УДК: 004.056

МЕТОДЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ В MANET

Раджух Маеин Ахмад
БНТУ, Минск, Hekr@mail.ru

Мобильная сеть Mobile Ad hoc Network (MANET) представляет собой динамическую сеть без каких-либо фиксированных инфраструктур.

MANET это набор мобильных узлов, которые осуществляют связь через беспроводные радиоссылки.

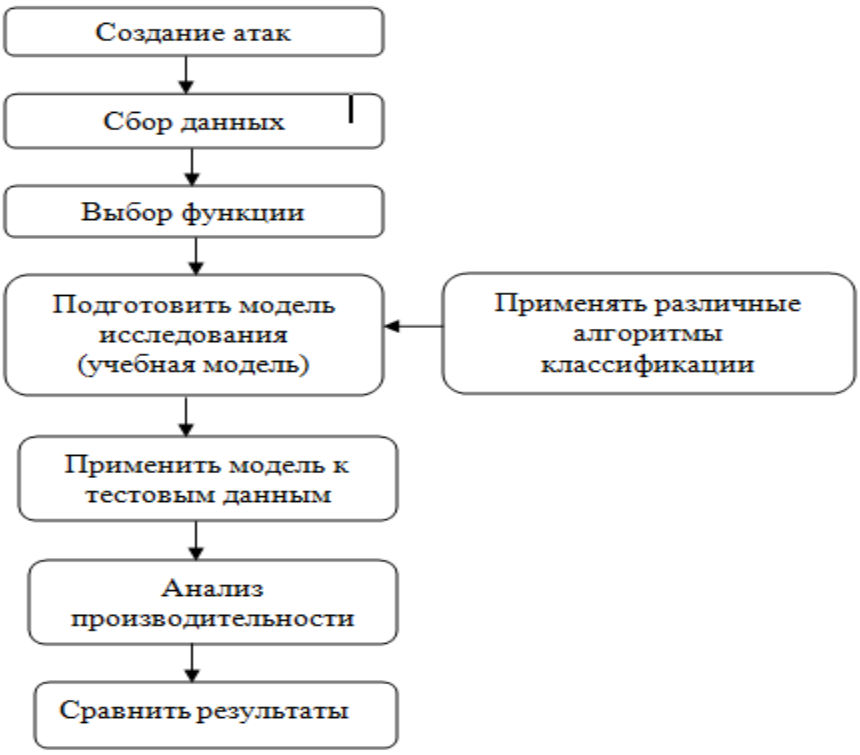
MANET предоставляет надежные услуги маршрутизации в военных и гражданских областях.

Гибкость в сети MANET больше, чем в проводных сетях, поэтому MANET более восприимчива к атакам из-за мобильности узлов, отсутствия централизованного управления и ограничения ширины полосы. Поэтому нам нужна сильная система безопасности.

Для повышения уровня безопасности MANET могут использоваться разные системы обнаружения вторжений: как (IDS) - это программная система, которая контролирует интрузии, происходящие в компьютерной системе или в сети и (COB) - система обнаружения вторжений, которая используется для анализа вредоносного поведения в сети и создания отчетов.

ПРЕДЛАГАЕМАЯ СИСТЕМА

Предложенная система показана на рисунке 1. Она представляет собой схематическую архитектуру обнаружения вторжений в MANET.



Рисунке 1- Архитектура предлагаемой системы

Цель предлагаемого подхода - классифицировать лучшую модель для борьбы с черной дырой и серой дырой атаки в MANET, которые включают в себя создание вторжений в сети, сбор данных аудита, обучение, анализ эффективности и сравнение результатов. Это предлагаемый подход обнаружения вторжений в MANET связанный с созданием интрузии в сети, то есть проектирование узлов черной дыры и серой дыры с различными комбинациями узлов, сбор данных аудита, обучение, набор образцов, состоящий из экземпляров с атакой и нормальным поведением. Затем следующий этап исследования выполняется с использованием данных, извлеченных из набора образцов, которые содержат как нормальные, так и атакованные данные. Впоследствии тестирование проводится для проверки соответствия набора данных (невидимых данных) с моделью.

Наконец, производительность этих моделей анализируется на лучшую модель, использующую различные показатели.

Список литературы

1. Алгулиев Р.М. Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных сетей. М.: УРСС, 2001.
2. Володин А.В., Устинов Г.Н., Алгулиев Р.М. Как обеспечить безопасность сети передачи данных // Технологии и средства связи. 1999. №4
3. Крис Касперски. Техника сетевых атак. М.: СОЛОН-Р, 2001.
4. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour.” A survey of routing attacks in mobile adhoc networks”, *IEEE Wireless Communication*, 14 (5), pp. 85-91, 2007.
5. Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *ACM J. Wireless Networks*, pp. 545-556, 2003.