Biuletyn WAT
Vol. LXII, Nr 3, 2013

Świadomość sytuacyjna węzła mobilnej sieci doraźnej w rozpoznaniu elektronicznym

JOANNA GŁOWACKA, MAREK AMANOWICZ

Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Telekomunikacji,
00-908 Warszawa, ul. gen. S. Kaliskiego 2,
joanna.glowacka@wat.edu.pl, marek.amanowicz@wat.edu.pl

Streszczenie. W artykule została przedstawiona potrzeba budowania świadomości węzłów w zakresie bezpieczeństwa oraz identyfikacja możliwych rozwiązań dotyczących tej tematyki. Następnie przedstawiono koncepcję mechanizmu budowania świadomości sytuacyjnej węzła oraz jego użycie w mobilnej sieci doraźnej wykorzystywanej w rozpoznaniu elektronicznym.
Słowa kluczowe: telekomunikacja, świadomość sytuacyjna, zaufanie, metody wnioskowania, wojskowe sieci doraźne, rozpoznanie elektroniczne

1. Wstęp

Mobilne sieci doraźne ze względu na samoorganizację oraz brak potrzeby zestawiania stałej infrastruktury mają istotne znaczenie w działaniach wojskowych. Węzłami sieci stają się żołnierze wyposażeni w urządzenia komunikacyjne, ale również pojazdy załogowe i bezzałogowe, będące zarówno urządzeniami końcowymi jak i elementami infrastruktury sieci.

Standardowo wykorzystywane mechanizmy bezpieczeństwa sieci doraźnych, takie jak uwierzytelnienie i autoryzacja, stają się często niewystarczające w przypadku realizacji działań w środowisku zdegradowanym i nieprzyjaznym. Budowanie świadomości sytuacyjnej umożliwia uzupełnienie standardowo wykorzystywanych przez węzeł mechanizmów, zapewniając zwiększenie poziomu bezpieczeństwa i skuteczności transferu danych w sieciach doraźnych, mających szczególne znaczenie dla działań wojskowych.

2. Specyfika środowiska

Sieci ad-hoc są zbiorami niezależnych węzłów, które mogą się komunikować za pośrednictwem fal radiowych. Sieci te cechują się dużą dynamiką zmian topologii, ograniczonymi zasobami sieciowymi oraz podatnościami na różnego typu ataki. Wykorzystanie ogólnodostępnego środowiska transmisyjnego stwarza możliwości łatwego wstrzykiwania i podsłuchiwania wiadomości, natomiast wprowadzenie niepożądanych węzłów destabilizację struktury routingu. Prócz ataków złośliwych w sieciach ad-hoc bardzo powszechne są ataki egoistyczne, które mają na celu przywłaszczenie dużej ilości pasma. Jedną z najpopularniejszych metod zachowania egoistycznego jest nieprzekazywanie przez węzeł egoistyczny pakietów na rzecz innych węzłów w celu zaoszczędzenia własnej energii.

Zapewnienie bezpieczeństwa jest szczególnie trudne w przypadku taktycznych sieci ad-hoc, ze względu na konieczność radzenia sobie z wrogim środowiskiem, różnorodnością węzłów oraz rygorystycznymi ograniczeniami wydajności spowodowanymi bateryjnym zasilaniem urządzeń mobilnych, niską wydajnością stosowanych podzespołów i ograniczonym dostępnym pasmem transmisji.

3. Świadomość sytuacyjna węzła

Budowanie świadomości węzła rozumiane jest jako zdolność posiadania dokładnych informacji o otaczającej węzeł rzeczywistości i rozumienia (interpretowania) aktualnej sytuacji z punktu realizowanych zadań.

W heterogenicznych sieciach ad-hoc ukończenie misji zależne jest od zaufania, jakim darzą się węzły. Dzięki budowie świadomości węzłów możliwa jest ocena otoczenia w celu zwiększenia prawdopodobieństwa powodzenia misji.

Głównymi produktami mechanizmu budowania świadomości sytuacyjnej węzła są określone poziomy zaufania do węzłów znajdujących się w sieci oraz informacje umożliwiające wykrycie węzłów cechujących się wrogim i niekooperacyjnym zachowaniem.

4. Zaufanie

4.1. Pojęcie zaufania

Zaufanie jest pojęciem interdyscyplinarnym, posiada ono swoją definicję w wielu dziedzinach nauki, między innymi w socjologii, ekonomii, filozofii, psychologii, zarządzaniu organizacją, informatyce i telekomunikacji. W przypadku zaufania w sieciach ad-hoc jest ono tłumaczone jako zbiór relacji między jednostkami

posługującymi się podobnymi protokołami komunikacyjnymi [1]. Relacje te są określone na podstawie wcześniejszych interakcji jednostek. W [2] zaufanie traktowane jest jako stopień wiarygodności zachowania innych jednostek. Zaufanie dla sieci ad-hoc można zdefiniować jako poziom wiary, który może być przypisany przez dany węzeł innym węzłom na podstawie obserwacji i rekomendacji pochodzących od innych węzłów.

4.2. Właściwości zaufania

Zaufanie w sieciach ad-hoc powinno być:
- wielkością dynamiczną — poziom zaufania zmienia swoją wartość w zależności od zachowań węzła, którego dotyczy,
- asymetryczne — jeśli węzeł A posiada zaufanie do węzła B, nie oznacza to, że węzeł B posiada zaufanie do węzła A,
- nieprzechodnie — jeśli węzeł A posiada zaufanie do węzła B, a węzeł B do węzła C, nie oznacza to, że węzeł A posiada zaufanie do węzła C,
- subiektywne — poziom zaufania zależny jest od indywidualnej oceny węzła, który je określa,
- zależne od kontekstu — poziom zaufania do danego węzła może mieć różne wartości w zależności od kontekstu jakiego dotyczy, np. wysoki poziom zaufania odnośnie do energii, a niski w stosunku do bezpieczeństwa.

4.3. Metryki zaufania

Zaufanie nie posiada również jednoznacznie określonej metryki. Metryka umożliwia określenie poziomu zaufania w postaci ilościowej, dzięki czemu poziomy zaufania mogą być porównane.

Przykładowymi metrykami zaufania są: eBay [3] i Beta Reputation System [4]. W metryce eBay oceniana jest każda z transakcji, a punkty przyznawane są według następujących reguł: dla pozytywnego komentarza +1, dla neutralnego 0, zaś dla negatywnego –1. Wartość metryki zaufania w metryce eBay wyznaczana jest według następującego wzoru:

$$R_{eBay} = \frac{g}{n+g}, \tag{1}$$

gdzie: g — transakcje pozytywne;
n — transakcje nieudane.

W przypadku metryki Beta Reputation System każda z transakcji może przyjąć wartość +1 dla pozytywnej transakcji, –1 dla neutralnej bądź negatywnej transakcji. Obie wartości pozytywne i negatywne sumowane są oddzielnie:

$$R_{\text{BetaSystem}} = \frac{g - n}{n + g + 2}, \tag{2}$$

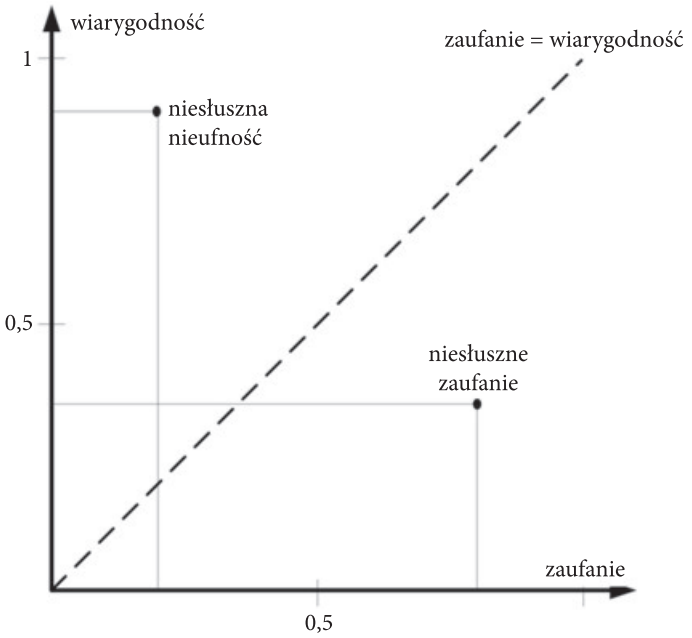
gdzie: g — transakcje pozytywne;
n — transakcje nieudane.

Przedstawione metryki określają wartość zaufania na podstawie transakcji, które zaszły w przeszłości.

4.4. Powiązanie zaufania, wiarygodności i ryzyka

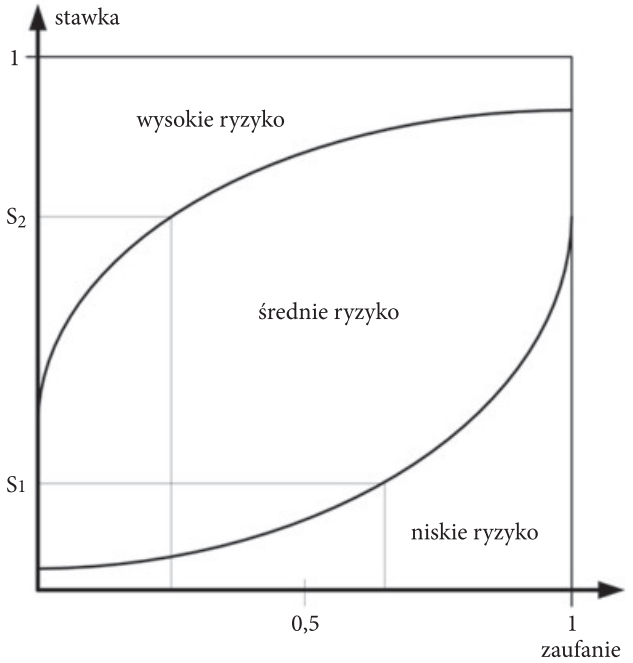
W literaturze pojęcia zaufanie (ang. *trust*) i wiarygodność (ang. *trustworthiness*) są często używane zamiennie. W [5, 6] wyjaśniono różnice między tymi wielkościami. Poprzez poziom zaufania rozumiane jest prawdopodobieństwo przekonania, na przykład w zakresie od 0 (brak zaufania) do 1 (całkowite zaufanie), zaś wiarygodność jest miarą prawdopodobieństwa, że węzeł zaufany zachowa się zgodnie z oczekiwaniem.

Na rysunku 1 przedstawiono różnice między zaufaniem i wiarygodnością. Linią przerywaną zaznaczono wartości, w których wielkości zaufania i wiarygodności są sobie równe.



Rys. 1. Zaufanie a wiarygodność [5]

Ryzyko rozumiane jest jako ilościowy bilans zagrożeń, strat wynikających z realizacji potrzeb w określonej sytuacji. Jak widać na rysunku 2, ryzyko jest zawsze niskie w przypadku zerowej stawki, podobnie w przypadku bardzo wysokiej stawki ryzyko jest zawsze wysokie niezależnie od poziomu zaufania. Najczęściej w przypadku wysokiego zaufania ryzyko jest niskie, jednak wartość ryzyka powinna być określana w oparciu o istniejące zagrożenia dla danej sytuacji, a nie poziom zaufania, gdyż ryzyko istnieje nawet w przypadku zaufania równego 1.

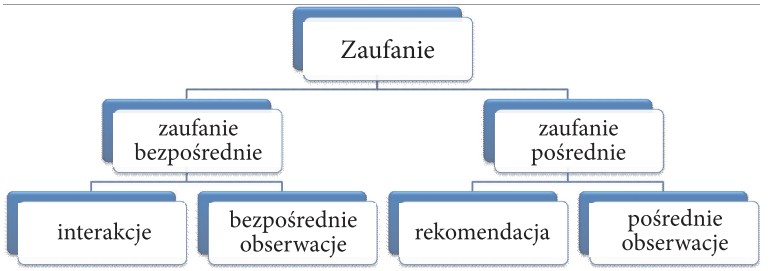


Rys. 2. Ryzyko a zaufanie [6]

5. Źródła danych procesu tworzenia świadomości sytuacyjnej

Zaufanie wyznaczane jest w większości przypadków na podstawie bezpośrednich interakcji, pośrednich obserwacji i rekomendacji (rys. 3).

Zaufanie określane przez węzeł na podstawie bezpośrednich interakcji i obserwacji zachowań innych węzłów nazywane jest zaufaniem bezpośrednim. Zachowania, na podstawie których wyznaczane jest zaufanie bezpośrednie, mogą dotyczyć: poprawności przekazywania rekomendacji — wykrywanie węzłów „kłamców", sprawdzania poprawności właściwości protokołu routingu, wykrywania niewspółpracujących węzłów oraz przestrzegania reguł bezpieczeństwa.



Rys. 3. Źródła danych procesu tworzenia świadomości sytuacyjnej

Zaufanie wyznaczone na podstawie pośrednich obserwacji i rekomendacji określane jest natomiast jako zaufanie pośrednie. Rekomendacje rozumiane są jako opinie innych węzłów odnośnie do węzła, dla którego określany jest poziom zaufania.

6. Analiza istniejących rozwiązań

Większość z dotychczasowych rozwiązań dotyczących zapewnienia bezpieczeństwa w mobilnych sieciach ad-hoc korzysta z zaadaptowanych mechanizmów bezpieczeństwa przeniesionych z sieci przewodowych. Typowe mechanizmy najczęściej nie umożliwiają weryfikacji przypisanego już węzłowi poziomu bezpieczeństwa węzłów, a tym bardziej podejmowania działań dotyczących ograniczenia ich uprawnień bądź współpracy z innymi węzłami.

Problem oceny węzłów, określania poziomu zaufania do węzłów w sieciach ad-hoc staje się ostatnio bardzo popularny i szeroko rozwijany w literaturze polskiej i światowej, co świadczy o wadze tego tematu.

6.1. Źródła danych procesu tworzenia świadomości sytuacyjnej

W analizowanych rozwiązaniach zaufanie wyznaczane jest w większości przypadków na podstawie bezpośrednich interakcji i rekomendacji.

W dokumencie [7] autorzy przedstawiają algorytm zaufanego ważonego grupowania TWCA (ang. *Trusted Weight Clustering Algorithm*). Zaufanie jest wyznaczane jako zaufanie bezpośrednie oraz zaufanie z rekomendacji. W pierwszym przypadku jest ono określane na podstawie bezpośrednich interakcji między dwoma węzłami. Interakcje klasyfikowane są jako pomyślne i nieprawidłowe. W drugim przypadku są wyznaczane na podstawie otrzymywanych rekomendacji od innych węzłów.

Przedstawiony w [8] model zaufania w oparciu o reputację SMRTI (*Secure MANET Routing with Trust Intrigue*) określa poziom zaufania na podstawie bezpośrednich interakcji z sąsiednimi węzłami, obserwacji oraz rekomendacji. Zostało

w nim przedstawione podejście do pobierania dowodów z rekomendacji, eliminując stronniczość.

W [9] została przedstawiona propozycja integracji podejścia opartego na polityce i reputacji dla adaptacyjnego systemu zarządzania zaufaniem. Zaufanie oparte na reputacji wyznacza poziom zaufania w oparciu o bezpośrednie opinie oraz rekomendacje. Rezultatem zarządzania zaufaniem opartym na polityce jest binarna decyzja, zgodnie z którą węzeł wysyłający zapytanie jest zaufany bądź nie, a tym samym określane jest, czy użytkownik posiada dostęp do zasobów.

W niektórych z rozwiązań wykorzystywane są również certyfikaty [10], ocena ryzyka [11] i reputacje [12].

6.2. Wagi informacji

Ze względu na różne źródła danych przy wyznaczaniu zaufania do węzłów uwzględniane są odpowiednie wagi dla różnych rodzajów informacji.

Protokół „CONFIDANT" — *Cooperation Of Nodes: Fairness In DynamicAdhoc Network* [13] — pracuje jako rozszerzenie reaktywnego protokołu routingowego dla sieci MANET. Ocena jest zmieniana zgodnie z funkcją oceniającą, która przyporządkowuje różne wagi dla danych typów zachowania. Największe wagi są przypisywane dla zdarzeń pochodzących z własnego doświadczenia, mniejsze dla zaobserwowanych w sąsiedztwie, a jeszcze mniejsze dla informacji z raportów. Uzasadnieniem takiego zachowania jest fakt, że węzeł ufa bardziej własnym obserwacjom niż informacjom otrzymanym od innych.

Dodatkową uwzględnianą wagą przy wyznaczaniu zaufania na podstawie rekomendacji jest waga proporcjonalna do poziomu zaufania węzła, który przekazuje rekomendacje [7, 8, 11, 14].

6.3. Wykrywanie węzłów „kłamców"

W sieciach MANET, gdzie świadomość węzła budowana jest na podstawie rekomendacji innych węzłów, bardzo często istnieje problem z węzłami „kłamcami" — węzłami przekazującymi nieprawidłowe rekomendacje dotyczące pozostałych węzłów w sieci oraz sposobu uwzględniania tych informacji. Sposób radzenia sobie z tym problemem został przedstawiony w [14]. Węzły wierzą informacjom z drugiej ręki jedynie w sytuacji, gdy nie różnią się one zbytnio od posiadanych przez nie informacji. Jest to nazwane testem odchylenia (ang. *deviation test*).

Model zaufania, uwzględniający radzenie sobie z kłamcami został również przedstawiony w [15], gdzie opisano sposób na łagodzenie skutków niepoprawnych ocen zaufania oraz w [16], gdzie opracowano model zaufania z pasywnym zaufaniem, które wykorzystywane było do filtrowania nieuczciwych obiektów.

6.4. Wykorzystywane metody wnioskowania

Najbardziej powszechną teorią przedstawienia wiedzy niepewnej jest teoria prawdopodobieństwa. Jednak niezależnie, w jaki sposób zostanie zdefiniowane prawdopodobieństwo, liczba je określająca odwzorowuje jedynie wiedzę obserwatora, a nie obiektywną jego wartość.

W artykule [17] został przedstawiony schemat Hermes ustalania zaufania, który ma pomóc w zapewnieniu niezawodności przesyłania pakietów. Zaproponowane rozwiązanie wykorzystuje Bayesowskie podejście do określania wartości zaufania. Jest ono wyliczane na podstawie prawdopodobieństwa modelowanego zgodnie z dystrybucją beta. Parametry dystrybucji beta są wyznaczane na podstawie zgromadzonych obserwacji zachowań podczas przekazywania pakietów.

W [18] sposób określania poziomu zaufania bazuje na teorii łańcuchów Markowa. Zaufanie jest wyznaczane na podstawie poprzednich zachowań w grupie. Proces ten jest ergodyczny w czasie. Czas określenia zaufania jest niezależny od warunków początkowych oraz klas zaufania. Określenie zaufania następuje w dwóch etapach: analiza poprzednich zachowań z wykorzystaniem teorii łańcuchów Markowa oraz wymiana określonego poziomu między członkami grupy.

Wnioskowanie probabilistyczne wykorzystywane jest również w [10-13, 15-16]. Umożliwia ono określenie w łatwy sposób poziomu zaufania do węzłów, jednak posiada pewne niedogodności. Klasyczna logika bazuje na dwóch wartościach reprezentowanych przez: 0 i 1 lub prawda i fałsz. Granica między nimi jest jednoznacznie określona i niezmienna. Dodatkowo klasyczna teoria prawdopodobieństwa nie pozwala na rozróżnienie niepewności (wyrażanej prawdopodobieństwem) od wiedzy niepełnej (braku wiedzy na dany temat).

Logika rozmyta stanowi rozszerzenie klasycznej logiki, wprowadza wartości pośrednie między standardowe 0 i 1, „rozmywa" granice między tymi wartościami. Jest wykorzystywana w sytuacjach, gdzie użycie klasycznej logiki stwarza problem z opisem matematycznym procesu lub gdy wyliczenie wymaganych zmiennych jest niemożliwe. Model zaufania oparty na podobieństwach rekomendacji (RFSTrust) określonych za pomocą matematyki rozmytej dla środowiska MANET, dla ochrony sieci przed węzłami samolubnymi został przedstawiony w [19]. Rozmyty model zaufania proponuje kwantyfikację i ocenę wiarygodności węzłów, która obejmuje pięć rodzajów relacji rekomendacji opartych na rozmytym zaufaniu.

Podobnie jak w przypadku wnioskowania opartego o klasyczną logikę, wnioskowanie rozmyte nie umożliwia rozgraniczenia wiedzy niepewnej od niewiedzy.

Kolejną z metod umożliwiających przedstawienie niepewności jest teoria ewidencji matematycznej. Teoria ta podobnie jak w przypadku logiki rozmytej pozwala na modelowanie rozmycia ocen. Umożliwia ona rozróżnienie wiedzy od niewiedzy oraz ma zastosowanie w przypadkach niepełnej informacji, składania ewidencji czy

aktualizacji przekonań. Dodatkowo w odróżnieniu od teorii Bayesa nie wymaga całkowitej specyfikacji modelu probabilistycznego.

Jedną z metod ewidencji jest teoria Dempstera-Shafera (DST) [20]. Podstawowym pojęciem teorii DST jest zbiór wszystkich hipotez, nazywany ramą rozróżniającą Θ. W modelu DST rama rozróżniająca składa się wyłącznie z elementów nienakładających się. Wykorzystanie teorii Dempstera-Shafera dla celów określenia zachowań niekooperacyjnych poszczególnych węzłów zostało przedstawione w [21-22]. Ocena kooperacyjności węzła odbywa się na podstawie obserwacji poprawności dostarczania pakietów, węzeł źródłowy określa dla każdego węzła w ścieżce funkcję nazywaną podstawowym przyporządkowaniem prawdopodobieństwa Θ. Każdy z węzłów w sieci wyposażony jest w dedykowany komponent realizujący algorytm oparty na teorii Dempstera-Shafera, który wykorzystuje odebrane rekomendacje oraz wyniki obserwacji. W rozwiązaniu zdefiniowane zostały dwa rodzaje zaufania. Pierwsze wyznacza, w jakim stopniu węzeł źródłowy ufa innemu węzłowi, że prześle on poprawnie pakiet. Do jego określenia wykorzystano funkcję przekonania zdefiniowaną przez teorię Dempstera-Shafera. Druga wartość zaufania określa stopień, w jakim węzeł ufa, że generowane przez inny węzeł rekomendacje są poprawne. DST umożliwia tworzenie jedynie skończonego, wyczerpanego i wyłącznego zbioru hipotez, w którym obowiązuje zasada wyłącznego środka.

Mimo wielości rozwiązań w literaturze brakuje rozwiązania, które w sposób wyczerpujący i spójny przedstawiałoby mechanizm zarządzania zaufaniem w sieciach MANET, uwzględniając jego proces określania, aktualizowania, przekazywania i przechowywania z istniejącymi ograniczeniami.

7. Koncepcja mechanizmu budowania świadomości sytuacyjnej węzła

7.1. Zbieranie informacji o węzłach

Zaproponowany mechanizm budowania świadomości węzłów jest procesem poznawczym, bazującym na obserwacji węzłów oraz uwzględniającym rekomendacje pochodzące od innych węzłów. Proces zbierania danych na temat zachowań węzłów składa się z następujących etapów:

— przechwytywania przekazywanych pakietów,
— analizy informacji zawartych w pakietach,
— oceny zachowań węzłów.

W zależności od rodzaju przechwytywanych pakietów oraz analizowanych w nich danych możliwe jest wykrywanie: niekooperacyjnych zachowań węzłów, przekazywania „przekłamanych" rekomendacji bądź nieprzestrzegania reguł bezpieczeństwa.

Rys. 4. Proces zbierania informacji o węzłach

7.1.1. Wykrywanie niekooperacyjnych zachowań

Niektóre z węzłów w sieciach ad-hoc cechują się samolubnym zachowaniem w celu pozbawienia innych węzłów udziałów, np. poprzez nieprzekazywanie przez węzeł egoistyczny pakietów na rzecz pozostałych węzłów, w celu zaoszczędzenia własnej energii. Wykrywanie węzłów niewspółpracujących możliwe jest przez śledzenie pakietów przekazywanych monitorowanemu węzłowi w czasie okresu rywalizacyjnego.

7.1.2. Przekazywanie „przekłamanych" rekomendacji

Jednym ze źródeł danych, na podstawie których określany jest poziom zaufania, są rekomendacje. Jednak uwzględnianie tych informacji wiąże się z możliwością występowania węzłów „kłamców" — węzłów przekazujących nieprawidłowe rekomendacje. Nieprawidłowe rekomendacje mogą przyczynić się do niewłaściwej oceny węzłów, a tym samym zmiany trasy przekazywania pakietów oraz danych do węzłów nieuprawnionych bądź niedostarczenia ich do węzła docelowego. Z tego względu konieczne jest wykrywanie „kłamców", nieuwzględnienie przekazywanych przez nie rekomendacji, a także zmniejszanie poziomu zaufania do tych węzłów.

Wykrycie węzłów „kłamców" możliwe jest dzięki porównaniu otrzymanych rekomendacji oraz posiadanych danych bezpośrednich dotyczących ocenianego węzła, a także informacji odnośnie do węzła przekazującego rekomendacje.

7.1.3. Nieprzestrzeganie reguł bezpieczeństwa

Pakiety, w ramach których przesyłane są wiadomości wrażliwe, mogą być etykietowane — zawierać informacje o poziomie wrażliwości danych. Dane o określonym poziomie wrażliwości mogą być przesyłane tylko do węzłów, które posiadają dostęp do informacji o określonym poziomie bądź poziomie wyższym. W celu weryfikacji przestrzegania reguł bezpieczeństwa węzeł przekazujący pakiet analizuje informacje na temat poziomu wrażliwości informacji oraz dostępu węzłów.

7.2. Wnioskowanie

Na podstawie pobranych i zgromadzonych informacji oraz rekomendacji węzły muszą wyciągnąć odpowiednie wnioski odnośnie poziomu zaufania do węzła. Jedną z metod eksploracji wiedzy jest fuzja danych.

Fuzja danych rozumiana jest jako metoda umożliwiająca łączenie i przetwarzanie wiedzy o badanym obiekcie lub zjawisku, pochodzącej z wielu różnych źródeł, tak aby uzyskać pełniejsze informacje, niemożliwe do osiągnięcia innymi metodami ani z każdego źródła danych osobno. Celem fuzji danych jest zmniejszenie niepewności końcowego wyniku oceny, zwiększenie efektywności klasyfikacji oraz poprawienie jakości identyfikacji.

Metodą, która umożliwia łączenie informacji niepewnych, skonfliktowanych i nieprecyzyjnych z wielu źródeł jest teoria Dezerta-Smarandache'a (DSmT) [23-25]. DSmT jest jedną z metod ewidencji i stanowi rozszerzenie DST. Wprowadza ona jednak wiele istotnych zmian, które umożliwiają łączenie informacji niepewnych, istotnie skonfliktowanych i nieprecyzyjnych.

W ramach teorii DSmT wyróżnia się dwa typy modeli:

— model swobodny — gdzie Θ składa się z wyczerpujących, ale niewyłącznych elementów, więc elementy mogą się wzajemnie nakładać,
— model hybrydowy — umożliwia modelowanie nieprecyzyjnych poglądów oraz ograniczeń wyłączności elementów Θ. W tym przypadku elementy mogą się nakładać, ale nie muszą.

DSmT wprowadza pojęcie zbioru hiperpotęgowego, który jest oznaczany przez D^{Θ}. Jest to zbiór wszystkich złożonych propozycji, które zostały utworzone z elementów Θ za pomocą operatorów ∩ oraz ∪. Przykładowo:

$$\begin{aligned} &\text{dla } \Theta = \{\theta_1, \theta_2\} \Rightarrow D^{\Theta} = \{\alpha_0, \alpha_1, ..., \alpha_4\}, \quad |D^{\Theta}| = 5, \\ &\alpha_0 = \varphi, \quad \alpha_1 = \theta_1, \quad \alpha_2 = \theta_1, \quad \alpha_3 = \theta_1 \cap \theta_2, \quad \alpha_4 = \theta_1 \cup \theta_2. \end{aligned} \tag{3}$$

Zastosowanie teorii Dezerta-Smarandache'a zapewnia określenie większej liczby hipotez, które umożliwią dokładniejszą ocenę zachowań. Dodatkowo dzięki tworzeniu hipotez wtórnych za pomocą operatorów sumy i iloczynu możliwa jest reprezentacja nieprecyzyjnych i niepewnych hipotez.

W trakcie obserwacji zachowań węzły mogą być oceniane jako:

— węzeł współpracujący (C) — węzeł przekazujący informacje,
— węzeł egoistyczny (E) — węzeł nieprzekazujący wiadomości,
— węzeł rzetelny (O) — węzeł przekazujący prawidłowe rekomendacje,
— węzeł kłamca (L) — węzeł przekazujący nieprawidłowe rekomendacje,
— węzeł bezpieczny (S) — węzeł przestrzegający zasady bezpieczeństwa,
— węzeł niebezpieczny (U) — węzeł nieprzestrzegający zasad bezpieczeństwa.

Zbiór wartości hipotez podstawowych w niektórych przypadkach może być niewystarczający do prawidłowej klasyfikacji węzłów. Prócz hipotez podstawowych istnieje możliwość określania hipotez wtórnych stworzonych z hipotez podstawowych za pomocą operatorów sumy i iloczynu logicznego. Wśród hipotez wtórnych możemy wyróżnić:

— węzeł niepewny współpracujący (*UC*) — węzeł, dla którego sprawdzana była poprawność przekazywania pakietów, ale nie ma możliwości podjęcia jednoznacznej decyzji, czy jest to węzeł współpracujący, czy egoistyczny

$$UC = C \cup E;$$

— węzeł podejrzany kłamca (*SL*) — węzeł, którego rekomendacje mogą być przekłamane, wartość przekazywanych rekomendacji odbiega od wcześniej zgromadzonej wiedzy oraz pozostałych rekomendacji, jednak różnica ta nie pozwala zarazem na stwierdzenie, że są one błędne i przekłamane

$$SL = H \cap L;$$

— węzeł niepewny rzetelny (*UH*) — węzeł, dla którego nie można określić, czy przekazywane przez niego rekomendacje są prawidłowe, ze względu na brak wcześniej zgromadzonej wiedzy

$$UH = H \cup L;$$

— węzeł podejrzany niebezpieczny (*SU*) — węzeł, którego zachowanie wskazuje na częściowe przestrzeganie reguł bezpieczeństwa, np. węzeł posiada dostęp do zasobów, do których nie jest uprawniony, ale udostępnia je tylko uprawnionym jednostkom

$$SU = S \cap U;$$

— węzeł niepewny bezpieczny (*US*) — węzeł, dla którego nie można określić, czy przestrzega reguł bezpieczeństwa ze względu na brak wiedzy dotyczącej poziomu dostępu węzłów

$$US = S \cup U.$$

Dzięki tak określonym hipotezom istnieje możliwość dokładniejszej oceny węzłów.

W celu uwzględniania rekomendacji pochodzących od węzłów sąsiednich oraz aktualizowania informacji o węźle wykorzystywana jest reguła kombinacji.

Poziom zaufania do węzła określany jest na podstawie zgromadzonych przesłanek dotyczących zachowania danego węzła oraz rekomendacji zebranych od węzłów sąsiednich. Do jego wyznaczenia może zostać wykorzystana funkcja przekonania zdefiniowana w ramach teorii ewidencji.

7.3. Przekazywanie rekomendacji

W przypadku braku bezpośrednich informacji na temat węzła, w celu wyznaczenia poziomu zaufania do węzła wykorzystywane są rekomendacje pochodzące od węzłów sąsiednich. Wymiana rekomendacji jest możliwa dzięki stworzonemu w tym celu protokołowi. W skład protokołu wchodzą trzy typy wiadomości:

- *Request* — wysyłana w przypadku, gdy węzeł nie posiada żadnych informacji na temat węzła znajdującego się w jego sąsiedztwie bądź gdy informacje są już nieaktualne. Wiadomość ta jest wysyłana multicastowo, do grupy węzłów o wysokim poziomie zaufania. Dodatkowo wiadomości te mogą być wysyłane do wszystkich węzłów sąsiednich (prócz węzła, którego ma dotyczyć) w celu weryfikacji poprawności przekazywanych przez nie rekomendacji.
- *Response* — wiadomość będąca odpowiedzią na Request, odsyłaną do węzła wysyłającego żądanie. Prócz informacji o poziomie zaufania przekazywany jest również znacznik czasu odpowiadający czasowi ostatniej aktualizacji oceny węzła.
- *Alert* — wiadomość wysyłana w trybie rozgłoszeniowym, zawierająca informacje o wyznaczonych poziomach zaufania do węzłów. Rekomendacje nie są wysyłane węzłowi, którego dotyczą.

8. Podsumowanie

Zaproponowany mechanizm budowania świadomości sytuacyjnej węzła umożliwia określenie poziomu zaufania do węzła na podstawie bezpośrednich obserwacji oraz rekomendacji pochodzących od węzłów sąsiednich. Ze względu na możliwość występowania nieprecyzyjnych, niespójnych bądź skonfliktowanych informacji pochodzących z różnych źródeł najbardziej odpowiednią metodą wnioskowania umożliwiającą uwzględnienie tych informacji jest DSmT. Wiedza gromadzona w ramach procesu budowania świadomości węzła może być wykorzystana jako uzupełnienie realizowanych projektów dotyczących efektywnego sterowania ruchem oraz zapewnienie bezpieczeństwa w mobilnych sieciach doraźnych wykorzystywanych w rozpoznaniu elektronicznym.

Artykuł powstał w ramach realizacji pracy naukowej finansowanej ze środków budżetowych na naukę w latach 2010-2013 jako projekt badawczy „Zaawansowane metody i techniki sterowania ruchem w taktycznych sieciach ad-hoc", PBW nr O N517 274839.

LITERATURA

[1] A. Chari, N. Kasiviswanth, K. Seshadri Ramana, *A survey on trust management for mobile ad hoc networks*, Int'l Journal of Network Security & Its Appl. (IJNSA), 2, 2, 2010.

[2] L. Capra, *Towards a Human Trust Model for Mobile Ad-hoc Networks*, Dept. of Computer Science, University College London.

[3] Jien Kato, Jie Li, Ruidong Li, *Future Trust Management Framework for Mobile Ad Hoc Networks*, IEEE Comm. Magazine, 2008, 108-114.

[4] Audun Jøsang, Roslan Ismail, *The Beta Reputation System*, 15th Bled Electronic Commerce Conf., Slovenia, June 17-19, 2002.

[5] B. Solhaug, D. Elgesem, K. Stolen, *Why Trust is not proportional to Risk*?, Proc. 2nd Int'l Conf. on Availability, Reliability and Security, Austria, 10-13 Apr. 2007, 11-18.

[6] A. Josang, S. LoPresti, *Analyzing the Relationship between Risk and Trust*, Proc. 2nd Int'l Conf. Trust Management, LNCS, 2004, 135-145.

[7] V.G. Rani, M. Punithavelli, *Optimizing On Demand Weight-Based Clustering Using Trust Model for Mobile Ad Hoc Networks*, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), 1, 4, December 2010.

[8] V. Balakrishnan, U. Kiran Tupakula, P. Lucs, V. Varadharajan, *Trust Enhanced Secure Mobile Ad-hoc Network Routing*, AINAW '07 Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops, vol. 02.

[9] Feng Yunfang, *Adaptive Trust Management in MANET*, 2007 International Conference on Computational Intelligence and Security.

[10] Jaydip Sen, Piyali Roy Chowdhury, Indranil Sengupta, *A Distributed Trust Mechanism for Mobile Ad Hoc Networks*, Ad Hoc and Ubiquitous Computing, ISAUHC '06, International Symposium, IEEE 2006.

[11] Tian Junfeng, Du Ruizhong, Ma Xiaoxue, Wang Zixian, *A Trust Model of P2P Network Based on Reputation and Risk*, World Congress on Software Engineering, IEEE 2009.

[12] Mingwu Zhang, Shenglin Zhu, Bo Yang, Wenzheng Zhang, *Trust-based Distributed Authentication Middleware in Ubiquitous Mobile Environments*, Third International Conference on Natural Computation, IEEE 2007.

[13] Jean-Yves Le Boudec, Sonja Buchegger, *Performance Analysis of the CONFIDANT Protocol* (*Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks*), IC/2002/01, January 2002.

[14] Jean-Yves Le Boudec, Jochen Mundinger, *Analysis of a reputation system for Mobile Ad-Hoc Networks with liars*, Performance Evaluation, 65, 2008, 212-226.

[15] Jianshu Weng, Zhiqi Shen, Chunyan Miao, Angela Goh Eck Soong, Cyril Leung, *How Agents Can Handle Unfair Third-Party Testimonies in Computational Trust Models*, IEEE Transactions on Knowledge and Data Engineering, 22, 9, September 2010, 1286-1298.

[16] Yanli Yu, Keqiu Li, Yong Zhang, Lianpeng Xu, *A Service Trust Model with Passive Trust*, 2008 IFIP International Conference on Network and Parallel Computing, IEEE 2008.

[17] C. Zouridaki, B.L. Mark, M. Hejmo, R.K. Thomas, *A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs*, In SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, New York, NY, USA, 2005, 1-10.

[18] Asmaa Adnane, Christophe Bidan, Rafael Timoteo de Sousa Junior, *Trust-based countermeasures for securing OLSR protocol*, 2009 International Conference on Computational Science and Engineering.

[19] Mingyu Fan, Xue Liu, Junhai Luo, *A trust model based on fuzzy recommendation for mobile ad-hoc networks*, Computer Networks, 53, 2009, 2396-2407.

[20] G. Shafer, *A mathematical theory of evidence*, Princeton U.P., Princeton, NJ, 1976.

[21] J. Konorski, R. Orlikowski, *DST-Based Detection of Non-cooperative Forwarding Behavior of MANET and WSN Nodes*, Proc. 2nd Joint IFIP WMNC., Gdansk, Poland, 2009.

[22] J. Konorski, R. Orlikowski, *Data-Centric Dempster-Shafer Theory-Based Selfishness Thwarting via Trust Evaluation in MANETs and WSNs*, IEEE International Conference on New Technologies, Mobility and Security NTMS 09, Cairo 20-23 December 2009.

[23] F. Smarandache, J. Dezert, *Advances and Applications of DSmT for Information Fusion*, 1, 2004.

[24] F. Smarandache, J. Dezert, *Advances and Applications of DSmT for Information Fusion*, 2, 2006.

[25] F. Smarandache, J. Dezert, *Advances and Applications of DSmT for Information Fusion*, 3, 2009.

J. GŁOWACKA, M. AMANOWICZ

Situational awareness of mobile ad-hoc network nodes for radio reconnaissance systems

Abstract. The article depicts the needs for building the situational awareness of military MANET nodes and identifying of some possible solutions. The authors present novel approach for situational awareness assessment and trust-based mechanisms that increase the efficiency and security of communications in military radio reconnaissance system.

Keywords: telecommunications, situation awareness, trust, inference methods, military ad-hoc network, radio reconnaissance