Efficient Random Route Mutation Considering Flow and Network Constraints

Qi Duan, Ehab Al-Shaer and Haadi Jafarian
Department of Software and Information Systems
University of North Carolina at Charlotte
Charlotte, NC, USA

Abstract—In the current network protocol infrastructure, forwarding routes are mostly static except in case of failures or performance issues. However, static route selection offers a significant advantage for adversaries to eavesdrop, or launch DoS attacks on certain network flows. Previous works on multipath routing in wireless networks propose using random forwarding to avoid jamming and blackhole attacks [18]. However, this work is far from being practical for wired network because of many topological and QoS constraints. Moreover, the potential of finding a significant number of disjoint paths in wired networks is extremely low, which consequently decreases the value of RRM.

In this paper, we present a proactive Random Route Mutation (RRM) technique that enables changing randomly the route of the multiple flows in a network simultaneously to defend against reconnaissance, eavesdrop and DoS attacks, while preserving end-to-end QoS properties. Our contributions in this paper are three-fold: (1) modeling RRM as a constraint satisfaction problem using Satisfiability Modulo Theories (SMT) to identify efficient practical route mutations, (2) proposing a new overlay placement technique that can maximize the effectiveness of RRM in visualized networks, and (3) developing analytical and experimental models to measure the effectiveness of RRM under different adversary models and network parameters. We develop a prototype RRM implementation in Software Defined Networks (SDNs). Our analysis, simulation, and preliminary implementation show that RRM can protect at least 90% of the packet flow from being attacked against realistic attackers, as compared with static routes. Our evaluation study also shows that RRM can be efficiently deployed on both conventional networks and SDNs without causing any significant disruption for active flows.

I. INTRODUCTION

In the current network protocol infrastructure, network configuration such as forwarding routes are mostly static. In many protocols, the route choice is based on the shortest path. The static route selection provides a significant advantage for adversaries to eavesdrop the network links and gather information about the network, or launch DoS attacks on certain network flows. Dynamic routing are used for load balancing and reliability, which are usually predictable and cannot provide resiliency to defend against eavesdropping and DoS attacks.

Randomization techniques are commonly used for security. Examples of information randomization include using the one-time virtual number instead of the real credit number for online transactions; instruction set randomization [8], memory address randomization [16], etc. In this paper, we present a proactive Random Route Mutation (RRM) technique that enables changing randomly the route of multiple flows in a network to defend against reconnaissance, eavesdrop and DoS attacks.

The main challenge of RRM is to change the route between given source and destination addresses randomly to disable the attack capabilities to launch an effective eavesdropping or DoS attacks on the specific node or link in the route while considering the following constraints: (1) increasing unpredictability by minimizing the overlap in route mutation (overlap constraint), (2) avoiding overloading any link in the network (capacity constraint), and (3) satisfying the maximum delay or number of hops (QoS constraint).

Mutated routes can be pre-calculated and staged in router configurations in advance and activated on demand. We present SMT [4] based formalizations to model all the RRM constraints in Boolean or arithmetic format and find the satisfying routes using SMT solvers. SMT is a powerful constraint satisfaction solver used in many different areas. An SMT instance is a formula in first-order logic, where some function and predicate symbols have additional interpretations. SMT is the problem of determining whether such a formula is satisfiable. SMT provides a much richer modeling language than is possible with Boolean expressions [2]. The SMT based method can deal with any kind of constraints that can be modeled in Boolean or arithmetic format, and it is convenient to incorporate new constraints.

RRM can be implemented on a traditional IP network by identifying the appropriate sequence of routing and access control changes in the network. We also implement RRM in virtual overlay networks by developing a new Overlay placement that satisfies RRM requirements. To allow for smooth transition between mutations, configuration changes are carefully managed to avoid disrupting any ongoing traffic.

We investigate the feasibility of RRM in conventional network and develop a prototype implementation in SDN. We evaluate the overhead and effectiveness of RRM through simulation and experimentation. Our evaluation results indicate that

- Our RRM formalization can handle many flows and constraints, and thousands of routers and hosts efficiently.
- The RRM is effective against eavesdropping and DoS attacks. RRM can decrease the percentage of attacked packets due to eavesdropping or DoS to less than 10% of the case of static routes.
Previous works on multipath routing in wireless networks propose using random forwarding to avoid jamming and black-hole attacks [18]. However, this work is far from being practical for wired network because of many topological and quality of services constraints. Moreover, unlike previous works [18], we do not use random walk heuristic based algorithms to identify random routes because it is almost infeasible to design a random walk algorithm to satisfy multiple constraints simultaneously.

The major contribution of our work as compared with related works includes:

- We provide an efficient and practical approach to implement RRM in conventional and SDN networks. Previous works in RRM mainly focus on sensor networks and only consider specific constraints for a single flow, while our approach considers the mutation of multiple flows and can accommodate multiple flow-based and and global network-based constraints.
- We developed a new RRM-based overlay placement to increase the number of disjoint paths for the flow, which is important for improving RRM effectiveness.
- We measured RRM effectiveness using different analytical metrics under different application scenarios. We also evaluate the RRM effectiveness under different flow and topology parameters and adversary models.

The rest of the paper is organized as follows: Sec II presents the adversary model for RRM. Sec III discusses the technique approaches for RRM. Sec IV presents the implementation of RRM and the prototype implementations. Sec V shows the evaluation results. Sec VII concludes the work.

II. PROBLEM DEFINITION, HARDNESS AND ADVERSARY MODEL

A. RRM Definition of Single Flow

We can model the network as a directed graph \( G = (V, E) \), where \( V \) is the set of hosts, \( E \) is the set of links. Suppose there is a flow with source \( S \) and destination \( D \) \((S, D \in V)\), and the duration of the flow can be divided into multiple intervals. The goal of RRM is to find a route between \( S \) and \( D \) that satisfies the following constraints for every interval of the flow duration:

- **Capacity constraint**: the new route should not include those nodes or links that are already overloaded or those nodes or links that do not have the bandwidth requirement for the flow.
- **Overlap constraint**: to increase unpredictability and achieve good load balancing, the new route should avoid those intermediate nodes that appear in recently used routes.
- **QoS constraint**: the mutated routes should maintain the required quality, such as bounded delays or number of hops.

These are the basic constraints for RRM. One may add other constraints based on the specific requirement of the flow and the properties of the network. Also note that if there are more than one satisfying routes for the flow, the RRM procedure should choose one satisfying route randomly.

RRM for multiple flows can be defined similarly. In this case one needs to find the route for every flow and there may be additional constraints that are related to the priority of the flows.

B. Hardness of RRM

For RRM of a single flow which requires the upper bound for route length and number of common nodes with previous routes, the problem is NP-complete in general [5]. If we only require an upper bound for the number of common nodes in the route with the most recent route, the problem can be solved in polynomial time [5].

For RRM of multiple flows which requires the upper bound for the number of common node among the flows, the problem is also NP complete since it is the generalization of the single flow case. Even for the special case that no common node among the flows is allowed, the problem is equivalent to the node disjoint path problem, which is also NP-complete [5].

C. Adversary Model

We assume the standard philosophy in network security that the adversary is aware of the route mutation methods used in the network. It is the intrinsic randomness exists in the mutation algorithm that can guarantee the unpredictability of the route selection, not the secrecy of the algorithm itself.

For eavesdropping attackers, we assume that the adversary does not interfere with the normal functioning of the network but only sniff on a portion of the links or nodes in a fixed amount of time. Note that the adversary does not have the ability to sniff the whole network, in which case the adversary can obtain all the traffic of the flow no matter what the routes are chosen. We believe this is a reasonable assumption since any adversary has only limited budget and sniffing on too many links or nodes will increase the probability of detection. We also assume that the adversary can gather all the information sniffed from the network to perform traffic analysis. However, the eavesdropping adversary does not compromise any node or generate/alter traffic in the network.

For DoS attackers, we also assume that the adversary can disrupt a limited number of the links or nodes for some period of time. The adversary may choose to attack the set of links that he/she believes critical for certain flows within the limit of his/her resource.

We define the following types of adversaries:

1. Naive adversary: the adversary can attack network links or nodes randomly for a random time independent of the flow knowledge (e.g., flow identification) and network knowledge (e.g., topology).
2. Realistic adversary: the adversary moves her attack randomly among network links as long as the target flow is not identified. The adversary can also gain the network knowledge (e.g., critical links) increasingly over time via reconnaissance (opportunistic attacker) and launch attack accordingly. Suppose the adversary mutates in every interval and the flow lasts
for $M$ intervals. If the flow uses static route, as long as the adversary hits the route of the flow (the adversary hits the route means that it hits one of the links or nodes in the route), it will stay in the route in the remaining intervals of the flow duration.

III. TECHNICAL APPROACH

A. SMT Formalization of RRM

In this section we present the SMT formalization for RRM.

1) SMT Formalization of a Single Flow: Suppose the network contains $n$ nodes $v_1, \ldots, v_m$ and $m$ edges $e_1, \ldots, e_m$. The incoming edge set of node $v_j$ (1 $\leq j \leq n$) is denoted as $I_j$ and the outgoing edge set of node $v_j$ is denoted as $O_j$.

A valid route of a flow with source $S$ and destination $D$ with QoS (length) constraint can be formalized as follows

$$\sum_{e_i \in O_j} u_i = \sum_{e_i \in I_j} u_i, \quad \forall v_j \text{ except } S \text{ and } D$$

$$\sum_{e_i \in O_j} u_i = 1$$

$$\sum_{e_i \in I_j} u_i = 1$$

$$u_i \leq L$$

$$u_i \in \{0, 1\}, \quad \forall i$$

Here the variable $u_i$ denotes if link $e_i$ appears in the route. If $u_i = 1$, then link $e_i$ is used for the flow. If $u_i = 0$, then $e_i$ is not used for the flow. $L$ is the maximum length for the flow. The first equation guarantees that any node (other than the source and destination) must have balanced outgoing and incoming edges for the flow. The second and third equation guarantees that the source and destination of the flow must be $S$ and $D$. The fourth equation guarantees that the length of the route should be in the required range. The last equation specifies the value range of variable $u_i$.

If we want to guarantee that a previous used route consisting links $e_{i1}, \ldots, e_{ig}$ should not be used for the current route, we can add the following constraint:

$$\neg((u_{i1} = 1) \land \ldots \land (u_{ig} = 1))$$

2) SMT Formalization of Multi-flow: Suppose there are $H$ flows $F_1, \ldots, F_H$, where flow $F_i$ (1 $\leq i \leq H$) has source $S^{(i)}$ and destination $D^{(i)}$. The RRM for these flows can be formalized as follows

$$\sum_{e_i \in O_j} u_{ik} = \sum_{e_i \in I_j} u_{ik}, \quad \forall v_j \text{ except } S^{(k)} \text{ and } D^{(k)}, \forall flow F_k$$

$$\sum_{e_i \in O_{S^{(k)}}} u_{ik} = 1, \forall flow F_k$$

$$\sum_{e_i \in I_{D^{(k)}}} u_{ik} = 1, \forall flow F_k$$

$$\sum_{1 \leq i \leq m} u_{ik} \leq L_k, \forall flow F_k$$

Here the variable $u_{ik}$ denotes if link $e_i$ is used by the route of flow $F_k$, and $L_k$ is the maximum length for flow $F_k$.

The capacity constraint can be formalized as

$$\sum_{k=1}^{H} u_{ik} \leq C_i, \quad 1 \leq i \leq m$$

Here $C_i$ is the maximum number flows allowed to simultaneously pass through the link $e_i$.

B. RRM Through Overlay Placement

Overlay networks were proposed to improve the reliability of the Internet and to facilitate performance sensitive services, such as mission critical networks, high performance cloud computing etc., that are difficult or impossible to deploy natively on the Internet. One important reason to apply RRM in overlay network is that the number of disjoint paths is important for the effectiveness of RRM (see Section V) and we may have large number of disjoint paths when applying RRM through overlay placement. As shown in [19], in conventional networks the number of disjoint paths for a fixed flow is usually very small. However, if we mutate the overlay placement, then the ending nodes of the flow will also mutate, which will increase the number of disjoint paths. In an overlay network, we can apply RRM in two levels. The first level RRM is to mutate the route in the substrate layer. The second level RRM is to mutate the overlay node placement. Any mutation in the overlay node placement will automatically enforce the mutation of route.

The formal definition of overlay network mapping is as follows. Suppose the overlay network can be modeled as graph $G' = (V', E')$, where $|V'| = n$. There are $H$ flows $F_1, \ldots, F_H$ in the overlay network. Flow $F_i$ has starting node $s(i)$ and ending node $d(i)$. The substrate network can be modeled as graph $G = (V, E)$, where $|V| = m_1$. We need to find a mapping between overlay nodes and substrate nodes with the following constraints:

- **Unique Mapping Constraint**: every overlay node should be mapped to exactly one substrate node, and two distinct overlay nodes should not be mapped to the same substrate node.
- **Disjoint Route Constraint**: the placement must guarantee that there are enough number of disjoint routes between the corresponding substrate source and destination of the overlay flows.
- **Unpredictability Constraint**: there should be enough difference between the old and new placement.

The unique mapping constraint can be formalized in SMT
as follows:

\[ \sum_{j=1}^{m_1} b_{ij} = 1, \ 1 \leq i \leq n \]

\[ \sum_{i=1}^{n} b_{ij} \leq 1, \ 1 \leq j \leq m_1 \]

\[ 0 \leq b_{ij} \leq 1, \ 1 \leq i \leq n, \ 1 \leq j \leq m_1 \]

Here we use variables \( b_{ij} \) (\( 1 \leq i \leq n, \ 1 \leq j \leq m_1 \)) to denote the mapping between overlay and underlay nodes. If \( b_{ij} = 1 \), overlay node \( i \) is mapped to substrate node \( j \), otherwise it is not mapped to substrate node \( j \).

If we require that the number of disjoint routes between the corresponding substrate nodes for flow \( F_i \) in overlay network should be at least \( \zeta_i \), we can formalize the disjoint route constraint as follows:

\[ ((b_{s(i)j} = 1) \land (b_{d(i)k} = 1)) \implies \Gamma_{jk} \geq \zeta_i, \ \forall i \]

In the above formalization, \( \Gamma_{jk} \) is the number of disjoint routes between \( v_j \) to \( v_k \) in the substrate.

To guarantee the unpredictability of the overlay placement, we can define the distance between two placements as the number of overlay nodes that have different substrate mappings in the two placements. Suppose the two overlay placements are \( \mu_1 \) and \( \mu_2 \), then the distance between \( \mu_1 \) and \( \mu_2 \) can be defined as

\[ d(\mu_1, \mu_2) = \sum_{1 \leq i \leq n} \sigma_i \]

\[ (\sigma_i = 1) \iff (\mu_1(i) \neq \mu_2(i)), \ 1 \leq i \leq n \]

\[ \sigma_i \in \{0, 1\}, \ 1 \leq i \leq n \]

Now the unpredictability constraint can be formalized as follows:

\[ \sigma_i \geq B \]

Here \( B \) is the lower bound for the distance between the old placement and new placement.

IV. RRM IMPLEMENTATION AND DEPLOYMENT

A. RRM IMPLEMENTATION IN CONVENTIONAL NETWORK

There are three steps to implement RRM: (1) identifying the optimal route mutation (as described before), (2) identifying the correct sequence of configuration changes that will implement this route change without interrupting on-going traffic or violating configuration and security requirements, (3) automating the configuration process of RRM to ensure state consistency.

Routing tables, in general, can be built by using static, default, and dynamic routes. Network administrators can configure the routes built by different routing protocols. For example, to configure static routes in Cisco routers the administrator can specify the exact routing entry by using the command "ip route" such as in this example: #ip route 192.168.1.0 255.255.255.0 serial0 permanent. This means creating a static route for IP destination 192.168.1.0 and mask 255.255.255.0 via interface serial 0. The administrator can also define the priority of the static entry (called also administrative distance) to override dynamic route entries.

To change the route of a flow, we need to make sure existing connections are not interrupted.

As an example, suppose in the network shown in Fig. 1, the original route from \( S \) to \( D \) is through routers \( R_1, R_2, R_3 \) and \( R_4 \) (shown in solid arrow lines in the figure). We want to switch the route from \( S \) to \( D \) through \( R_1, R_5, R_6, R_3, R_7 \), and \( R_8 \) (shown in dashed arrow lines in the figure). To maintain the consistency of the update, we require that every packet from \( S \) to \( D \) either take the old route or the new route, but not the combination of two routes. We can see that there is no satisfying order to achieve the consistent update. If we first modify the routing table of \( R_3 \), then some packet coming from \( R_2 \) may be routed to \( R_7 \), which is a violation because it uses both routes. If we first modify the routing table of \( R_1 \), then some packet coming from \( R_6 \) may be routed to \( R_4 \), which is also a violation. One possible way to solve this problem is to add a label in the packet header. The route transition can be done with following steps:

- Add the new routing entry for packets with new label in routers \( R_1, R_5, R_6, R_3, R_7, R_8 \).
- \( S \) begin to send packets with new labels.
- Wait a period of time that equals the maximum delay between \( S \) and \( D \).
- Delete the routing entry for packets with old labels in \( R_1, R_2, R_3 \) and \( R_4 \).

B. RRM IMPLEMENTATION IN SDNs

Software-defined networks (SDNs) provide flexible infrastructure for developing and managing random host mutation efficiently and with minimal operational overhead. In SDN, the network controller (e.g., NOX [6]) monitors and controls the entire network from a central vantage point via an interface, such as OpenFlow [13] and defines the forwarding and address translation behavior of switches distributed in the network accurately and synchronously.

We implement RRM in a large Mininet network controlled by a NOX controller. The NOX controller acts as the central authority to manage flow installation and route mutation in switches. For scalability, this architecture can be easily extended to include several controllers, each managing a segment of the network. OF-switches are configured to encapsulate unmatched packets (that have no matching flows in flow tables) and send them to the controller. The NOX controller
installs necessary routing entries in all OF-switches in the route of every flow, and each connection must be associated with a unique flow. This property guarantees the end to end reachability of hosts, because the connectivity for a specific connection must be maintained regardless of subsequent route mutations. Any route update is handled directly by the NOX controller. Our prototype implementation shows that RRM can be done smoothly in SDN. The details of the prototype implementation can be found in [3].

V. EVALUATION

We evaluate the overhead and effectiveness of RRM through simulation and experimentation.

A. Evaluation Metrics

In this paper, we use two metrics to evaluate the effectiveness of RRM, namely \( MPE \) (Mutation Protection Effectiveness) and threshold \( MPE \). \( MPE \) is defined to be the percentage of packets in a flow that do not pass through any intermediate nodes that are being eavesdropped or compromised. Note that the requirement for minimum \( MPE \) is application dependent. If the packets of the flow have plaintext content such as emails, the adversary may only need to eavesdrop a small percentage of the packets of the flow. If the packets in the application are encrypted and the adversary wants to collect encrypted packets to carry out cryptanalysis, he/she may need to sniff simultaneously on multiple routes to get enough number of packets for cryptanalysis. \( MPE \) calculates the average case effectiveness which is appropriate to use to compare between different RRM techniques. Threshold \( MPE \) denotes the probability that there is at least \( l \) (\( l < M \)) compromised intervals, given that there are \( N \) available disjoint routes, attacker can choose \( R \) from \( N \) at each mutation interval to attack in \( M \) mutation intervals.

If the defender randomly chooses a route in every mutation interval, and the attacker always randomly chooses \( R \) routes to attack, then the expected \( MPE \) is

\[
MPE = 1 - \sum_{i=1}^{M} \frac{R}{N} \frac{1}{M} d_i
\]

Here \( d_i \) is the damage rate when the attacker attacks the route that is used by the flow during interval \( i \). For example if a DoS attack on a link causes 20% packet drop, then \( d_i = 0.2 \). \( R/N \) is the probability that the chosen route is attacked, and \( 1/M \) is the fraction of packets sent in this interval. If \( d_i = 1 \), then \( MPE \) is just \( R/N \).

Threshold \( MPE \) can be calculated as

\[
\left( 1 - \sum_{i=0}^{l-1} \binom{M}{i} (R/N)^i (1 - R/N)^{M-i} \right)
\]

(1)

Note that when the routes are not disjoint, we cannot use Equation 1 to calculate the threshold \( MPE \) since the probability of compromising two different routes may not be independent, in this case we should not apply the binomial formula.

Note that both the \( MPE \) metric and the threshold \( MPE \) metric are useful to evaluate the effectiveness of RRM. Threshold \( MPE \) is useful if the defender uses Shamir's threshold \( k \)-out-of-\( n \) secret sharing scheme [17] or other information redundancy coding schemes. In this case the threshold can be precisely defined. In the scenario that one needs the precise measurement of packet loss or information gained by the adversary, one should use \( MPE \). \( MPE \) provides a precise view for packet loss or adversary information gain. Threshold \( MPE \) uses the precise threshold which may not capture the complete picture of the behavior of RRM. Also, for some topology or simulation parameters, \( MPE \) can show the impact where threshold \( MPE \) cannot show the impact because the \( MPE \) metric is more sensitive than the threshold \( MPE \) metric.

B. Evaluation Methodology

We evaluate the overhead and effectiveness of RRM. For RRM overhead, we measure the time for SMT solving for the flow mutation. For RRM effectiveness, we study the RRM effectiveness in ideal topologies (topologies with a number of complete disjoint routes between the source and destination) and random topologies. We study the impact of the following parameters on \( MPE \):

- The number of disjoint routes between flow source and destination (denoted as \( N \)).
- The knowledge of the attacker (percentage of routes known to the attacker, denoted as \( p \)).
- The attack capability, that is, the maximum number of routes that an attacker can attack simultaneously (denoted as \( R \)).
- The number of mutation intervals of the flow (denoted as \( M \)).

Suppose the sender randomly uses \( N \) routes uniformly between the source and destination. These routes have length from 1 to \( L \) (which means the maximum length is \( L \)). Denote the fractions of routes with length \( i \) over the total number of distinct routes \( N \) as \( a_i \), and the probability of compromising one link is \( x \), then the prob. of compromising one route is

\[
T = \sum_{i=1}^{L} a_i (1 - (1 - x)^i)
\]

The \( MPE \) equals \( 1 - T \) if the mutation over these routes is uniform.

For random topologies with overlapping routes, we consider the following factors that may have impact on \( MPE \):

- Network size, denoted as \( N_1 \).
- Average network degree, denoted as \( D_1 \).
- Attacker knowledge (percentage of links known to the attacker), denoted as \( p \).

In our evaluation, all the evaluation examples were done on a machine with a 3G Intel Pentium IV CPU and Linux Operating System.
C. Network Generation and Parsing Module

We use BRITE [14] as the network generator for the evaluation. We use the Waxman model [14] to generate random topology with the two parameters of Waxman model as \( \alpha = 0.2 \) and \( \beta = 0.15 \). The network growth type is set to be incremental.

D. Mutation Overhead Evaluation

**Overhead of SMT Formalization for Multi-flow Route Selection:** Fig. 2 shows the time of SMT solving for route selection with overlap constraint in a network that have 5 flows. In the figure, \( w \) is the number of previous intervals that the new route should not repeat. We can see that the SMT solving time increases when the network size increases, especially when the number of routers in the network reaches 300. This is also because the number of possible routes increases exponentially with the size of the network. We consider the improvement of the SMT formalization as future work.

Fig. 3 shows the time of SMT solving for route selection with capacity constraint in a network that have \( H \) flows. We can see that the SMT solving time increases when the number of flows increases. This is because that the solver needs to consider more constraints than the single flow case. The SMT solving time decreases when the allowed number of flows in the routers increases. This is because that the solver may be able to find more solutions when the allowed number of flows in the routers increases. In other words, the SMT solving time decreases when there are more possible satisfying solutions. Note that when the allowed capacity is less than 2 (which is equivalent to no router should have two flows), then the SMT solver may not be able to find a satisfiable solution so the X axis of the figure starts at 2. When the SMT solver failed to find a solution, it means that the constraints cannot by satisfied at the same time. In this case one must relax some of the constraints until a satisfying solution is found.

**Overhead of SMT Formalization for Overlay Mapping:** Fig. 4 shows the time of SMT solving for the mapping of an overlay network with 100 nodes. The mapping should satisfy unique mapping and unpredictability constraint.

**Routing Update Overhead of RRM:** The routing update overhead of RRM can be estimated by the average length of the route of every RRM interval, if we assume the number of overlapping nodes between the old route and new route is small. Fig. 6 shows the average length of the route found by the SMT formalization for Waxman random networks with different size and different length upper bound. We can see time increases when the size of the substrate network or the number of overlay flow increases. Fig. 5 shows the time of SMT solving for the mapping of an overlay network with \( N_2 \) nodes and 20 flows. The mapping should satisfy unique mapping and unpredictability constraint.
that the average route length of the RRM algorithm converges to some value with the increase of the network size.

E. Comparison Between RRM and non-RRM in Topologies with Disjoint Routes

It is easy to see when the adversary moves naively uniformly, RRM has no effect. To see this, first assume that the defender and the attacker mutates with the same speed and the number of disjoint routes used by the flow is $N$. The probability that both the defender and the attacker are in the same route during all $N$ intervals is $1/(N*N) + N = 1/N$. If the defender is static (no RRM) and the attacker is moving uniformly, then the flow will also be hit with probability $1/N$ for every interval. Assuming the ratio of mutation speed between the defender and attacker is $k$. If $k < 1$, then for every defender mutation interval, the attacker will move $1/k$ times, and every time the flow will be hit with probability $1/N$. So in total for every defender mutation interval, the average damage done by the attacker will be the same as that in the case where $k = 1$ (moving with same speed). The case where $k > 1$ is similar. This proves that RRM has the no effect under the naive uniform attacker model. So in the evaluation we will focus on the realistic attacker model.

Fig. 7, Fig. 8 and Fig. 9 show the comparison of $MPE$ between RRM and non-RRM for realistic attackers. Fig. 7, we can see RRM has significant advantage over non-RRM under the realistic attacker model. The RRM $MPE$ is a constant for a fixed $T$. The advantage of RRM increases when the flow duration is longer. With the increase of $T$, the advantage gradually decreases. From Fig. 8 we can see that for fixed $R$, the advantage of RRM over static route gradually diminishes with the increase of $N$. This is because for large $N$, the attacker needs longer time to hit the static route. In Fig. 9, all routes used by the sender have length $L$. The advantage of RRM decreases when $L$ increases or $x$ increases. This is because when $L$ increases or $x$ increases, the probability that a route is compromised will increase.

F. Evaluation of Threshold $MPE$ Metric in Disjoint Routes

Impact of Flow Tolerance on Threshold $MPE$: Here we define the percentage of compromised packets that a flow can tolerate as $Tol^+ = l/M$. Fig. 10 shows the effect of $Tol^+$ and $N$ on threshold $MPE$. Here we have $M = 20$ and $R = 10$. This figure shows that

- For non-RRM (static flow), the threshold $MPE$ is always the value $R/N$.
- When $N$ increases, threshold $MPE$ decreases and approaches 0.
- Threshold $MPE$ approaches 1 more quickly for smaller $Tol^+$ values.
• When $N$ is less than threshold value $R/T_{ol}^+$, increasing $M$ hurts RRM. When $N$ is greater than $R/T_{ol}^+$, increasing $M$ helps RRM.

• The impact on threshold $MPE$ diminishes quickly after $N$ reaches some value. This means that after some threshold (which depends on tolerance), increasing $N$ has very low payoff.

Note that in this comparison we assume that the attacker is static. For non-RRM (static route), if the attacker is also static, when the route is hit, the flow will be hurt under the threshold $MPE$ metric. So in this case the threshold $MPE$ value is always $R/N$, the probability of the static route is hit. This is independent of value of $T_{ol}^+$. So in the figure we can see that the three curves for the cases of non-RRM are the same.

If the attacker is also moving with the same speed as the defender (attack different $R$ routes in every interval), then the threshold $MPE$ for non-RRM can also be calculated using Equation. 1, which is the same as the case of RRM. This means that RRM has no effectiveness under the threshold $MPE$ metric if the attacker is moving with the same speed as the defender.

Impact of $M$ on Threshold $MPE$: Fig. 11 shows the impact of $M$ on threshold $MPE$ when $T_{ol}^+ = 0.2$ and $R = 10$. This figure also shows that when $N$ is less than threshold value $R/T_{ol}^+$, increasing $M$ hurts RRM. When $N$ is greater than $R/T_{ol}^+$, increasing $M$ helps RRM.

G. Comparison Between RRM and non-RRM in Topologies with Overlapping Routes

Impact of Network Size: Fig. 12 shows the $MPE$ for a flow in a network with 300 nodes and $p = 70\%$. We can observe that network degree has significant impact on $MPE$. When $D_1$ increases from 4 to 7, the $MPE$ may increase more than 2 times.

• The $MPE$ of the flow approaches 1 when the percentage of sniffed links increases reaches certain threshold. This means that if the adversary sniff on too many links, all possible routes will be sniffed and RRM will lose its effectiveness. However, an adversary has only limited budget and it is difficult to sniff on a large number of links without being detected.

Impact of Average Network Degree: Fig. 13 shows the $MPE$ for a flow in a network with 300 nodes and $p = 70\%$. We assume that every satisfying route is selected with equal probability. Note that in this figure and Fig. 13 and Fig. 14 we also show the $MPE$ for the case of static routes (non-RRM) with number of intervals $M=20$. We have the following observations:

• The percentage of sniff packets of the flow (which is equal to $1 - MPE$) increases when the percentage of sniffed links increases.
effectively. We show that it is feasible to deploy RRM in defense against eavesdropping and infrastructure DoS attacks. Our work provides a general formalization for RRM with various operational and QoS constraints. The route selection is random and the new constraints can be added conveniently.

VI. RELATED WORKS

The introduction of SMT can be found in [2]. Applying multipath routing in computer networks had been proposed as early as 1970s, but the original purpose is mainly for load balancing. The protocols such as Split Multiple Routing (SMR) [9], multipath DSR [7], AODV [11], AODMV [19], try to find disjoint paths in routing. However, in practical networks, the number of disjoint paths is usually very small [19]. Other protocols that try to improve security through multipath routing such as SPREAD [10], SRP [15], SecMR [12]. The route selection in these protocols are deterministic. This means if the attacker knows the algorithm, the routes can be predicted. The multipath algorithm in [18] can generate randomized multipath routes that are also highly dispersive and energy efficient in wireless sensor networks. The algorithm is also based on random walk and its variants and the generated multipath routes are highly resilient to black hole attacks.

Our work provides a general formalization for RRM with various operational and QoS constraints. The route selection is random and the new constraints can be added conveniently.

VII. CONCLUSION

In this paper we present a mutable network framework called random route mutation (RRM) for proactive moving target defense. To the best of our knowledge, RRM is the first proposed technique that offers an efficient practical random route mutation that considers flow and network constraints for any general network. Our analysis, simulation and preliminary implementation show that RRM is feasible, flexible and can defend against eavesdropping and infrastructure DoS attacks effectively. We show that it is feasible to deploy RRM in conventional network and develop a prototype implementation in SDN network. We show that RRM can decrease the percentage of eavesdropped or disrupted packets to less than 10% of the case without RRM by comprehensive evaluation. RRM proposed in this paper is purely proactive and it does not assume any real-time feedback or knowledge about the adversary. However, in the future we plan to apply game theory based technique to develop a reactive RRM.

REFERENCES