Reputacja, bezpieczeństwo i anonimowość w mobilnych sieciach ad hoc

Tomasz Ciszkowski
Instytut Telekomunikacji
Politechnika Warszawska
Maj 2007

Plan prezentacji

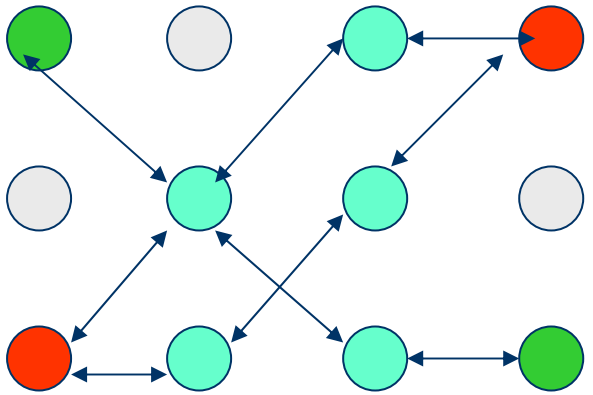
- Wprowadzenie do mobilnych sieci ad hoc (MANET)
- Bezpieczeństwo w MANET
- Anonimowość w MANET
- ANAP – protokół anonimowego uwierzytelnienia w mobilnych sieciach ad-hoc
- Rozproszony model reputacji węzłów

T.Ciszkowski@tele.pw.edu.pl

MANET – koncepcja sieci multi-hop (1)

- Zalety (w stosunku do single-hop)
  - Brak struktury, samoorganizacja węzłów sieci,
  - Wielościeżkowa komunikacja, zwiększająca wydajność
  - Krótszy zasięg radiowy, mniejsza moc nadajnika, stopień interferencji – mniejsze zużycie energii
- Wady
  - Liczba węzłów zaangażowanych w komunikację wzrasta
  - Bardziej skomplikowane protokoły komunikacji

- Sieć multi-hop



- PRnet (DARPA) – sieci bezprzewodowa typu multi-hop

T.Ciszkowski@tele.pw.edu.pl

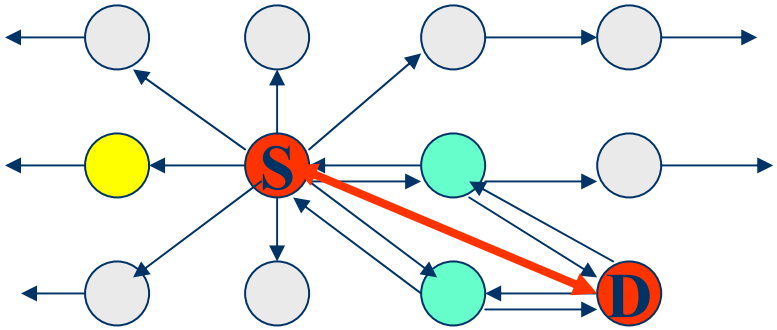
MANET – komunikacja (2)

- Routing w sieciach MANET – IETF
  - Warstwa IP (IETF)
  - Warstwa łącza danych (MAC – 802.1x)
  - Funkcje routingu
    - Odkrycie dwukierunkowej ścieżki pomiędzy węzłami źródłowym i docelowym
    - Zbudowanie tablica routingu (forwarding)
    - Utrzymanie ścieżki, detekcja uszkodzonych ścieżek

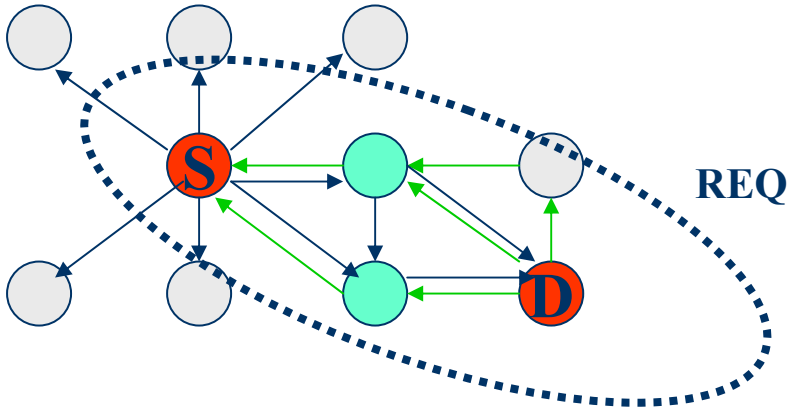
T.Ciszkowski@tele.pw.edu.pl

MANET (3) – Odkrycie ścieżki

- Reaktywne (na żądanie, DSR, AODV, ANAP)
  - REQEST, odrzucanie powtórzeń, D może wybrać kilka ścieżek
  - REPLY
  - Tworzenie tablic rutingu



- Proaktywne (stanu łącza) – HELLO (DSDV, LSR)



- Hybrydowe (LAR)

T.Ciszkowski@tele.pw.edu.pl

Bezpieczeństwo w MANET

- Bezpieczeństwo protokołów rutingu
  - Rozszerzenia istniejących wersji protokołów
  - Uwierzytelnianie
    - Współdzielony klucz sesyjny dla wszystkich węzłów
    - Klucz sesyjny dla każdej pary węzłów – ***N(N-1)/2***
    - Kryptografia klucza publicznego - ANAP

T.Ciszkowski@tele.pw.edu.pl

Anonimowość w MANET

- Anonimowość
  - Prywatność – ukrycie działalności
  - Anonimowość – ukrycie tożsamości całkowite lub nadanie użytkownikom pseudonimów
    - Unlinkability – niemożność powiązania stron
    - Unobservability – uniemożliwienie obserwowania komunikacji
    - Odpowiedzialność za działalność użytkowników – unieważnianie anonimowości na żądanie
- Propozycje protokołów (reaktywnych) gwarantujących bezpieczeństow i ananimnowość :
  - ANODR – całkowita anonimowość, ‘Trapdoor’, ‘Onion routing’,
  - MASK, anonimowe są pary węzłów, tunele szyfrowane, uwierzytelnienie w warstwie aplikacji,
  - SDAR, ‘Onion Routing’ – zmiana długości wiadomości, reputacja węzłów

T.Ciszkowski@tele.pw.edu.pl

ANAP – Anonymous authentication protocol for MANET (1)

- Cel – zapewniać bezpieczeństwo i anonimowość komunikacji użytkowników korzystających z sieci MANET
  - Uwierzytelnianie, wydajny mechanizm adresowania i przesyłania wiadomości, brak onion routingu
  - Faza inicjalizacji sieci - TA
  - Anonimowe odkrywanie ścieżki routingu z wzajemnym uwierzytelnieniem stron – podejście reaktywne
  - Utrzymanie ścieżki
  - Rozproszony system reputacji

T.Ciszkowski@tele.pw.edu.pl

ANAP (2)
Faza inicjalizacji sieci

- Wymagania
  - Każdy użytkownik posiada ***N x <pseudonim, klucz publiczny, klucz prywatny>***
  - Istnieje zaufana strona **TA** dystrybuująca wszystkim węzłom listę ***<pseudonim, klucz publiczny>***
  - Użytkownik związany z węzłem źródłowym zna przynajmniej jeden pseudonim użytkownika węzła docelowego
  - Anteny radiowe są dookólne – komunikacja dwukierunkowa
  - W środowisku znajdują się węzły skompromitowane

T.Ciszkowski@tele.pw.edu.pl

ANAP (3)
Anonimowe odkrywanie ścieżki

- Podejście reaktywne – na żądanie
- Trzyetapowy proces
  - Inicjalizacja anonimowego uwierzytelnienia - żądanie znalezienia węzła docelowego
  - Anonimowa odpowiedź
  - Anonimowe uwierzytelnienie obu stron – zestawienie kanału komunikacyjnego

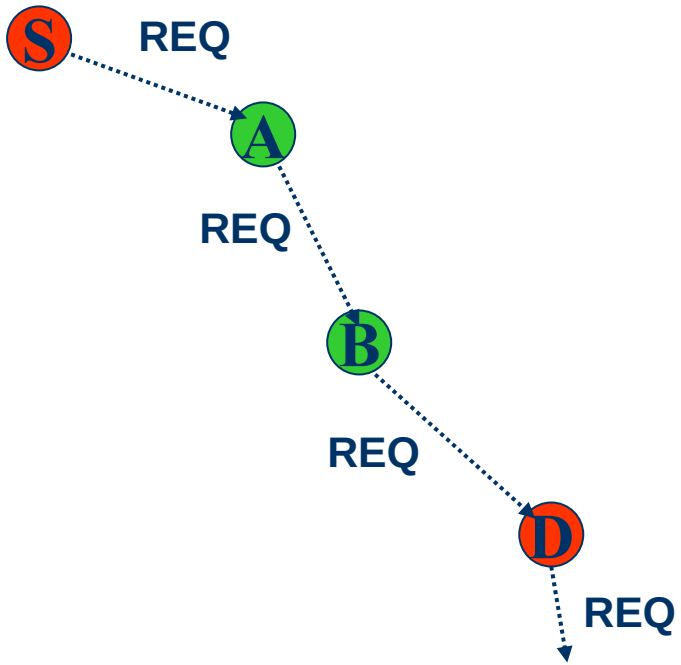
T.Ciszkowski@tele.pw.edu.pl

ANAP (4) - Inicjalizacja anonimowego uwierzytelnienia

S: $M_S = S_{ID}$, ISeq, L_P, P
S: $R_{ID} = h(D_{ID})$
S: REQ, R_{ID}, Seq, $E_{PK\_D}(M_S, Sig_S(M_S))$
S: $RqT_S \leftarrow < R_{ID}$, Seq, false >

A: REQ, R_{ID}, Seq, $E_{PK\_D}(M_S, Sig_S(M_S))$
A: $RT_A \leftarrow < R_{ID}$, Seq, S >
A: If $h(A_{ID}) \neq R_{ID}$ rebroadcast **REQ**

B: …
D: …

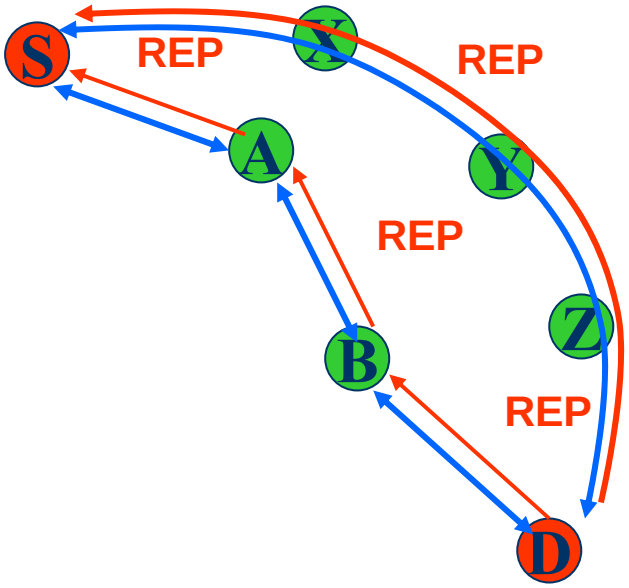


T.Ciszkowski@tele.pw.edu.pl

ANAP (5)
Anonimowa odpowiedź

D: h(D_{ID}) == R_{ID}; <S_{ID}, ISeq, L_P, P, Sig (M_S)>
D: Verify **Sig (M_S)**
D: RT_D : <R_{ID}, Seq> => B
D: SecK(K_N), K_N = K_{DB}
D: M_D = REP, F_{ID}, D_{ID}*, $K_{SES\_D,}$ ISeq+1, L_P, P
D: generate **K_{NN}** for next hop – **A,**
D: M_B =R_{ID}, Seq, F_{ID},K_{NN}, E_{PK_S}(M_D, $Sig_D(M_D)$)
D: E_{K_N}(M_B)
D: RqT_D ← < R_{ID}, Seq, true >
D: FT ← <R_{ID}, Seq, D, null, B, K_N >
D: FT ← <F_{ID}, Seq, B, K_N, D, null >

B: If < R_{ID}, Seq > is not inside **RqT_B**
B: RT_C : <R_{ID}, Seq> => A;
B: FT ← <R_{ID}, Seq, D, K_{DB}, B, K_{BA}>,
B: FT ← <F_{ID}, Seq, A, null, D, null>; K_{DA} = K_N, K_{BA}=K_{NN}

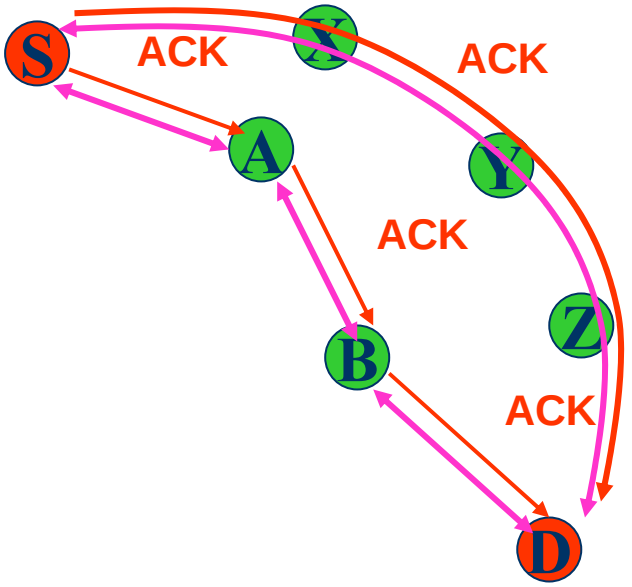


A: SecK(K_N), K_N = K_{BA}

T.Ciszkowski@tele.pw.edu.pl

ANAP (6)
Obustronne uwierzytelnienie

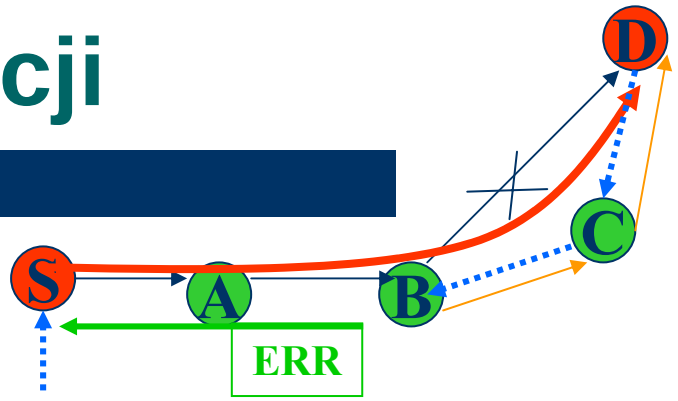
S: $<R_{ID}, Seq, F_{ID}, K_{NN}, E_{PK\_S}(M_D, Sig_D(M_D))>$
S: $< R_{ID}, Seq >$ is inside RqT_C; **Reply = true**
S: M_D=REP, D_{ID}*, K_{SES_D},ISeq+1, L_P, P,$Sig_D(M_D)$
S: Verify **Sig** (M_D)
S: M_S = ACK, S_{ID}*, ISeq+2, L_P, P,
S: FT_S: $<F_{ID}, Seq>$, to **S => A**
S: SecK(K_N), $K_N = K_{SA}$
S: $M_D = E_{K\_SES\_D}(M_S)$
S: $E_{K\_N}(F_{ID}, Seq, K_{NN}, M_D), K_{NN} = K_{AB}$



A: FT_A : $<F_{ID}, Seq, S>$ => **B** and update keys
$FT\text{-}_A < F_{ID}, Seq, S, K_{SA}, B, K_{AB} >$
$FT\text{-}_A < R_{ID}, Seq, B, K_{BA}, S, K_{AS} >$, $K_{SA} = K_N$, $K_{AB} = K_{NN}$
D: RqT_A: $< R_{ID}, Seq, true>$,
D: $E_{K\ SES\_D}$ (M_S), verify **ISeq+2**

T.Ciszkowski@tele.pw.edu.pl

ANAP (7)
Utrzymanie komunikacji



- Detekcja błędów komunikacji
  - Węzły pośredniczące generują wiadomości do nadawcy, czyszczenie tablicy routingu po ustalonym czasie (TIMER)

B: $<ERR, R_{ID}, Seq, K_{NN}, E_{K\ SES}(M_D)>$

- Mobilność węzłów źródłowego i docelowego
  - Fazę odnowienia ścieżki

D: $<REQ, F_{ID}, Seq, E_{K\ SES}(ISeq+1, L_P, P)>$

  - Odpowiedzi udzielają:
    - węzeł pośredniczący:

B: $<REP, F_{ID}, Seq, K_{NN}, E_{K\ SES}(ISeq+1, L_P, P)>$

    - węzeł końca ścieżki:

S: $<F_{ID}, Seq, K_{NN}, E_{K\ SES}(REP, K_{SES,}\ ISeq+1, L_P, P)>$

- Przy braku odpowiedzi, węzeł **S** lub **D** rozpoczyna nową fazę z ***Seq+1***

T.Ciszkowski@tele.pw.edu.pl

ANAP (8)
Odporność na wybrane ataki

- Analiza danych i ruchu
  - Atak pasywny
  - Atak grupowy
- Atak kodowania wiadomości
- Atak długości pakietu
- Atak powtórzenia wiadomości
- Atak analizy czasowej
- Atak wielu tożsamości (Sybil)
- Atak Man in the middle
- Atak Wormhole

T.Ciszkowski@tele.pw.edu.pl

ANAP (8)
Rozproszony system reputacji

- Detekcja nietypowej, złośliwej aktywności węzłów i zarządzanie poziomem zaufania w celu zwiększenie wydajności anonimowej komunikacji
  - Poprzez tworzenie anonimowej reputacji węzłów, za pomocą monitorowania i wymiany informacji z lokalnym sąsiedztwem,

T.Ciszkowski@tele.pw.edu.pl

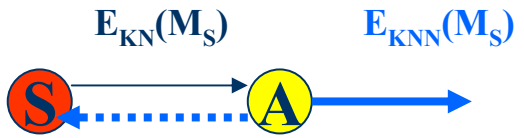
Model rozproszonej reputacji (1)

- Model reputacji
  - Wirtualny czas, sterowany elementarnymi zdarzeniami (interakcje węzłów)
  - Własne doświadczenie (Own Experience)
  - Reputacja usługi (Service Reputation)
  - Informacje z drugiej ręki (Votes)
  - Reputacja informacji z drugiej ręki – wiarygodność informacji (Information Reputation)
  - Analiza korelacyjna

T.Ciszkowski@tele.pw.edu.pl

Reputacja (2)

- Elementarne interakcje **STE** - monitorowanie zachowania **P**
  - Przesłanie (forwarding), parametry QoS (straty pakietów, opóźnienia transmisji)
  - Odbiór (błędy weryfikacji)
  - Zdublowane pakiety
  - Ciche zrywanie połączenia (brak wiadomości ERR)
  - Modyfikacja ładunku pakietów
- Stopień satysfakcji **ST** w chwili **n**



$$STE_i^S(A) = \sum_{l=0}^{k-1} w_l P_l$$

$$ST_n^S(A) = \frac{1}{Q} \sum_{i=0}^{Q-1} STE_i$$

T.Ciszkowski@tele.pw.edu.pl

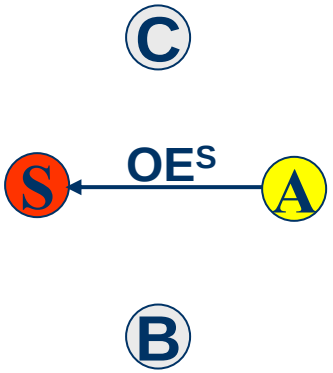
Reputacja (3)

- Własne doświadczenie **OE** na bazie skończonej liczby doświadczeń (historii)

$$OE_n^S(A) = \frac{\sum_{j=0}^{L-1} \gamma_j ST_{n-j}^S(A)}{\sum_{j=0}^{L-1} \gamma_j},$$

- Szybkość zapominania

$$\gamma_n = \begin{cases} \rho, & n = 0 \\ (1-\rho)^{n+1}, & n > 0 \end{cases} \qquad 0 < \rho < 1$$



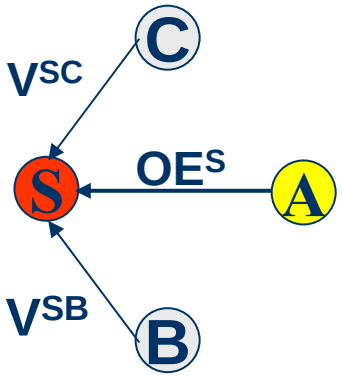
T.Ciszkowski@tele.pw.edu.pl

Reputacja (4)

- Reputacja usługi **SR**

$$SR_n^S(A) = \alpha OE_n^S(A) + (1-\alpha)\frac{\sum_{p \in GVS} IR_n^S(p) V_n^{Sp}(A)}{\sum_{p \in GVS} IR_n^S(p)}$$

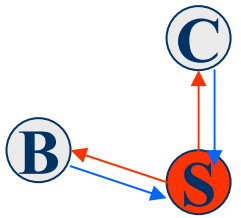
$$IR_n^S(p) > 0, \qquad 0 < \alpha < 1, \qquad \{B, C\} \subset GVS$$



- Wymiana informacji **V** o reputacji między sąsiadującymi węzłami
  - Dla uczciwych węsłów: **$V^{SC}(A) = SR^C(A)$**

S: REQV, Seq, TPK

B: REPV, Seq+1, E_{TPK}(<C,V><S,V>...)
C: REPV, Seq+1, E_{TPK}(<B,V><S,V>...)



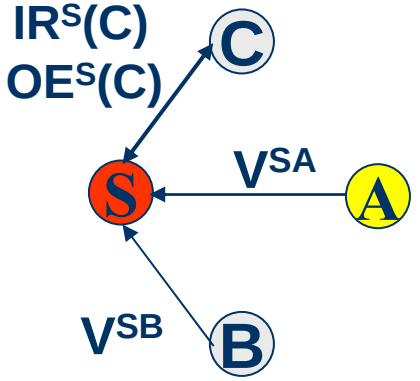
T.Ciszkowski@tele.pw.edu.pl

Reputacja (5)

- Reputacja informacji **IR** z „drugiej ręki” – budowana zgodnie z zasadą – „głos V bliższy naszym oczekiwaniom jest bardziej wiarygodny”

$$IR_n^S(C) = \beta OE_n^S(A) - \frac{\sum_{p \in GIRSC} IR_n^S(p) \left| V_n^{Sp}(C) - OE_n^S(C) \right|}{2 \sum_{p \in GIRSC} IR_n^S(p)},$$

$$IR_n^S(p) > 0, \qquad 0 < \beta < \alpha < 1, \qquad \{A, B\} \subset GIRSC$$



T.Ciszkowski@tele.pw.edu.pl

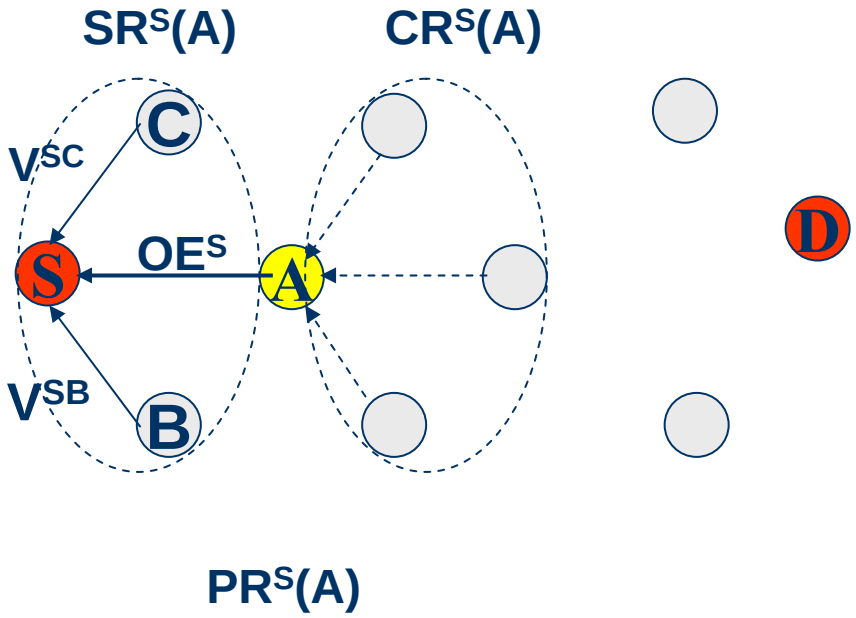
Reputacja – wybranie ścieżki (7)

- Reputacja skumulowana

$$CR_n^S(A) = IR_n^S(A)\frac{\sum_{p \in GA \setminus GS} V_n^{SA}(p)}{|GA \setminus GS|}, IR_n^S(A) > 0$$

- Reputacja ścieżki

$$PR_n^S(A) = SR_n^S(A) CR_n^S(A)$$



T.Ciszkowski@tele.pw.edu.pl

Reputacja – detekcja anomalii (8)

- Analiza korelacyjna

$$D_O = \sum_{i=0}^{L-1} (\hat{R}_i^O - \hat{R}_{i+1}^O)^2 \qquad \hat{R}_i^O = \sum_{n=0}^{L-1} OE_n OE_{n-i}$$

$$D_V = \sum_{i=0}^{L-1} (\hat{R}_i^V - \hat{R}_{i+1}^V)^2 \qquad \hat{R}_i^V = \sum_{n=0}^{L-1} V_n V_{n-i}$$

- Detekcja nietypowych zachowań
  - **$D_O > Th_O$ & $D_V > Th_V$** – odrzucanie otrzymanych informacji **V**, zmniejszenie **IR**
  - **$D_O < Th_O$ & $D_V > Th_V$** – informacje **V** są, akceptowane, **SR** aktualizowany ze zwiększonym α, większym **OE**
  - **$D_O > Th_O$ & $D_V < Th_V$** – jak wyżej, może sygnalizować długoterminowy atak na system reputacji

T.Ciszkowski@tele.pw.edu.pl

Zastosowania MANET

- Militarne
  - DARPA (Defense Advanced Research Projects Agency) dla wojsk USA
- Cywilne
  - Ograniczona przepływność łączy radiowych, zakłócenia – rozwiązania hybrydowe, Wireless Distribution Systems, bezprzewodowe sieci metropolitarne (Mesh Networks, Tropos Networks)
  - Straż, policja, służby cywilne,
  - Klęski żywiołowe, obszary bez infrastruktury telekomunikacyjnej
  - Medycyna, edukacja
  - Zabawa

T.Ciszkowski@tele.pw.edu.pl

Podsumowanie

- Alternatywna metoda komunikacji bezprzewodowej z gwarancją bezpieczeństwa i anonimowości
- Reputacja i monitorowanie złośliwej aktywności węzłów sieci pozwala zwiększyć wydajność komunikacji

- Istnienie zaufanej instytucji TA
- Optymalizacja wydajności dla ruchomych węzłów

T.Ciszkowski@tele.pw.edu.pl

Literatura

- MANET
  - IETF – http://www.ietf.org/html.charters/manet-charter.html
- Bezpieczeństwo w MANET
  - Hu Y., Perrig A.: *A Survey of Secure Wireless Ad Hoc Routing*, IEEE Security & Privacy, 2004
- Anonimowość
  - A. Pfitzmann, M. Hansen.: *Anonymity, Unobservability, Pseudonymity, and Identity Management* – A Proposal for Terminology, 2005
- Reputacja
  - J. Liu, V. Issarny, *Enhanced Reputation Mechanism for Mobile Ad Hoc Networks,* Springer-Verlag Berlin Heidelberg, 2004
- http://wirelessanarchy.com/

T.Ciszkowski@tele.pw.edu.pl

Dziękuję

- Pytania ?

Tomasz Ciszkowski,
PW, T.Ciszkowski@tele.pw.edu.pl

T.Ciszkowski@tele.pw.edu.pl

ANODR (2)

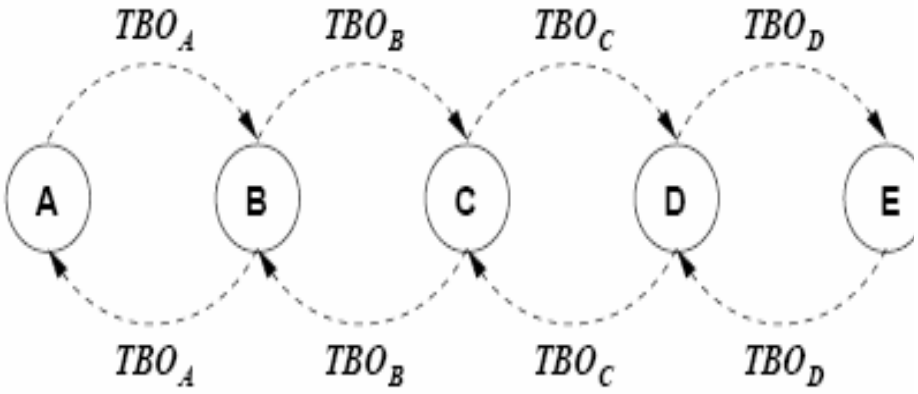
- Protokół anonimowego rutowania na żądanie
  - Trapdoor węzła przeznaczenia – klucz sesyjny dla pary węzłów, TA
  - Trapdoor Boomerang Onions - TBO
  - Kryptografia symetryczna, losowe klucze i tokeny N
- Zmienna długość wiadomości
- Mała wydajność dla MANET

$$TBO_A = K_A(src)$$

$$TBO_B = K_B(N_B, K_A(src))$$

$$TBO_C = K_C(N_C, K_B(N_B, K_A(src)))$$

$$TBO_D = K_D(N_D, K_C(N_C, K_B(N_B, K_A(src))))$$



T.Ciszkowski@tele.pw.edu.pl

MASK (3)

- Wymagana trzecia zaufana strona TA
- Połączenia pomiędzy wszystkimi sąsiadami są szyfrowane kluczem sesyjnym, a węzły są anonimowo uwierzytelnione – proaktywny
- Proces wyszukiwania ścieżki - reaktywny
- Strony kanału komunikacyjnego nie są uwierzytelnione
- Kryptografia symetryczna
- Utrzymanie wiele ścieżek komunikacyjnych dla zestawionego połączenia

T.Ciszkowski@tele.pw.edu.pl

SDAR (4)

- Wymagana trzecia strona zaufana TA dla PKI
- Proces wyszukiwania ścieżki - reaktywny
  - Bazuje na kryptografii klucza publicznego dla mechanizmu ‘trapdoor’
  - Koncepcja ‘onion routing’
  - Węzły pośredniczące współdzielą klucz sesyjny z węzłem docelowym – wykorzystywane przy odpowiedzi
  - Długość zależna od liczby węzłów pośredniczących
- Strony kanału komunikacyjnego są uwierzytelnione
- Rozproszony system reputacji oparty o kryptografię symetryczną i lokalne społeczności z trzypoziomowym stopniem zaufania

T.Ciszkowski@tele.pw.edu.pl