RESEARCH AND DEVELOPMENT OF THE SECURE ROUTING FLOW-BASED MODEL WITH LOAD BALANCING

O. Yeremenko, M. Persikov, V. Lemeshko, B. Altaki
Kharkiv National University of Radio Electronics

Abstract – The article is devoted to developing and researching the model of secure routing with load balancing in SD-WAN-based networks. In addition, an analysis of numerical research results using Python, GEKKO Optimization Suite, and NumPy has been carried out. The technical task of secure routing with load balancing was formulated as an optimization problem with quadratic optimality criterion. Such a criterion form allows for balancing the flow shares transmitting in the network. The simulation results showed that the link load (namely, the transmitted part of the flow) under study decreases with an increased probability of the link compromise. The analysis of the calculated results revealed the value of the security and performance ratio metric when the model is most sensitive to the network link compromise probability deterioration. That is, the best sensitivity of the model to the network security indicator (compromise probability) appears when the ratio between performance and security metric takes values of 100 to 300. Therefore, the presented model of secure routing with load balancing with an additive metric that accounts for network performance and security allows using network resources more efficiently but also considers the link compromise probability in making routing decisions.

Introduction

Currently, deploying such network architectures as Software-Defined Wide Area Networks (SD-WAN) meets new cybersecurity threats that require specific security solutions [1-6]. In turn, approaches used for analysis include modeling and simulating network infrastructure using attributes, functionalities, operations, and behaviors to support various security analysis viewpoints, recognizing and appropriately managing associated security risks. Despite the available network infrastructure protection approaches, effectively modeling the complex behavior of interconnected network elements and configuring their protection remains challenging.

A significant problem with underlying communication networks is the dynamic nature of the network applications and their environment. It means that the Quality of Service (QoS) and security requirements of the transferred data flows can vary over time [5, 6]. Therefore, for the applications to perform securely and effectively, the underlying network should be flexible enough to dynamically change in response to application re-
requirements and their environment changes. The novel approaches require network solutions to consider network performance and security concurrently [7-12].

Thus, a meaningful way to address this problem is through traffic management by analyzing the network state, predicting, and balancing the transmitted data load over the network resources [10, 11, 13-16]. It is a technique used to adapt the traffic routing to the changes in the network condition. However, the traditional routing techniques do not provide mechanisms to allocate network resources optimally.

To address this problem, the research community made significant efforts toward Traffic Engineering (TE) direction. It proposed new approaches to improve network robustness in response to the growth of traffic demands to QoS and network security [13-17]. Therefore, the joint solutions under load balancing and network security reduce service degradation due to congestion and network elements compromising.

The presented work aims to develop and analyze the model of secure routing with load balancing in the core networks. Therefore, Section I is devoted to a mathematical flow-based model of secure routing with load balancing. Section II contains the modeling results, behavior, and evaluation of the secure routing with load balancing model in the network core.

I. Mathematical Flow-Based Model of Secure Routing with Load Balancing

Within the model, let it be assumed that the following inputs are known [19]:

- \( n \) – number of links in the network;
- \( m \) – number of nodes in the network;
- \( s \) – source node;
- \( d \) – destination node;
- \((i, j)\) – network link;
- \( c_{i,j} \) – link capacity;
- \( p_{i,j} \) – link compromise probability;
- \( f_{i,j}^{OSPF} \) – link metric based on performance (link capacity);
- \( f_{i,j}^{SEC} \) – link metric based on security parameter (compromise probability);
- \( r \) – flow rate arriving at the network (packets per second, pps);
- \( x_{i,j} \) – fraction of the flow in the network link between the \( i \)th and \( j \)th nodes.

Task list for the research and numerical study:

- determine the multipath from the source node to the destination via network links being modeled that is the best within the selected metric;
- construct the dependence of the flow distribution over the paths under the secure routing with load balancing on the ratio between performance and security metrics and link compromise probability.
Let us describe the secure multipath routing with load balancing in the network core task. Then the number of network links \( n \) determines the vector \( \bar{x} \) dimension, the coordinates \( x_{i,j} \) of which characterize the fraction of the flow in the communication link between the \( i \)th and \( j \)th nodes. The metric vectors \( f_{i,j}^{\text{OSPF}} \) and \( f_{i,j}^{\text{SEC}} \) dimensions also correspond to the number of network links \( n \). The coordinates \( f_{i,j}^{\text{OSPF}} \) and \( f_{i,j}^{\text{SEC}} \) characterize the metric of the link \((i,j)\) between the \( i \)th and \( j \)th nodes based on performance (bandwidth) and security (compromise probability). The vector \( \bar{x} \) coordinates are subject to the following restrictions in order to implement a multipath routing strategy [1, 15]:

\[
0 \leq x_{i,j} \leq 1, \quad i, j = 1, \ldots, m, \quad i \neq j.
\]

(1)

i.e., the variables \( x_{i,j} \) take values from 0 to 1.

The physical meaning of variables (1) determines the possibility of the flow distribution over the network paths, i.e., packets can be transmitted over one or multiple routes.

While solving the routing problem, it is necessary to ensure the fulfillment of the flow conservation conditions for every node and the whole network [14]:

\[
\begin{align*}
\sum_{j \neq (i,j)} x_{i,j} - \sum_{j \neq (i,j)} x_{j,i} &= 1 \text{ for source node;} \\
\sum_{j \neq (i,j)} x_{i,j} - \sum_{j \neq (i,j)} x_{j,i} &= 0 \text{ for transit nodes;} \\
\sum_{j \neq (i,j)} x_{i,j} - \sum_{j \neq (i,j)} x_{j,i} &= -1 \text{ for destination node.}
\end{align*}
\]

(2)

Let each network link \((i,j)\) will be assigned a metric used in analogy to the OSPF protocol, i.e.,

\[
f_{i,j}^{\text{OSPF}} = \frac{10^8}{c_{i,j}}
\]

where \( c_{i,j} \) is the link \((i,j)\) capacity (bandwidth).

While the security-based metric will be determined considering the link \((i,j)\) compromise probability:

\[
f_{i,j}^{\text{SEC}} = \frac{10^8}{R} p_{i,j}
\]

(4)

where the ratio between performance and security metrics weighting coefficients \( R \) is defined as follows:
\[ R = \frac{w_{\text{OSPF}}}{w_{\text{SEC}}} \]  \hspace{1cm} (5)

where \( w_{\text{OSPF}} = 10^8 \).

Then security metric weighting coefficient is obtained as:

\[ w_{\text{SEC}} = \frac{w_{\text{OSPF}}}{R} = \frac{10^8}{R}. \]  \hspace{1cm} (6)

In addition to the flow conservation conditions (2), it is necessary to meet the overload prevention conditions for every \((i, j)\) link [1]:

\[ r \cdot x_{i,j} \leq c_{i,j}, \quad i, j = 1, m, \quad i \neq j. \]  \hspace{1cm} (7)

Within the work, the quadratic optimality criterion regarding the routing variables \(x_{i,j}\) will be used to implement secure routing with load balancing:

\[ J = \min_x \sum_{(i,j)} \left( f_{i,j}^{\text{OSPF}} + f_{i,j}^{\text{SEC}} \right) x_{i,j}^2. \]  \hspace{1cm} (8)

Therefore, the technical task of secure routing with load balancing is formulated as an optimization problem with constraints (1)-(7) and quadratic optimality criterion (8). The quadratic form allows for balancing the flow shares transmitting in the network.

Within the numerical study, the Python GEKKO Optimization Suite solves the multipath routing optimization problem when several conditions are presented as constraints on equations and inequalities [13-17].

**II. Numerical Study of Secure Routing with Load Balancing Mathematical Model**

Fig. 1 demonstrates the structure of the network under study. The investigated network characteristics are as follows:

- \( n = 6 \) – number of links in the network;
- \( m = 5 \) – number of nodes in the network;
- \( s \) – source node is node #1;
- \( d \) – destination node is node #5.

Additionally, with every network link \((i, j)\) the following parameters are associated (Table 1):

- \( c_{i,j} \) – link bandwidth;
- \( p_{i,j} \) – link compromise probability.
The link bandwidth and compromise probability values are shown in link gaps as a fraction (Fig. 1). The nominator is the link capacity, and the denominator is the link compromise probability.

![Link Diagram](http://pt.nure.ua)

**Fig. 1.** Structure of the IoT-enabled critical infrastructure network core under study

<table>
<thead>
<tr>
<th>Link</th>
<th>Bandwidth (pps)</th>
<th>Compromise probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1→2</td>
<td>150</td>
<td>0.4</td>
</tr>
<tr>
<td>1→3</td>
<td>70</td>
<td>0.1</td>
</tr>
<tr>
<td>2→3</td>
<td>180</td>
<td>0.5</td>
</tr>
<tr>
<td>2→5</td>
<td>50</td>
<td>0.1</td>
</tr>
<tr>
<td>3→4</td>
<td>160</td>
<td>0.4</td>
</tr>
<tr>
<td>4→5</td>
<td>170</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Within the network structure, the three paths (routes) can be distinguished, namely:

- Path #1: 1→2→5;
- Path #2: 1→3→4→5;
- Path #3: 1→2→3→4→5.

Suppose that the flow with the rate $r = 150$ pps is transmitted between the first and fifth nodes. While the ratio between performance and security metrics weighting coefficients $R$ varies from 1 to 1000, as shown in Table 2.

**Table 2.** The flow distribution under the secure routing with load balancing mathematical model ($r = 150$ pps)

<table>
<thead>
<tr>
<th>$R$</th>
<th>1000</th>
<th>600</th>
<th>500</th>
<th>300</th>
<th>100</th>
<th>50</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path #1 flow rate, pps</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Path #2 flow rate, pps</td>
<td>60.5</td>
<td>61.7</td>
<td>62.3</td>
<td>64.4</td>
<td>70</td>
<td>70</td>
<td>70</td>
</tr>
<tr>
<td>Path #3 flow rate, pps</td>
<td>39.5</td>
<td>38.3</td>
<td>37.7</td>
<td>35.6</td>
<td>30</td>
<td>30</td>
<td>30</td>
</tr>
</tbody>
</table>
Application of the model (1)-(7) and quadratic optimality criterion (8) for solving the problem of secure routing with load balancing is demonstrated in Table 2. In this case, the flow is distributed among all three paths. The corresponding flow rates for every path and R value are also indicated in Table 2.

Let us describe the Python scripts with the Python GEKKO Optimization Suite application responsible for solving the optimization problem (1)-(8).

Firstly, the Python GEKKO Optimization Suite must be installed:

```
pip install gekko
```

Then the initial input data for the numerical study is entered according to the following code snippet:

```python
from array import *
from gekko import GEKKO
import numpy as np

# Initialize Model
m = GEKKO()
# c - links capacities
c=[150,70,180,50,160,170]
# c - links compromise probabilities
p=[0.4,0.1,0.5,0.1,0.4,0.5]
# r - flow rate
r=m.Param(value=150)
```

Next, the metrics calculation is performed considering the $R$ value entered, as well as routing variables initialization:

```python
# f1 - performance metric
# f2 - security metric
R = float(input(’Ratio: ’))

f_sec = (10**8)/R
f1 = [(10**8)/c[0], (10**8)/c[1], (10**8)/c[2], (10**8)/c[3], (10**8)/c[4], (10**8)/c[5]]

f2 = [f_sec*p[0], f_sec*p[1], f_sec*p[2], f_sec*p[3], f_sec*p[4], f_sec*p[5]]
# initialize variables
x1,x2,x3,x4,x5,x6 = [m.Var(lb=0, ub=1) for i in range(6)]
# initial values
x1.value = 0
x2.value = 0
x3.value = 0
x4.value = 0
x5.value = 0
x6.value = 0
```

The flow conservation (2) and overload prevention (7) conditions are implemented as follows:
# Equations
m.Equation(x1+x2==1)
m.Equation(x1-x3-x4==0)
m.Equation(x2+x3-x5==0)
m.Equation(x5-x6==0)
m.Equation(x4+x6==1)
m.Equation(r*x1<=c[0])
m.Equation(r*x2<=c[1])
m.Equation(r*x3<=c[2])
m.Equation(r*x4<=c[3])
m.Equation(r*x5<=c[4])
m.Equation(r*x6<=c[5])

Finally, the optimization problem solving is performed as:

# Objective

# Solve simulation
m.options.IMODE = 3  # LP solver
m.solve()

The following code presents the resulting solution output:

# Results
print('')
print('Results')
print('x1: ' + str(x1.value))
print('x2: ' + str(x2.value))
print('x3: ' + str(x3.value))
print('x4: ' + str(x4.value))
print('x5: ' + str(x5.value))
print('x6: ' + str(x6.value))
print('')
print('Flow rates in links')
xx = [x1.value[0],x2.value[0],x3.value[0],x4.value[0],x5.value[0],x6.value[0]]
xx = np.array(xx)
rr = int(r.value[0])
yy = rr*xx
print('y1: ' + str(yy[0]))
print('y2: ' + str(yy[1]))
print('y3: ' + str(yy[2]))
print('y4: ' + str(yy[3]))
print('y5: ' + str(yy[4]))
print('y6: ' + str(yy[5]))

Fig. 2 demonstrates the visualization of the secure routing with load balancing problem solving under the $r = 150$ pps shown in Table 2.
After decreasing the flow rate to \( r = 30 \) pps, the following flow distribution has been obtained (Table 3).

**Table 3.** The flow distribution under the secure routing with load balancing mathematical model 
\((r = 30 \text{ pps})\)

<table>
<thead>
<tr>
<th>Path</th>
<th>Flow Rate, pps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path #1</td>
<td>12.8 13.1 13.2 13.7 15.4 16.8 19.8</td>
</tr>
<tr>
<td>Path #2</td>
<td>11.5 11.6 11.7 12 13 13.2 10.2</td>
</tr>
<tr>
<td>Path #3</td>
<td>5.7 5.3 5.1 4.3 1.6 0 0</td>
</tr>
</tbody>
</table>

In turn, Fig. 3 demonstrates the visualization of the secure routing with load balancing problem solving under the \( r = 30 \text{ pps} \) shown in Table 3.

Analysis of the obtained results (Table 2 and Table 3) show that if the flow rate and consequently network load are low \((r = 30 \text{ pps})\), then only two routes are used within the multipath in a case of low values of the ratio \((R = 1, R = 50)\):
- Path #1: 1→2→5;
- Path #2: 1→3→4→5.

In the case of the high flow rate \((r = 150 \text{ pps})\), all the routes are used in the multipath.

The following numerical results were obtained for the case when the compromise probability \( p_{2,3} \) of the (2,3) link varied from 0.1 to 0.8. Table 4. demonstrates the model behavior for this input parameter. Also, \( R \) changed within the range from 100 to 1000.
Fig. 3. The flow distribution over the paths under the secure routing with load balancing
(r = 30 pps, R=1+1000)

Table 4. The dynamics of changes in the flow distribution in the multipath depending on the
parameter R and the link compromise probability \( p_{2,3} \)

<table>
<thead>
<tr>
<th></th>
<th>( R )</th>
<th>1000</th>
<th>500</th>
<th>300</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p_{2,3} )</td>
<td>0.1</td>
<td>0.8</td>
<td>0.1</td>
<td>0.8</td>
<td>0.1</td>
</tr>
<tr>
<td>Path #1 flow rate, pps</td>
<td>21.3</td>
<td>21.5</td>
<td>22</td>
<td>22.1</td>
<td>22.6</td>
</tr>
<tr>
<td>Path #2 flow rate, pps</td>
<td>19</td>
<td>19.2</td>
<td>19.3</td>
<td>19.7</td>
<td>19.7</td>
</tr>
<tr>
<td>Path #3 flow rate, pps</td>
<td>9.6</td>
<td>9.3</td>
<td>8.7</td>
<td>8.2</td>
<td>7.7</td>
</tr>
</tbody>
</table>

Therefore, the simulation results showed that the link (2,3) load (the transmitted part
of the flow) under study decreases with an increased link compromise probability. In addition, the best sensitivity of the model to the \( f_{i,j}^{SEC} \) security metric appears when the \( R \) ratio takes values of 100 to 300.

In turn, Table 5 and Fig. 4 present the model behavior for the case when \( r = 50 \) pps, \( R = 300, \ p_{2,3} = 0.1 \div 0.8 \). Numerical calculations have shown a decrease in the share of the flow in the link (2,3) if its compromise probability increases.

Thus, a numerical study of the secure routing with load balancing model in SD-
WAN infrastructure network core was conducted. The analysis of the calculated results
revealed the value of the security and performance ratio metric when the model is most sensitive to the network link compromise probability deterioration.
Table 5. The flow distribution under the secure routing with load balancing mathematical model 
\( (r = 50 \text{ pps}, R = 300, p_{2,3} = 0.1 \div 0.8 ) \)

<table>
<thead>
<tr>
<th>( p_{2,3} )</th>
<th>0.1</th>
<th>0.2</th>
<th>0.3</th>
<th>0.4</th>
<th>0.5</th>
<th>0.6</th>
<th>0.7</th>
<th>0.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path #1</td>
<td>22.6</td>
<td>22.66</td>
<td>22.71</td>
<td>22.76</td>
<td>22.80</td>
<td>22.85</td>
<td>22.89</td>
<td>22.9</td>
</tr>
<tr>
<td>flow rate, pps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path #2</td>
<td>19.7</td>
<td>19.77</td>
<td>19.84</td>
<td>19.91</td>
<td>19.99</td>
<td>20.05</td>
<td>20.12</td>
<td>20.2</td>
</tr>
<tr>
<td>flow rate, pps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path #3</td>
<td>7.7</td>
<td>7.57</td>
<td>7.45</td>
<td>7.33</td>
<td>7.21</td>
<td>7.10</td>
<td>6.99</td>
<td>6.9</td>
</tr>
<tr>
<td>flow rate, pps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig. 4. The flow distribution over the paths under the secure routing with load balancing 
\( (r = 50 \text{ pps}, R = 300, p_{2,3} = 0.1 \div 0.8 ) \)

**Conclusions**

This work is devoted to developing and researching the model of secure routing with load balancing in SD-WAN-based networks. In addition, an analysis of numerical research results using Python, GEKKO Optimization Suite, and NumPy has been carried out.

Hence, the technical task of secure routing with load balancing is formulated as an optimization problem with constraints (1)-(7) and quadratic optimality criterion (8). The quadratic form allows for balancing the flow shares transmitting in the network.

The simulation results showed that the link load (namely, the transmitted part of the flow) under study decreases with an increased probability of the link compromise. The analysis of the calculated results revealed the value of the security and performance ratio metric when the model is most sensitive to the network link compromise probability deterioration. That is the best sensitivity of the model to the \( f_{i,j}^{SEC} \) security metric appears when the \( R \) ratio takes values of 100 to 300.
Therefore, the presented model of secure routing with load balancing with an additive metric that accounts for network performance and security allows using network resources more efficiently but also considers the link compromise probability in making routing decisions.

References

Advanced Computing Systems: Technology and Applications (IDAACS), No. 1, Metz, France, 18-21 September, P. 117-122. DOI: https://doi.org/10.1109/IDAACS.2019.8924294


