left[1 - \Phi\left(\frac{a-m_x}{\sigma_x} \right) \right], \quad (27)$$

gdzie funkcja $\Phi(x)$ oznacza całkową funkcję Laplace'a.

Jednym z ważniejszych zagadnień praktycznych w procesie eksploatacji barier ochronnych jest zagadnienie wyznaczania prawdopodobieństwa tego, że przy zadanej wartości progowej a, określającej, jak wiadomo, dopuszczalną wielkość amplitudy wychylenia tej bariery ochronnej pod wpływem np. wiatru, nie nastąpi w przedziale czasu o długości T ani jedno przewyższenie tej wartości progowej przez proces stochastyczny $X(t)$, opisujący, jak już też wiadomo, zachowanie tej bariery pod wpływem oddziaływania czynników losowych. Jest to zagadnienie trudne do rozwiązania na drodze analitycznej, nawet w przypadku procesów normalnych. Ułatwieniem w rozwiązaniu omawianego zagadnienia jest przypadek, gdy oczekiwana liczba przewyższeń w określonym przedziale czasu jest na tyle mała, że występowanie kolejnych przewyższeń można potraktować jako zdarzenia losowe niezależne. takim przypadku można przyjąć, iż liczba przewyższeń wartości progowej przez proces jest zmienną losową o rozkładzie Poissona i zagadnienie obliczenia prawdopodobieństwa tego, że w dowolnym przedziale czasu o długości T nie nastąpi ani jedno przewyższenie ustalonej wartości progowej przez rozpatrywany proces, może zostać rozwiązane w sposób satysfakcjonujący. Zależności (28-30) pozwalają obliczyć poszukiwane prawdopodobieństwo w przypadku procesu ogólnego, stacjonarnego oraz normalnego stacjonarnego:

$$P_0(a,t) = \exp\left[-\int_0^T \int_0^\infty v \cdot f(a,v \mid t) dv dt \right], \quad (28)$$

$$P_0(a,t) = \exp\left[-T \int_0^\infty v \cdot f(a,v) dv \right], \quad (29)$$

$$P_0(a,t) = \exp\left\{ -\frac{T}{2\pi} \cdot \sqrt{\left[-\frac{K_x''(\tau)}{K_x(\tau)} \right]} \cdot \exp\left[-\frac{(a-m_x)^2}{2\sigma_x^2} \right] \right\}. \quad (30)$$

W zagadnieniach praktycznych często korzysta się z oszacowania prawdopodobieństwa nieprzewyższenia wartości progowej a przez normalny stacjonarny proces stochastyczny $X(t)$ w przedziale czasu o długości T:

- oszacowanie od dołu:

$$P_0(a,T) \geq P_0^{\min} = \Phi\left(\frac{a-m_x}{\sigma_x} \right) - n_0 \cdot T \cdot \exp\left[-\frac{(a-m_x)^2}{2 \cdot \sigma_x^2} \right] \quad (31)$$

- oszacowanie od góry:

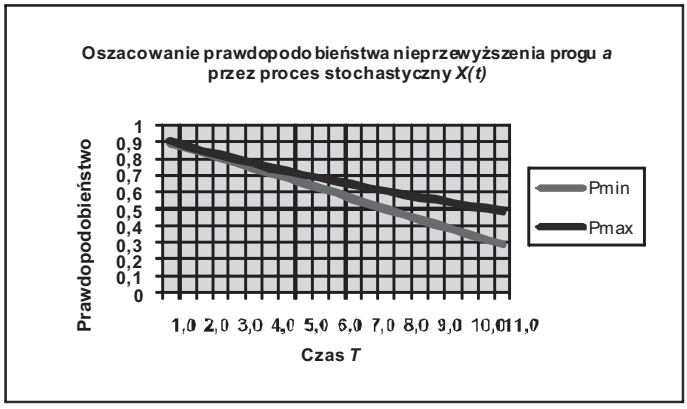
$$P_0(a,T) \leq P_0^{\max} = \Phi\left(\frac{a-m_x}{\sigma_x} \right) \cdot \exp\left\{ -n_0 \cdot T \cdot \exp\left[-\frac{(a-m_x)^2}{2 \cdot \sigma_x^2} \right] \right\} \quad (32)$$

Oszacowaniem (32) można posługiwać się w przypadku, gdy spełniona jest następująca nierówność:

$$T \leq \frac{\Phi\left(\frac{a-m_x}{\sigma_x} \right)}{n_0} \cdot \exp\left[\frac{(a-m_x)^2}{2 \cdot \sigma_x^2} \right]. \quad (33)$$

Przykład

Na przedstawionym na rys. 4 wykresie pokazano zmiany wartości dolnego i górnego oszacowania prawdopodobieństwa nieprzewyższenia wartości progowej $a = 16$ w funkcji czasu przez stacjonarny normalny proces stochastyczny $X(t)$ o wartości oczekiwanej $m_x = 9$ i odchyleniu standardowym $\sigma_x = 4$.



Rys. 4. Przykładowy przebieg krzywych dolnego i górnego oszacowania prawdopodobieństwa nieprzewyższenia wartości progowej wychylenia czujki naciągowej zamontowanej w barykadzie

4. Zakończenie

Przy rozwiązywaniu zadań praktycznych na ogół występują trudności związane z określeniem analitycznej postaci funkcji korelacyjnej procesu $X(t)$, koniecznej do obliczenia wielkości n_0, która z kolei jest niezbędna do wyznaczenia prawdopodobieństw (31) i (32).

W takim przypadku przyjmuje się najczęściej górne oszacowanie tej wielkości, które jest równe:

$$n_0 = \frac{1}{2\sqrt{\pi}}, \tag{34}$$

a zależności (31) i (32) przyjmą postać następujących wyrażeń:

- oszacowanie od dołu:

$$P_0(a,T) \geq P_0^{\min} = \\ = \Phi\left(\frac{a-m_x}{\sigma_x}\right) - \frac{1}{2\sqrt{\pi}} \cdot T \cdot \exp\left[-\frac{(a-m_x)^2}{2\cdot\sigma_x^2}\right] \tag{35}$$

- oszacowanie od góry:

$$P_0(a,T) \leq P_0^{\max} = \\ = \Phi\left(\frac{a-m_x}{\sigma_x}\right) \cdot \exp\left\{-\frac{1}{2\sqrt{\pi}} \cdot T \cdot \exp\left[-\frac{(a-m_x)^2}{2\cdot\sigma_x^2}\right]\right\} \tag{36}$$

które będzie można stosować przy spełnieniu warunku (33). W rozważanym przypadku zależności (35) i (36) dadzą dolne oszacowanie obliczanych prawdopodobieństw.

Jeżeli istnieje możliwość obserwacji procesu $X(t)$, to wielkość n_0 można będzie oszacować za pomocą metod statystycznych bez potrzeby znajomości analitycznej postaci funkcji korelacyjnej tego procesu.

W opracowaniu rozpatrywano dotychczas przypadek odchylenia bariery ochronnej od jej stanu spoczynkowego tylko w jedną stronę i dla tego przypadku zostały podane zależności. Gdyby czynniki losowe oddziałujące na barierę ochronną powodowały jej losowe odchylanie się od stanu spoczynkowego w obydwu kierunkach (np. w przód i w tył), to przy każdym takim odchyleniu mogłaby być przekroczona wartość progowa a, raz z jednej, a raz z drugiej strony, z identycznymi skutkami dla wszczęcia alarmu w systemie ochrony. Fakt ten powoduje dwukrotne zwiększenie wartości oczekiwanej zmiennej losowej N_a, określającej liczbę przewyższeń wartości progowej a przez proces $X(t)$ (zależność (21)), tj.:

$$E(N_a) = 2 \cdot n_a \cdot T. \tag{37}$$

5. Bibliografia

[1] D. Bobrowski, *Wstęp do losowych równań różniczkowych zwyczajnych*, PWN, Warszawa, 1987.

[2] G. Konopacki, J. Koszela, C. Opacki, *Inteligentne komputerowe systemy ochrony obiektów wojskowych. Wstępne teoretyczne rozpoznanie zagadnienia fałszywych alarmów w systemach ochrony wyposażonych w ogrodzenia typu „barykada". Eliminowanie fałszywych alarmów w systemach ochrony obiektów,* WAT, Warszawa, 2000.

[3] I.N. Kowalenko, N.J. Kuzniecow, W.M. Szumienkow, *Procesy stochastyczne. Poradnik*, PWN, Warszawa, 1989.

[4] A. Papoulis, *Prawdopodobieństwo, zmienne losowe i procesy stochastyczne*, WNT, Warszawa, 1972.

[5] E.C. Pierievierziev, *Słuczajnyje procesy v parametriczeskich modelach nadiożnosti*, Naukovaja Dumka, Kijev, 1987.

[6] S.M. Ross, *Stochastic processes*, John Wiley & Sons, New York, 1996.

[7] A.A. Swiesznikow, *Podstawowe metody funkcji losowych,* PWN, Warszawa, 1965.

The problem of eliminating false alarms in computer systems for the protection of peripheral

G. KONOPACKI, K. WORWA

The article examines the problem of protection of surface objects via a computer security system peripheral control security barricades set up in the form of integrated in its take-detectors. Examines the problem of false alarms in this type of protection systems, which are random and continuous and variable over time. Described in a formal way through a process of stochastic behavior of the barricade at the impact of random factors, and it is formulated and solves the task of determining the sensitivity of the detectors tightening to minimize the formation of false alarms.

Keywords: computer security system, false alarm