

Fragmentation-based Multipath Routing for Attack Resilience in Software Defined Networks

Purnima Murali Mohan, Teng Joon Lim, Mohan Gurusamy

Department of Electrical & Computer Engineering

National University of Singapore, Singapore

E-mail: purnima.m@u.nus.edu, eleltj@nus.edu.sg, elegm@nus.edu.sg

Abstract—In this paper, we propose a Fragmentation-based Multipath Routing (FMR) model for Software Defined Networks (SDNs) to enable attack-resilient data transfer. With the use of erasure encoding to fragment a message, the fragments are routed along multiple paths such that no intermediate node receives enough fragments required for message decoding. This ensures that, any intruder on a compromised node does not infer the original data from the received fragments. We develop an optimization programming formulation of the problem to choose reliable paths that provide resilience to attacks. Using FMR, the SDN controller dynamically routes the data fragments along a set of most reliable paths to achieve multipath diversity and hence improve data availability at the destination even in the presence of an attack. We carry out performance studies and demonstrate the effectiveness of our approach in terms of weighted path reliability and blocking performance.

Index Terms—Software Defined Networks, Multipath routing, Reliability, Resilience, Constrained routing.

I. INTRODUCTION

With the emergence of the Software Defined Network (SDN) paradigm, dynamic and adaptive management of a network becomes possible [1]. To address security issues in an SDN, the security policies are implemented in the network dynamically with a programmable centralized SDN controller through software instead of low-level device configurations [2]. Consider an SDN-enabled IoT network with several sensor nodes in the edge network sensing information and transmitting to aggregate nodes which then route the information to a server through the core network. When such an amount of data is routed in a network with a few compromised nodes, even before the SDN controller monitors and reacts to the spurious network changes due to the compromised nodes, a large amount of sensitive data that is routed along those compromised nodes may already have been lost or intercepted. Hence there is a need for resilience towards attacks to protect the data transmitted while still conforming to the security policy updates from the SDN controller.

In this paper, we aim to improve the security of the SDN-enabled network through improved resilience to node attacks or failures. By resilience we mean that compromising a few nodes in the network will neither affect the availability of the data being routed, nor allow the attacker to reconstruct the original message. To enable resilience, we propose the transmitted messages be fragmented so that intercepting a small number of fragments does not allow the passive attacker to derive any valid information. We make use of the Erasure Resilient Coding (ERC) approach [3] for data fragmentation which has been well-studied in the context of resilient data

storage [4]. However, erasure coding for data transmission over networks has not gained much attention due to its complexity, dynamically changing network state and constrained routing. With SDN, the algorithmic complexity and monitoring functions are handled at the centralized SDN controller.

We develop an optimization programming formulation of the Fragmentation-based Multipath Routing (FMR) problem, to enable resilient data transmission. Multipath routing has been proposed for several core and edge networks like the Internet, wireless sensor networks to address various network issues like energy balancing, maximizing throughput, minimizing end-to-end delay, load balancing and other traffic engineering issues [6], [7], [8]. However none of these works consider a fragment routing problem to enable network resilience towards attacks by maximizing the route reliability. The proposed multipath routing FMR ensures that data availability at the destination node is guaranteed even in the presence of an attack and that none of the intermediate nodes receive the original data in its entirety. With changing network state, the multipath solution is recalculated by the SDN controller which installs forwarding rules at the corresponding nodes in the network. To provide improved availability, we take into consideration the reliability of the chosen paths. Hence FMR ensures that the fragments are routed along paths with maximum reliability, assuming that the probability of nodes being compromised or faulty is known. We evaluate the performance of the proposed FMR in terms of weighted path reliability and blocking performance through simulations on random topologies.

II. FRAGMENTATION-BASED MULTIPATH ROUTING USING SOFTWARE DEFINED NETWORKING

Given a data stream to be routed at the source node, the steps to securely transmit the data to the destination are:

Step 1: Fragment the data into k segments at the source node.

Step 2: Encode the k segments into n (where $n > k$) fragments at the source node based on erasure coding.

Step 3: Distribute the n encoded fragments along multiple paths determined by the SDN controller.

In *Step 1*, the original data is fragmented into k segments so that any intruder in the network does not receive complete information related to the original data. Once the k segments are encoded into n fragments in *Step 2*, the original message can be recovered from any $(k + \epsilon)$ fragments of the n encoded fragments at the destination node even when up to $(n - k)$ fragments are lost due to an intruder in the network. Redundancy is thus added in the form of encoding rather than

pure replication. In the last step, we distribute the n fragments along multiple paths so that not all packets are lost due to the presence of compromised nodes on a subset of these paths during the transmission. Our approach is hence resilient to fragment losses (due to active attack) of up to $(n - k)$ on several of these paths as long as more than k fragments reach the destination node. By routing along multiple paths, we also ensure that no single node receives more than k fragments as a passive intruder would require the encoding codeword and more than k fragments to reconstruct the original data.

There are several advantages of using such secure fragment routing approach for network resiliency. When the data is encoded into n fragments and routed along multiple paths, the intruder has to attack several nodes that are a part of the set of multipaths used to transmit the fragmented data rather than just one. Also, the proposed fragment routing is resilient to both active attacks like black hole/sink hole attacks and passive attacks where an intruder monitors the data transmission for vulnerabilities without any intervention in the network.

The SDN controller continuously monitors the traffic in the network based on which the abnormalities could be detected. These abnormal traffic patterns through the SDN-enabled nodes can be used by the SDN controller to find threat probabilities and hence the node reliabilities. We assume that these reliability values are known at the SDN controller for a network. For reliable transmission, the data is encoded into several fragments at the source node based on the encoding codeword at the SDN controller. All the communication between the SDN controller and the SDN-enabled nodes takes place through a secure channel — OpenFlow [1]. Whenever the SDN controller identifies an increased probability of threat on a node due to abnormal traffic pattern, it first modifies the encoding codeword and the routing state is modified based on the updated reliability values and encoding information (n, k) . The SDN controller then communicates the forwarding rules to the corresponding nodes in the network through the secure channel. The flow is hence routed along a new set of reliable paths as instructed by the SDN controller such that no complete information on the routed data can be obtained at any of the intermediate nodes in the network.

III. SYSTEM MODEL

In this section, we present the optimization problem formulation for the fragmentation-based multipath routing problem that determines the optimal set of multipaths for a given flow request based on network status. In Table I, we summarize all mathematical notations used throughout this paper.

A. Objective Function

The objective function is a measure of the reliability of the paths chosen for routing the n encoded fragments belonging to a flow f . Reliability of a node is defined as the probability that a given node is not compromised due to an attack. We assume that every node's reliability is dynamically updated and known at the SDN controller using the data collected from the network. The reliability of a link r_l is defined as the logarithmic function of the minimum of the reliability of the two nodes that the link connects i.e., $r_l = \log(\min(r_{l_s}, r_{l_d}))$. The $\min$ function ensures that the ingress and egress links of

TABLE I: Mathematical notations

Notation	Description
$\mathcal{G}(\mathcal{N}, \mathcal{E})$	Graph representing the network topology
$\mathcal{N}$	Set of nodes in the network
$\mathcal{E}$	Set of edges/links in the network
f	A traffic flow in the network
s	The source node of flow f
d	The destination node of flow f
$\mathcal{P}$	Set of paths available between a (s, d) pair
n	Total number of encoded fragments for a flow f
k	Total number of data segments for a flow f
l_s	Source node of link l
l_d	Destination node of link l
r_l	Reliability of a link l in the network represented in $\log()$
L	Acceptable delay in choosing a path
β_f	The bandwidth requirement of flow f
B_l	Residual bandwidth on link l
$x_{p,l}$	Integer variable: $x_{p,l}$ represents the total number of fragments routed along link l on path p
y_p	Binary decision variable: $y_p = 1$ if path p is used for routing the flow f , $y_p = 0$ otherwise

a node with low reliability are not selected for routing traffic and hence the unreliable node is most likely ignored while routing. The $\log$ function is used so that, the path reliability of a path p can be given by the summation of r_l over all $l \in p$. Given a flow f , the objective function is to choose a set of paths $p \in \mathcal{P}$ to reliably route the fragments of the flow such that more fragments are routed along the most reliable paths. The objective function is hence to maximize the reliability of the paths chosen for routing weighted by the number of fragments routed along those path.

$$\text{Maximize}_x \sum_{p \in \mathcal{P}} \sum_{l \in \mathcal{E}} r_l x_{p,l} \quad (1)$$

where $x_{p,l}$ is the number of fragments routed on link $l \in p$.

B. Constraints

The optimization problem (1) is subject to the following constraints, imposed by the network and by design.

1) *Flow Conservation Constraints*: A path p selected for routing should be continuous from the source node s , to the destination node d and all the n encoded fragments of the flow f should be routed along the selected set of continuous paths. This constraint is represented by the below three equations.

$$\sum_{p \in \mathcal{P}} \sum_{l \in p, l_s = s} x_{p,l} y_p - \sum_{p \in \mathcal{P}} \sum_{l \in p, l_d = s} x_{p,l} y_p = n, \quad (2)$$

$$\sum_{p \in \mathcal{P}} \sum_{l \in p, l_s = d} x_{p,l} y_p - \sum_{p \in \mathcal{P}} \sum_{l \in p, l_d = d} x_{p,l} y_p = -n, \quad (3)$$

$$\sum_{p \in \mathcal{P}} \sum_{l \in p, l_s = i} x_{p,l} y_p - \sum_{p \in \mathcal{P}} \sum_{l \in p, l_d = i} x_{p,l} y_p = 0, \quad (4)$$

$\forall i \in \mathcal{N} \setminus \{s, d\}$

2) *Reliability Constraint*: For an intruder on a compromised node in the network to be unable to decode the routed flow, the number of fragments on any of the multipaths should not be more than the critical value k . This is because, using erasure coding at least $(k + \epsilon)$ fragments are required for reconstruction of the message at any node in the network if the encoding is known at the node. We assume that the graph $\mathcal{G}$ is m -connected ($m \geq 2$) otherwise the reliability constraints

cannot possibly be satisfied. The constraint is represented by the following two equations.

$$\sum_{l \in p, l_s=s} x_{p,l} y_p - \sum_{l \in p, l_d=s} x_{p,l} y_p \leq k, \quad \forall p \in \mathcal{P} \quad (5)$$

$$\sum_{l \in p, l_d=i} \sum_{p \in \mathcal{P}} x_{p,l} y_p \leq k, \quad \forall l \in \mathcal{E}, \forall i \in \mathcal{N} \setminus \{s, d\} \quad (6)$$

3) *Delay Constraint*: For any path p to be chosen for routing, the total delay (hops) has to be no larger than a given threshold L . The constraint is represented as follows.

$$\sum_{l \in p} y_p \leq L \quad \forall l \in \mathcal{E}, \forall p \in \mathcal{P} \quad (7)$$

where $\mathcal{E}$ is the set of all links in the network topology.

4) *Bandwidth Constraint*: The bandwidth constraint ensures the availability of bandwidth on the links chosen for routing along a path p . With the bandwidth requirement of flow f denoted as β_f , for any link l to be used to route the flow f , it must have sufficient residual bandwidth to accommodate that flow. The constraint is presented as follows.

$$\sum_{p \in \mathcal{P}, l \in p} y_p \beta_f \leq \mathcal{B}_l, \quad \forall l \in \mathcal{E} \quad (8)$$

where $\mathcal{B}_l$ is the residual bandwidth on link l which is updated in the SDN controller based on the current network state.

C. Formal Problem Statement

The Fragmentation-based Multipath Routing (FMR) problem at the SDN controller is formally defined as follows. *Given a flow request with a specified bandwidth requirement, the SDN controller has to select an optimal set of paths from a set of predetermined paths between the source and destination such that each node traversed by the flow does not receive more than k fragments and that the total reliability of the set of paths chosen for routing the n encoded fragments of that flow is maximized.* The FMR problem is mathematically represented as follows:

$$\text{Maximize} \quad \sum_{p \in \mathcal{P}} \sum_{l \in \mathcal{E}} r_l x_{p,l} \quad (9)$$

$$\text{subject to:} \quad (2), (3), (4), (5), (6), (7) \text{ and } (8). \quad (10)$$

The optimization program is solved using the linux GLPK solver. The FMR problem is run for every flow request based on the current network state and updated reliabilities (r_l) at the controller to determine the optimal multipath required to route the n encoded fragments of the flow with segmentation k . Based on the optimal multipath solution, the high performance SDN controller installs the forwarding rules on the corresponding SDN-enabled nodes in the network.

IV. PERFORMANCE STUDY

A. Simulation Setting

The proposed FMR was tested on random topologies with 10 – 50 nodes in the network and an edge connectivity probability of 0.6. The network bandwidth is set to 1000 units on all links. The performance metrics used to evaluate FMR are average weighted path reliability and rejection ratio.

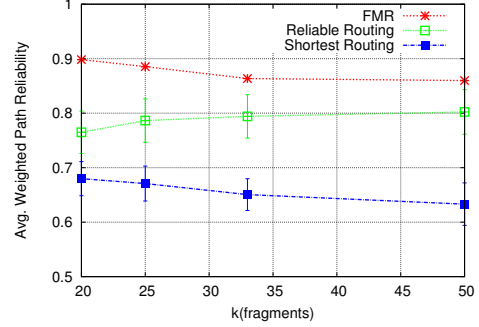


Fig. 1: Single LRN Scenario: Average weighted path reliability with increasing segmentation k .

Average weighted path reliability is the average reliability of the paths chosen for routing the fragments of a flow, weighted by the number of fragments routed on that path. The weighted path reliability of a flow with x fragments routed along path p_1 with reliability r_{p_1} and y fragments routed along path p_2 with reliability r_{p_2} is given by $(x.r_{p_1} + y.r_{p_2})/(x + y)$. Rejection ratio — a measure of blocking performance is the ratio of the number of flows rejected to the total number of flow requests.

We compare the performance of the proposed FMR with disjoint path reliable and shortest routing [7]. The reliable routing mechanism is a less-complex heuristic that can address the FMR problem where the fragments are routed along multiple link-node-disjoint reliable paths. Similar to FMR, the reliable routing mechanism ensures that not more than k fragments are routed along a link-node-disjoint path and hence a node. The shortest routing is a similar to reliable routing mechanism except that the objective of the routing is not reliability but the number of hops between the source and destination of a flow (and hence lesser delay). The fragments of a flow are hence routed along multiple link-node-disjoint shortest paths available in the network topology. The results obtained are plotted with 95% confidence interval.

B. Analysis of Results

1) *Single LRN Scenario*: A Low Reliability Node (LRN) is the node which has a higher probability of attack compared to other nodes in the network. In this scenario, the node reliabilities in the network are uniformly distributed between (0.9, 0.99) and one of the nodes is assigned a very low reliability value of 0.2. FMR and reliable routing are likely to ignore this LRN while routing since they consider reliability values for choosing the paths. However, if no link-node-disjoint paths are available excluding the LRN, the reliable routing may forward the fragments to the LRN. Whereas with shortest routing, if the LRN belongs to the shortest path between the source and destination of that flow, it will forward the fragments to the LRN.

The average weighted path reliabilities of FMR, reliable routing and shortest routing are plotted in Fig. 1. Though reliable routing is less complex than FMR, the average weighted path reliability of FMR is better than reliable routing. This is because, in reliable routing, the fragments are routed along the maximum reliable link-node-disjoint paths. Whereas, FMR is not constrained by link-node-disjoint paths of reliable routing

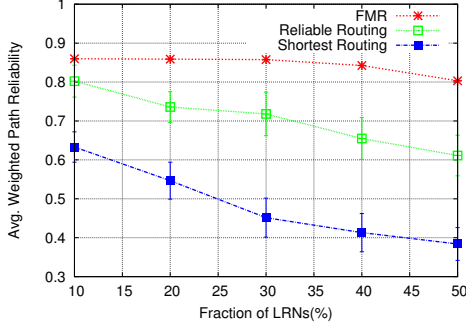


Fig. 2: Multiple LRN Scenario: Average weighted path reliability with varying no. of LRNs, $k = 50$.

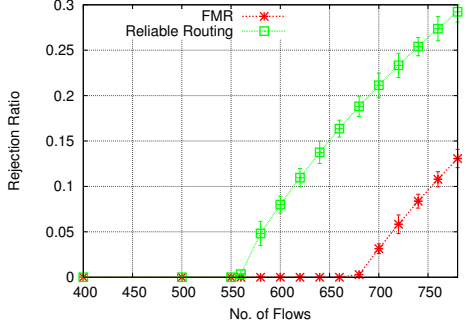


Fig. 3: Rejection ratio with increasing load, $k = 50$.

and hence we observe better reliability values. The slight decrease in the average weighted path reliability in FMR with increasing k is because the path reliabilities are weighted by the number of fragments routed along those paths. In case of shortest routing, as its objective is not reliability, it is observed that it performs worse in terms of average weighted path reliability than both FMR and reliable routing.

2) *Multiple LRN Scenario*: In this scenario, the fraction of LRNs to the total number of nodes in the network is varied and the performance of the routing mechanisms are observed in terms of average weighted path reliability. Fig. 2 presents the weighted path reliabilities of FMR, reliable routing and shortest routing with encoding values (100, 50). It is observed that the weighted path reliability of FMR is 25% higher than reliable routing and 50% higher than shortest routing. This is because FMR searches in a wider set of paths to route the fragments whereas reliable routing searches only among the link-node-disjoint path set. With increasing LRNs in the network, the reliable routing may not be able to find a link-node-disjoint path that excludes the LRNs. Hence the path reliability decreases with increase in the fraction of LRNs in the network. The behaviour of shortest routing is also due to the same reason that the shortest paths available do not exclude the LRNs in their shortest paths for a flow.

3) *Rejection Ratio*: From the previous results, it is observed that with increasing number of LRNs in the network, FMR performs much better than reliable routing. However, with less than 10% of LRNs in the network, the average weighted path reliability of FMR is greater than reliable routing by less than 5%. The difference is significant only with more LRNs in the network. In spite of its complexity, the need for FMR in a scenario with smaller number of LRNs is observed

from the rejection ratio performance. Each data flow in the network is generated with random bandwidth requirement distributed uniformly between (0, 5) units. This data flow is split into k segments and the encoded n fragments are distributed in the network and routed towards the destination. Fig. 3 shows the flow rejection ratio of FMR and reliable routing due to unavailability of bandwidth along the multipaths with increasing network load for $k = 50$ with less than 10% LRNs in the network. It is observed that with increasing load, reliable routing starts rejecting earlier than FMR. This is because, unlike reliable routing FMR is not constrained by link-node-disjoint paths. The traffic is distributed across increased number of paths and hence more number of flows can be accommodated in the network with FMR.

V. CONCLUSIONS

In this paper, we proposed a dynamic Fragmentation-based Multipath Routing (FMR) to provide resilience to security attacks in SDN-based networks. The FMR problem is solved dynamically by the SDN controller based on the current network state. It is to be noted that, while ensuring resiliency through data fragmentation based on erasure coding, FMR tends to ignore the less-reliable nodes in the network to route the data fragments. The results show that on a random topology with the increasing number of low reliability nodes in the network, FMR performs better than disjoint reliable routing by up to 25% in terms of average weighted path reliability. Although disjoint shortest routing incurs lower delay than FMR, the average weighted path reliability of FMR is significantly better than disjoint shortest routing by up to 50%. Also, in terms of flow rejection ratio, FMR accommodates more flows than reliable routing due to better load distribution in the network and hence better blocking performance.

VI. ACKNOWLEDGEMENT

This research work was supported by MoE AcRF Tier-1 grant WBS No: R-263-000-C14-112, NUS, Singapore.

REFERENCES

- [1] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: enabling innovation in campus networks," *ACM CCR*, vol. 38, no. 2, pp. 69–74, Mar. 2008.
- [2] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "Sdn Security: A Survey," in *Future Networks and Services (SDN4FNS)*, 2013 *IEEE SDN for*, Nov 2013, pp. 1–7.
- [3] M. Sathiamoorthy, M. Asteris, D. Papailiopoulos, A. G. Dimakis, R. Vadali, S. Chen, and D. Borthakur, "XORing Elephants: Novel Erasure Codes for Big Data," *Proc. VLDB Endow.*, vol. 6, no. 5, pp. 325–336, Mar. 2013.
- [4] A. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A Survey on Network Codes for Distributed Storage," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476–489, March 2011.
- [5] A. Dimakis, P. Godfrey, Y. Wu, M. Wainwright, and K. Ramchandran, "Network Coding for Distributed Storage Systems," *Information Theory, IEEE Transactions on*, vol. 56, no. 9, pp. 4539–4551, Sept 2010.
- [6] S. Sharma and S. K. Jena, "Cluster based multipath routing protocol for wireless sensor networks," *SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 2, pp. 14–20, Apr. 2015.
- [7] S. K. Singh, T. Das, and A. Jukan, "A survey on internet multipath routing and provisioning," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2157–2175, Fourthquarter 2015.
- [8] X. Liu, S. Mohanraj, M. Piro, and D. Medhi, "Multipath routing from a traffic engineering perspective: How beneficial is it?" in *Network Protocols (ICNP)*, 2014 *IEEE 22nd International Conference on*, Oct 2014, pp. 143–154.