Studia i Materiały Informatyki Stosowanej, Tom 17, Nr 3, 2025
str. 13-16

MODELOWANIE I SYMULACJA ATAKÓW NA PROTOKOŁY ROUTINGU W SIECIACH MANET

Mateusz Rzemieniewski

Kazimierz Wielki University, Faculty of Computer Science
Kopernika 1, 85-074 Bydgoszcz
e-mail: mateusz.rzemieniewski@ukw.edu.pl

Streszczenie: *Artykuł dotyczy badań nad zagrożeniami systemu routingu w sieciach MANET, które wymagają specjalnych protokołów ze względu na dynamiczną strukturę i brak centralnego punku zarządzającego siecią. Z wykorzystaniem symulatora ns-3 zdefiniowany został symulator pozwalający na przeprowadzenie badań pozwalających na realizację kilku typowych dla tej sieci ataków. Przeprowadzono również analizę wyników symulacji, które wykazały, że sieci MANET są podatne na specyficzne ataki, które znacząco obniżają ich bezpieczeństwo.*

Słowa kluczowe: *Sieci MANET, symulator ns-3, routing, bezpieczeństwo sieci*

MODELING AND SIMULATION OF ATTACKS ON ROUTING PROTOCOLS IN MANET NETWORKS

Streszczenie: *This article examines threats to the routing system in MANETs, which require specialized protocols due to their dynamic structure and lack of a central network management point. Using the ns-3 simulator, a simulator was defined to allow for testing several attacks typical of this network. Simulation results were also analyzed, demonstrating that MANETs are vulnerable to specific attacks that significantly compromise their security.*

Słowa kluczowe: *MANET networks, ns-3 simulator, routing, network security*

1. WPROWADZENIE

Głównym celem przedstawionych badań było przeanalizowanie zagrożeń dotyczących protokołów routingu w sieciach MANET (Mobile Ad Hoc Network). Sieci tego typu umożliwiają komunikację pomiędzy urządzeniami, które nie muszą znajdować się w bezpośrednim zasięgu swoich nadajników lub wymagają szybkiej wymiany danych w modelu peer-to-peer. Taka architektura wymusza zastosowanie specjalistycznych protokołów routingu. Charakterystyka sieci MANET sprawia, że są one podatne na określone rodzaje ataków, wykorzystujących ich specyficzne słabości. W ramach pracy stworzono symulator, który posłużył do przeprowadzenia ataków testujących możliwość realizacji wybranych zagrożeń bezpieczeństwa w sieciach MANET.

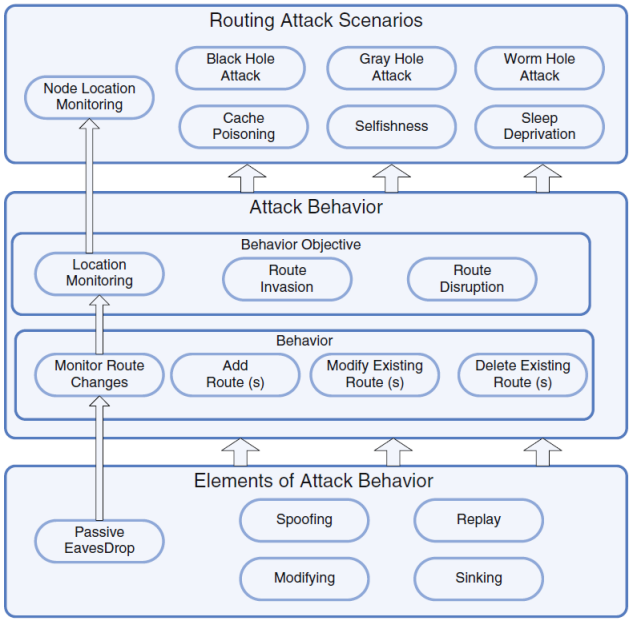
2. PROTOKOŁY ROUTINGU W SIECIACH MANET

Mobilne sieci ad-hoc wymagają specyficznych metod routingu, które różnią się od rozwiązań stosowanych w klasycznych sieciach przewodowych. Wynika to z dynamicznej topologii tych sieci oraz konieczności efektywnego zarządzania energią. Protokoły routingu powinny zapewniać wysoką niezawodność i szybkość działania. Trasy przechowywane w tablicach routingu powinny stanowić jednokierunkowe łącza. Jest to wymaganie wynikające z faktu, że transmisja danych jest bezprzewodowa. Łącze nie powinno być otwierane w trybie jednokierunkowym, ponieważ będzie to skutkowało brakiem możliwości dwukierunkowej transmisji danych. Dla protokołów routingu stosowanych w tego rodzaju sieciach wyróżnia się trzy podejścia:

1. Proaktywne - utrzymywanie aktualnych tras do wszystkich węzłów, co może być nieefektywne i energochłonne w dynamicznych sieciach. Może sprawdzać się przy małej liczbie rzadko przemieszczających się węzłów.
2. Reaktywne - wyznaczanie trasy na żądanie, co zmniejsza ruch w dynamicznych sieciach, ale powoduje opóźnienia w transmisji. Jest mniej efektywne w sieciach statycznych.
3. Hybrydowe - łączy proaktywne i reaktywne metody routingu, dzieląc sieć MANET na klastry z aktualnymi trasami i stosując routing na żądanie między nimi, co zwiększa efektywność, ale utrudnia projektowanie i eksploatację protokołu.

3. ZAGROŻENIA ROUTINGU W SIECIACH MANET

Sieci MANET to środowisko, w którym komunikacja opiera się na wzajemnej współpracy wszystkich węzłów. Niestety, mechanizmy funkcjonujące w tych sieciach mogą być stosunkowo łatwo wykorzystane w sposób złośliwy, prowadząc do zakłócenia lub nawet całkowitego paraliżu działania sieci. Typowe ataki w tego typu sieciach zostały zdefiniowane na rysunku poniżej:



Rysunek 1. Routing attacks taxonomy [5].

Na podstawie taksonomii przedstawionej wyżej w ramach badań przeprowadzono badanie odporności na następujące ataki w sieciach MANET:

1. Black Hole Attack - polega na przekierowaniu pakietów do nieistniejącego węzła, przez co adresat nie otrzymuje danych, a pakiety są tracone bez śladu.
2. Worm Hole Attack - Tworzony jest tunel między dwoma węzłami, umożliwiając podsłuchiwanie lub modyfikowanie pakietów oraz skracanie tras w sieci.
3. Cache poisoning - polega na modyfikowaniu, dodawaniu lub usuwaniu wpisów w tablicach routingu, co prowadzi do nieprawidłowego kierowania pakietów.
4. Selfishness - węzły samolubne odbierają i wysyłają pakiety tylko dla siebie, ale ignorują przekazywanie cudzych danych, przez co zakłócają komunikację.
5. Sleep Deprivation - atakujący generuje nadmiarowy ruch, by szybko wyczerpać zasoby energii węzłów i wykluczyć je z sieci.
6. Network Partitioning - część sieci zostaje odizolowana, co uniemożliwia komunikację z wyłączonym fragmentem.

4. ŚRODOWISKO SYMULACYJNE DO BADANIA ODPORNOŚCI NA ATAKI

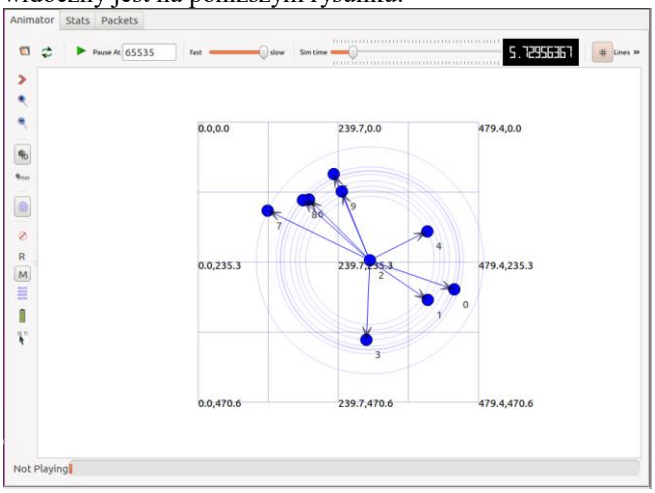
Środowisko do testowania odporności sieci MANET na ataki zostało wykonane w postaci maszyny wirtualnej, na której zainstalowany jest system operacyjny Ubuntu 16.04.4 LTS. Wybór tej platformy umożliwia instalację i wykorzystanie symulatora ns-3.

Symulator ns-3 to powszechnie stosowane narzędzie do przeprowadzania eksperymentów związanych z działaniem sieci komputerowych. Scenariusze sieciowe można w nim tworzyć z użyciem miedzy innymi języka C++. Kluczową zaletą ns-3 jest możliwość modyfikowania jego kodu źródłowego, co daje szerokie możliwości dostosowania środowiska do specyficznych potrzeb, takich jak badanie zagrożeń i realizacja różnych typów ataków na sieci MANET.

Osoba przeprowadzająca badania może uruchomić symulator, wybrać rodzaj ataku oraz określić protokół routingu wykorzystywany podczas symulowanej komunikacji w sieci.

W ramach środowiska testowego wykorzystano dwa typy protokołów: jeden reprezentujący podejście proaktywne oraz jeden reaktywne. Pozwala to ocenić, które

z tych rozwiązań wykazuje większą odporność na ataki. Przykładem protokołu proaktywnego, utrzymującego w tablicach routingu możliwie najaktualniejsze trasy do wszystkich węzłów jest DSDV (Destination-Sequenced Distacne Vector). Z kolei podejście reaktywne zostanie zilustrowane protokołem AODV (Ad hoc On-Demand Distance Vector). Przykład zobrazowania symulacji widoczny jest na poniższym rysunku:



Rysunek 2. Przykład zobrazowania symulacji.

5. WYNIKI ATAKÓW PRZEPROWADZONYCH PRZY UŻYCIU SYMULATORA

Badania rozpoczęto od wykonania próby polegającej na uruchomieniu symulatora w warunkach normalnych, bez działań nieuprawnionych, co pozwoliło uzyskać punkt odniesienia. Próby wykonano dla protokołów proaktywnego oraz reaktywnego. Następnie dla obu rodzajów protokołów uruchomiono symulator inicjując kolejno wszystkie zdefiniowane rodzaje ataków. Wyniki prezentują się w następujący sposób:

1. Black Hole Attack – zgodnie z oczekiwaniami przekierowanie pakietów do nieistniejącego w sieci węzła powodowało całkowity brak komunikacji niezależnie od użytego protokołu routingu.
2. Worm Hole Attack – w ramach tego scenariusza testowego przyjęto, że węzeł będący intruzem doprowadził do sytuacji, gdzie każdy pakiet musiał być przekazywany za jego pośrednictwem. W tym przypadku jakość komunikacji dla obu protokołów spadła tylko nieznacznie, zachowując nadal skuteczność na poziomie 85%. Jednak należy pamiętać, że sukcesem tego ataku jest podsłuchanie wiadomości, a nie pogorszenie komunikacji.
3. Cache poisoning – przyjęto scenariusz gdy tablice routingu były zmodyfikowane dla każdego węzła w sieci. W takim skrajnym przypadku komunikacja w całej sieci była niemożliwa. W tym przypadku użyty protokół nie miał znaczenia.
4. Selfishness – w ramach tego scenariusza połowa węzłów zachowywała się w sposób "samolubny". W wyniku tego ataku dla protokołu AODV skuteczność wysyłania pakietów spadła do 39%, a dla protokołu DSDV do 62%.
5. Sleep Deprivation – dla tego scenariusza testowego wprowadzono dodatkowy węzeł, którego zadaniem było generowanie zbędnego ruchu w sieci. Na skutek tych działań skuteczność prawidłowo dostarczanych pakietów spadła dla protokołu reaktywnego do poziomu 61 %. Co ciekawe w przypadku używania podejścia proaktywnego nie odnotowano znaczącego wpływu na jakość komunikacji.
6. Network Partitioning - w ramach tego scenariusza wyznaczono obszar, w ramach którego nie była możliwa komunikacja. Obejmował on 25% obszaru, po którym mogły poruszać się węzły. Skutkiem było odebranie 56% pakietów w porównaniu ze scenariuszem testowym dla protokołu AODV oraz 74% dla protokołu DSDV.

6. PODSUMOWANIE I WNIOSKI

Przeprowadzone symulacje w sieci MANET pozwoliły na ocenę wpływu różnych typów ataków na skuteczność komunikacji, przy zastosowaniu zarówno protokołu proaktywnego (DSDV), jak i reaktywnego (AODV). Badania rozpoczęto od testów w warunkach bezpiecznych, uzyskując punkt odniesienia dla dalszych eksperymentów. Następnie wprowadzano kolejno wybrane scenariusze ataków, analizując ich skutki dla obu typów protokołów. Najważniejsze wnioski są następujące:

1. Wszystkie analizowane ataki istotnie wpływają na bezpieczeństwo i wydajność sieci MANET, przy czym niektóre z nich (np. Black Hole, Cache Poisoning) mogą całkowicie uniemożliwić komunikację.
2. Protokół proaktywny (DSDV) wykazał większą odporność na niektóre ataki (np. Sleep Deprivation, Selfishness) w porównaniu do

protokołu reaktywnego (AODV), choć oba są podatne na ataki destrukcyjne.

3. Ataki takie jak Worm Hole mogą być trudne do wykrycia, ponieważ nie powodują dużych strat w komunikacji, lecz umożliwiają podsłuchiwanie ruchu.
4. Wybór protokołu routingu powinien być dostosowany do spodziewanych zagrożeń i charakterystyki sieci – nie istnieje rozwiązanie całkowicie odporne na wszystkie typy ataków.
5. Projektowanie systemów zabezpieczeń dla MANET wymaga uwzględnienia różnorodności zagrożeń oraz specyfiki działania poszczególnych protokołów.

Badania potwierdzają, że skuteczna ochrona sieci MANET wymaga zarówno odpowiedniego doboru protokołów, jak i wdrożenia dedykowanych mechanizmów bezpieczeństwa.

Literatura

1. Ade S., Tijare P. Performance Comparison od AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks, International Journal of Information Technology and Knowledge Management, 2010.
2. Condomines J., Zhang R., Larrieu N.: Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation, Elsevier, 2019.
3. Hinds A. A review od Routing Protocols for Mobile Ad-Hoc NETworks (MANET), International Journal of Information and Education Technology, 2013.
4. Malinowski T., Smolarek A. Protokoły trasowania w sieciach Ad Hoc, Materiały konferencyjne Systemy i Sieci Teleinformatyczne.
5. Mirsa S., Mirsa S. C.: Woungang I., Guide to Wireless Ad Hoc Networks, Springer-Verlag, Londyn 2009.
6. Rzemieniewski M.: Demonstrator systemu routingu w sieci o dynamicznie zmieniającej się strukturze, praca dyplomowa, Warszawa 2019.
7. Rzemieniewski M.: Badanie zagrożeń routingu w sieciach MANET metodą symulacyjną, praca dyplomowa, Warszawa 2020.