Impact of network attacks implementation on performance metrics of simulated mobile adhoc network segment

L V Legashev¹, D I Parfenov¹, L S Zabrodina¹, Yu A Ushakov¹

¹ Orenburg State University, 13, Pobedy ave., Orenburg, 460018, Russia
E-mail: silentgir@gmail.com

Abstract. Mobile adhoc networks are one of the promising areas of the edge computing paradigm and used in a wide variety of areas included but not limited to intelligent transport systems, smart homes and smart cities and so on. The main feature of mobile adhoc networks is the constantly changing dynamic network topology, as a result of which it is necessary to use reactive routing protocols when transferring packets between nodes in the network. Mobile adhoc networks are vulnerable to cyber-attacks of various kinds, so there is a need to develop measures to identify such network threats and develop rules for responding to emerging network security incidents. This paper presents a model for detecting traffic anomalies in wireless distributed adhoc networks based on machine learning methods, as well as an experimental study of the simulation of a network segment in terms of performance degradation for the case of various scenarios of network attacks implementation. Distributed denial-of-service attack and cooperative blackhole attack have the most impact on performance metrics degradation in mobile adhoc networks.

1. Introduction

The paradigm of mobile adhoc networks (MANETs) is the absence of a predefined network infrastructure during the information transfer between two wireless devices. Each node in a mobile wireless network can serve as both a router and a host and forward packets on demand. A mobile adhoc network is characterized by a dynamic topology, increased mobility of network nodes, and multi-hop routing. The most popular network routing protocols in MANET are reactive protocols such as AODV (Ad hoc On-Demand Distance Vector), DSDV (Destination-sequenced Distance-vector Routing), OLSR (Optimized Link-state Routing), DSR (Dynamic Source Routing) and many others. Typically, the nodes in the MANET are mobile devices with small amounts of disk and memory and processing power, whereby such network devices can perform a certain computational load. In particular, a binary classification of network threats with pre-trained classifier can be performed at the edge nodes of a mobile adhoc network. The development of the architecture of software-defined networks (SDN) and edge computing technology make it possible to optimally increase the efficiency of routing in mobile adhoc networks, make them more flexible in terms of detecting network threats and developing rules for responding to such threats.

The most common attacks in mobile adhoc networks are Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, as well as Blackhole attacks [1]. In the case of DoS and DDoS attacks, one or another network node temporarily fails, receiving many similar requests to process generated by malicious nodes. In the case of Blackhole attacks, the malicious node drops all incoming
packets, making it difficult to route network flows in MANETs. Kamel M. B. M. et al. in [2] propose an approach to isolate malicious nodes based on a trust model to improve the security of the AODV routing protocol in MANET. Khare A. K. et al. in publication [3] propose the use of fuzzy logic for a methodology to calculate the trust metric of network nodes, in order to detect attacks such as Blackhole, Grayhole and DDoS. El-Semary A. M. et al. in [4] describe a variation of AODV protocol to protect against a cooperative blackhole attack based on chaotic mappings. Khan S. et al. in [5] use an authentication mechanism based on a simplified encryption algorithm and MAC authentication to detect DDoS and Blackhole attacks, proving the effectiveness of the proposed solution based on the NS-2 network simulator. Li G. et al. in [6] use the NS-3 network simulator to study the impact of a Blackhole attack on mobile adhoc network performance parameters such as throughput, end-to-end delay, and packet loss rate. Khan D. M. et al. in [7] use ant colony optimization to prevent a Blackhole attack in MANETs. Gautam D. et al. in [8] carry out experimental studies to detect DDoS attacks using the support vector machine and particle swarm optimization.

2. Formalization of the segment of mobile adhoc network

We represent a segment of a mobile adhoc network at the moment of time $t_j$ in the form of a random geometric undirected graph $G^j = (V, E^j)$, $E^j \subseteq V \times V$, $|V| = n$, $|E^j| = m$, with a set of nodes $V = \{v_1, v_2, \ldots, v_n\}$ of size $n$ and a set of arcs $E^j = \{e_1, e_2, \ldots, e_m\}$ of size $m$. Graph $G^j$ is a spatial network built by randomly placing $n$ nodes in a two-dimensional plane $A$ of size $s_1 \times s_2$ meters, while two nodes are connected by an arc $e_k$ only if their distance at the moment of time $t_j$ is in a given radio range. Due to dynamics of the elements of mobile adhoc network and the change in the distance between them, at each next moment of time $t_{j+1}$ the set of arcs $E^{j+1}$ changes and, therefore, the undirected graph $G^{j+1}$ changes too.

Each vertex of graph $G^j$ represents a wireless router in the form of a tuple of values $v^j_l = (r^j_l, \text{mob}_l^j, \text{spd}_l^j, (x^j_l, y^j_l), t = t_j | V|$, where: $r^j_l$ – radio range of the wireless router signal in mW, \text{mob}_l^j – the node mobility type at the moment of time $t_j$, \text{spd}_l^j – node movement speed in m/s at the moment of time $t_j$, $(x^j_l, y^j_l)$ – node location on plane $A$ at the moment of time $t_j$. By default, all nodes of the graph $G^j$ have linear mobility, \text{mob}_l^j = \text{Linear}$, but if the node is stationary, then its mobility is \text{mob}_l^j = \text{Fixed}$, and the speed is \text{spd}_l^j = 0. The set of arcs $E^j$ of the graph $G^j$ is the set of network connections between nodes, the size of which dynamically changes over time depending on the current topology of the mobile adhoc network. Let’s define the distance between two wireless routers $v^j_a$ and $v^j_b$ at the moment of time $t_j$ as Euclidean distance:

$$d(v^j_a, v^j_b) = \sqrt{(x^j_a - x^j_b)^2 + (y^j_a - y^j_b)^2} \tag{1}$$

The arc $e(v^j_a, v^j_b)$ is built only in the case when $d(v^j_a, v^j_b) \leq r^j_a + r^j_b$, which means that nodes are in each other’s radio access.

When a connection is established between two arbitrary nodes in the network $G^j$, the packets are forwarded according to the selected routing protocol. The set of all network traffic flows in the MANET segment is denoted as $F = \{flowID, bR, fB, fA\}$, $|F| = fNUM$, where: $flowID$ is the unique identifier of the flow, $bR$ is the bitrate of the flow in Mbps, $fB$ is the set of basic features of flow and $fA$ is the set of acquired features of flow. The set of basic features is denoted by a tuple of values $fB = \{srcIP, srcPort, dstIP, dstPort, protocolNum, packetSize, flowDuration\}$, where: $srcIP$ is the IP address of the source node, $srcPort$ is the port number of the source node, $dstIP$ is the IP address of the destination node, $dstPort$ is the port number of the destination node, $protocolNum$ is the number of the network protocol used when sending data, $packetSize$ is the size of the transmitted data packet in
bytes, $flowDuration$ is the duration of the network flow in seconds. When machine learning algorithms are used to detect anomalies, a set of basic features $fB$ is used at the data preprocessing stage to markup benign and malicious traffic (i.e., traffic reflecting the behavior of a particular network attack). Before carrying out the classification operation, the columns with the basic features of the network flows are removed from the dataset, otherwise the classifiers will be trained to classify attacks only from certain IP addresses. The set of acquired features $fA$ is specified in an arbitrary form and can contain up to several dozen of features.

Let us denote a binary classifier of network threats in the form of an objective function $h(z): Z \rightarrow [0,1]$, which assigns each traffic flow $z_i$ from the set of all network flows $Z = \{z_1, \ldots, z_n\}$ a label “0” in the absence of a network attack and label “1” in case of a network attack. Let us denote by $bCLF$ the machine learning method chosen for binary classification. Let us denote a multi-class network threat classifier as an objective function $f(z): Z \rightarrow K$, which assigns a label $k_j \in K, |K| > 2$, to each traffic flow $z_i$, corresponding to a specific type of network attack. Let us denote by $mCLF$ the machine learning method chosen for multi-class classification.

To assess the performance of the MANET segment, as well as the efficiency and accuracy of the anomaly detection system, we introduce the following quantitative metrics:

1. Packet Delivery Ratio is defined as the ratio of the number of received packets to the number of sent packets for the nodes of the network segment, measured in %:

$$PD_R = \frac{numR}{numS} \cdot 100$$  \hspace{1cm} (2)

where: $numR$ – the number of packets received by the destination node, $numS$ – the number of packets sent by the source node.

2. Throughput is defined as the ratio of the size of successfully transmitted packets over the network to the total simulation time $simT$ of the network, measured in bytes / second:

$$T/h_4t = \frac{numReceived}{simT}$$  \hspace{1cm} (3)

3. The time of packet transmission from source to destination and back (round-trip-time) is calculated as:

$$TR_{tr} = T_{rep} - T_{req}$$  \hspace{1cm} (4)

where: $T_{rep}$ is the time when a response was received from the destination node, $T_{req}$ is the time when the request was sent from the source node.

4. End-to-end Delay is defined as the ratio between the time a packet is sent from the source node and received by the destination node:

$$E2E = T_{recv} - T_{req}$$  \hspace{1cm} (5)

where: $T_{recv}$ is the time when the packet was received by the destination node. On average, End-to-end Delay is half of the round-trip-time (4).

5. Overhead is defined as the average number of routing packets required to deliver single data packet, and calculated as the ratio of transmission count to the number of packets received:

$$OH = \frac{transmissionCount}{numR}$$  \hspace{1cm} (6)

where: $transmissionCount$ - total number of routing operations.
We also introduce the metric of the computational resources spent on the operation of trained network threats classifiers:

\[ CR = CR_b + CR_m, \]  

where: \( CR_b \) is the processing power, the amount of RAM and disk space required for the operation of the \( bCLF \) binary classifier, and \( CR_m \) is the processing power, the amount of RAM and disk space required for the operation of the \( mCLF \) multi-class classifier.

The presented metrics (2) - (6) will make it possible to evaluate the effectiveness of simulated network threats in the mobile adhoc network segment in order to further form the MANET dataset for research using machine learning methods. Metric (7) will make it possible to assess the possibility of classifiers operating on the edge elements of a mobile adhoc network in accordance with the concept of edge computing. The general scheme for generating the MANET dataset is shown in Figure 1, starting from the simulation stage of a network segment and ending with data preprocessing before applying machine learning methods to classify simulated network threats. In this paper, we are focusing on the first stage of the scheme, running several simulation scenarios and examining the impact of network attacks on metrics (2) - (6).

![Figure 1. General scheme for generating a dataset to train classification methods of network traffic anomalies detection. PCAP files contain network traffic flows information.](image)

3. Modelling a segment of a MANET and assessing the performance metrics

Within the OMNeT++ simulation tool, on the basis of the INET framework showcases, a segment of a mobile adhoc network is built, the general simulation parameters are presented in Table 1. The
functioning of a mobile adhoc network segment is shown in Figure 2. There are three minimum possible routes from source node to destination node: direct diagonal route, “upper” arc and “lower” arc, while five moving nodes ensure the dynamic of the network segment topology. The blue circles represent the radio signal strength of each node in the network segment. The red and orange broken lines represent a successful route between the source node and destination node. Red squares mark nodes potentially implementing a blackhole attack.

Table 1. General simulation parameters.

| Parameter                  | Value          |
|----------------------------|----------------|
| Protocol                   | AODV           |
| Number of nodes $n$        | 21             |
| Size of plane $A$          | 800m, 600m     |
| Simulation time $simT$     | 1500s          |
| Wlan bitrate               | 24 Mb/s        |
| Size of packets            | 350 byte       |
| Signal range $r_i$         | 0.8 mW         |
| Node speed                 | 16-24 m/s      |
| Mobility of nodes 1..10, 16..19 | Fixed         |
| Mobility of nodes 11..15   | Linear         |

The functioning of a mobile adhoc network segment is shown in Figure 2. There are three minimum possible routes from source to destination: direct diagonal route, “upper” arc and “lower” arc, while five moving nodes ensure the dynamic of the network segment topology. The blue circle represents the radio signal strength of each node in the network. The red and orange broken lines represent a successful route between the source and destination. When the simulation script finishes, the $transmissionCount$ value is automatically calculated. The elements of INET framework by default collect statistics on the number of transmitted and received packets, round-trip-time, queueing time, etc. Based on the simulation output, the remaining metrics from (2) - (6) are calculated.

Figure 2. Demonstration of simulating a MANET segment without network attacks. In this case potential blackhole attack nodes BHNode and BHNode2 used as relay nodes.
To assess the performance indicators of a segment of a mobile adhoc network, we will consider several simulation scenarios: without attacks (scenario 1), with blackhole attack (scenario 2), with cooperative blackhole attack (scenario 3), with DoS attack (scenario 4) and with DDoS attack (scenario 5). As a result, the following changes were obtained in the values of the metrics (2) - (6) in comparison with the simulation of the MANET segment without attacks, as it shown in Figure 3. Pale green indicates an improvement in performance metric, pale red indicates deterioration in performance metric.

| Scenario       | Queueing time, s | rtt, s  | PDR, %  | Thpt, b/s | E2E, s | OH, packets |
|----------------|------------------|---------|---------|-----------|--------|-------------|
| Without attacks| 4.29             | 1.15    | 36      | 60.43     | 0.58   | 121         |
| Blackhole      | 8.85↑            | 0.84↓   | 78↑     | 145.83↑   | 0.42↓  | 51↓         |
| Coop. blackhole| 1.69↓            | 0.62↓   | 5↓      | 8.40↓     | 0.31↓  | 551↑        |
| DoS            | 4.62↑            | 0.98↓   | 58↑     | 99.17↑    | 0.49↑  | 153↑        |
| DDoS           | 7.04↑            | 1.2↑    | 32↓     | 52.50↓    | 0.60↑  | 919↑        |

Figure 3. Changes in the performance metrics in the case of network attacks implementation.

The blackhole attack scenario improves most of the metrics under consideration, unintentionally providing routing along the most stable route along the “lower” arc of the considered topology of the MANET segment, but a rapid increase in the average queueing time of packet in the queue should be noted. Implementing a cooperative blackhole attack improves the round-trip-time, end-to-end delay and queueing time metrics, but at the same time degrades the indicators of the three remaining metrics - packet delivery ratio, throughput and overhead. The DoS attack scenario improves the four metrics round-trip-time, packet delivery ratio, throughput, end-to-end delay, but degrades overhead and queueing time. The node that implements the DoS attack has the same behavior as the source, but sending packets which are marked with the “Attack” label, so it doesn’t affect performance metrics that much. At the same time, the implementation of a DDoS attack with three malicious nodes deteriorates all six indicators; an increase in the overhead and queueing time values should be noted.

It can be concluded that network attacks such as cooperative blackhole attacks and distributed denial-of-service attacks have the greatest negative impact on the performance of a mobile adhoc network, and the intrusion detection system should primarily focus on classifying the patterns of behavior of network threats characteristic typical for these types of attacks.

4. Conclusion
Mobile adhoc networks have great potential for application, especially in the development of intelligent transport systems. The developed model for detecting traffic anomalies will form the basis of the architecture of a distributed intelligent system for detecting networks threats and ensuring security during data transmission in wireless distributed adhoc networks. As part of further research the generalized algorithm for detecting traffic anomalies will be implemented.

5. Acknowledgments
The reported study was funded by the grant of the President of the Russian Federation for state support of young Russian scientists (MK-2959.2021.1.6).

References
[1] Alani M M 2014 IEEE International Conference on Control System, Computing and Engineering (ICCSCE 2014) 559-64
[2] Kamel M B M, Alameri I and Onaizah A N 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) 1278-82
[3] Khare A K, Rana J L and Jain R C 2017 *International Journal of Computer Network and Information Security* 9(7) 29
[4] El-Semary A M and Diab H 2019 *IEEE Access* 7 95197-211
[5] Khan S 2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN) 109-114
[6] Li G, Yan Z and Fu Y 2018 *IEEE Conference on Communications and Network Security (CNS)* 1-6
[7] Khan D M 2020 *Information Technology and Control* 49(3) 308-19
[8] Gautam D and Tokekar V 2020 *Materials Today: Proceedings* 29 674-77