Path Hopping: an MTD Strategy for Quantum-safe Communication

Reihaneh Safavi-Naini
University of Calgary
Calgary, Canada

Alireza Poostindouz
University of Calgary
Calgary, Canada

Viliam Lisy
Czech Technical University
Prague, Czech Republic

ABSTRACT

Moving target defense (MTD) strategies have been widely studied for securing computer communication systems. We consider using MTD strategies as a cryptographic mechanism for providing secure communication when the adversary has access to a quantum computer and security is required over a long period of time. We assume Alice and Bob are connected by multiple disjoint paths, not all of which can be eavesdropped by the attacker at the same time. We propose a cryptographic system that uses an MTD strategy that achieves long-term quantum-safe security. We model the system as a Markov chain, and propose two security measures that correspond to two types of adversaries, called risk-taking and risk-averse. Our numerical simulations shows dependencies between system parameters, and leads to new insights, such as quantifying the cost of being a risk-averse adversary.

KEYWORDS

Moving Target Defense; Quantum-safe communication; Mobile adversary; Markov game for security

1 INTRODUCTION

Cryptographic infrastructure of the Internet allows users from across the world to establish authenticated, confidential communication channels and interact securely. Peter Shor's discovery of a quantum algorithm that can efficiently solve integer factorization and discrete logarithm problems [9], the two mathematical problems that are the basis of the security of the most prominent public key crypto algorithms such as RSA public key encryption and Diffie-Hellman key agreement, effectively brings down the cryptographic infrastructure of the Internet. The main approaches to quantum-safe cryptography are by using (i) quantum cryptographic models and algorithms, (ii) cryptographic algorithms that rely on computational assumptions that do not have known efficient quantum algorithms for solving them [7], and (iii) cryptographic systems that use physical assumptions. This last approach results in information theoretically secure systems and is followed in this paper.

A prominent and widely researched direction in information theoretically secure communication is *physical layer security* systems that base security on assumptions about physical environment [10]. In this paper we assume there are multiple disjoint communication *paths* between the sender and the receiver. A path is an abstraction of a channel and can have different realizations. For example a communication frequency between a sender and a receiver in wireless communication, corresponds to a path. Similarly, a sequence of routers that are used to transmit messages from the sender to the receiver, define a path over the Internet. We assume that although the set of all paths (e.g. possible frequencies) is known to the attacker, there is a bound on the attacker's resources and so they cannot eavesdrop all the paths at the same time. Communicants also have limited resources and use a subset of paths at a time.

To provide cryptographic security against the attacker whose goal is to eavesdrop the message, the sender chooses K of the N available paths, breaks the message m into K shares, and sends each share along one of the paths. If the shares are generated using a (K, K)-secret sharing scheme, eavesdropping even $K-1$ paths will provide perfect information theoretic security for the message against the attacker. We propose "path hopping", where the sender and the receiver regularly change ("hop") one or more of their chosen paths, and effectively extend the protection of the system that was initially due attacker's lack of knowledge about the K paths, over time. This is effectively using MTD for providing cryptographic security.

2 THE MTD GAME OF PATH HOPPING

We consider the following setting: there is a message source that generates a stream of data that must be protected against an eavesdropper (Eve). There are N communication paths that connect the sender (Alice) to the receiver (Bob). To protect message transmission against an eavesdropper who can get access to up to K paths, the sender does the following: (i) randomly chooses a subset S_D of K out of N available paths; (ii) uses a (K, K)-secret sharing to construct K shares for the message, and (iii) sends each share on one of the selected paths. The paths in S_D are also called *target paths.* The receiver knows the paths that are used by the sender (we assume sender and receiver share a secure pseudorandom generator) and so can reconstruct the sent message. The eavesdropper gets access to a subset $S_A \subseteq S_D$ of the target paths. Because of the security of the (K, K)-secret sharing scheme, if $|S_A| \leq K-1$, the attacker will stay completely uncertain about the message.

We assume an *adaptive and mobile* eavesdropper who can probe a path to see if it carries the sought message stream (e.g specified by header information), and if not, will try another path in their next action point (time step). If the set S_D is fixed, the eavesdropper will eventually compromise the system and will find the message stream. The attacker can do this slowly and so will remain fully

MTD'17, October 30, 2017, Dallas, TX, USA

ACM ISBN 978-1-4503-5176-8/17/10…$15.00
https://doi.org/10.1145/3140549.3140560

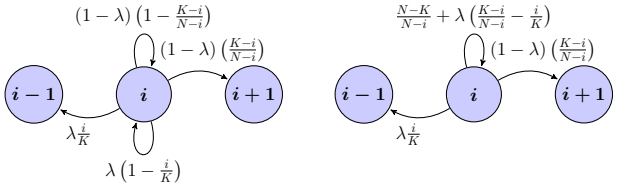

Figure 1: State transition probabilities for case C1. The left diagram shows the defender's moves, λM^D, with arrows bellow and attacker's moves, $(1-\lambda)M^A$, with arrows above. The right diagram shows the combined transition matrix $M = \lambda M^D + (1-\lambda)M^A$.

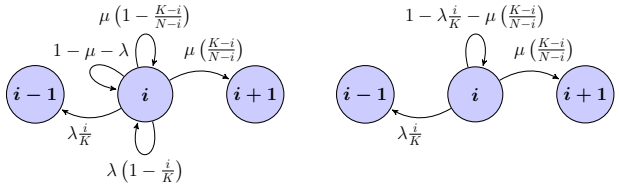

Figure 2: State transition probabilities for case C2. The left diagram shows the defender's moves, λM^D, with arrows bellow and attacker's moves, μM^A, with arrows above and the no move $1-\mu-\lambda$. The right diagram shows the combined transition matrix $M = \lambda M^D + \mu M^A + (1-\lambda-\mu)I$.

undetected. We assume the attacker can eavesdrop up to K paths, but only eavesdrop those that carry data[1].

To protect against this adversary, the sender and receiver will *hop* one or more of the paths in S_D. We assume in each time step, the defender only hops one path and attacker only changes one of his probing paths. We use the MTD game framework of [3] and model the problem as a dynamic system (game) influenced by (between) two *players,* a *defender* that includes the *sender* and the *receiver*, and an *attacker*. The attacker wins the MTD game if they find the K target paths in S_D. The system implements the defender's MTD strategy. In each time step we have one of the three possibilities: only defender moves with probability λ, only attacker moves with probability μ and we have no action with probability $1-\lambda-\mu$.

The system is modelled as a Markov chain, where states are labeled by $i \in \{0, 1, \cdots, K\}$, and in state i the number of target paths known to the adversary is i. The winning state is labeled by K (the adversary knows all the K target paths). We consider a defender who plays a *memoryless strategy*: at every time step, the defender plays (issues a move) irrespective of the information learnt about the attacker. In each move, the defender will choose one of the K target paths at random, and re-allocate it to a randomly chosen non-target path ($N-K$ possible non-target paths). The chosen path may belong to S_A (attacker's set of known paths), or be outside the set. In each time step, the adversary moves with probability μ and randomly selects one of the possible target paths (paths outside S_A) and learns if it is a message carrying path (target path) or not.

In each time step, defender gets the chance to act first and they move with probability λ. In the same time step, attacker will have the chance to move also. If the attacker does not move, they will have the chance of loosing one of the paths in S_A in the next time step, because the defender plays a memoryless strategy.

To reduce the probability of loosing a target path while waiting, the attacker should act when possible and use the available $1-\lambda$ action rate. We refer to this attacker as a *risk-taking* attacker. On the other hand more frequent attacks have the risk of triggering alarm in the defender's intrusion detection system (IDS), tightening security and reducing access to the system. Let τ be a threshold that is used by the defender's IDS to raise the threat level of the system. To avoid reduction in accessing the system, the attacker may try to keep their attack rate below τ. We refer to this attacker as a *risk-averse* attacker. Thus, in each time step the attacker moves with probability

$$\mu = \min\{\tau, 1-\lambda\}. \tag{1}$$

The system transition matrix thus, will be

$$M = \lambda M^D + \mu M^A + (1-\lambda-\mu)I_{k+1},$$

where M^D and M^A describe defender's and attacker's actions, respectively. Equation (1) shows that, depending on the value of τ (the attack detection threshold of the defender), we have two cases.

C1: $\tau > 1-\lambda$. In this case from (1), we have $\mu = 1-\lambda$, and

$$M = \lambda M^D + (1-\lambda)M^A. \tag{2}$$

C2: $\tau < 1-\lambda$. In this case from (1), we have $\mu = \tau$ and,

$$M = \lambda M^D + \tau M^A + (1-\lambda-\tau)I_{k+1}. \tag{3}$$

Note that we refer to C1 and C2 as risk-taking and risk averse attacker, respectively, to emphasize that the attacker may ignore the threshold τ and use all available probability $1-\lambda$, or prefer to stay below alarm state of IDS, defined by τ.

The case C1

State transition probabilities are given by Equation (2). Figure 1 (left) shows state transition probabilities due to the attacker's and defender's actions. The transition probabilities on the upper part of the figure are due to attacker's action. Figure 1 (right) shows the combined transition probabilities.

The state transition matrix M can be obtained from transition probabilities in Figure 1 (right). It is easy to see that the Markov chain is irreducible and aperiodic. The stationary probability distribution of the system is given by $\pi = (\pi(0) \cdots \pi(K))$, where $\pi M = \pi$.

The case C2

In this case, state transition is given by Equation (3). At each time step, either (i) defender moves (randomize) with probability λ, or (ii) attacker moves with probability τ, or (iii) no-one moves with probability $1-\lambda-\tau$.

The adversary knows the state and moves with probability τ. There will be no move with probability $1-\lambda-\tau$. The state transition matrix M can be obtained from transition diagram in Figure 2 (right). Again the Markov process is irreducible and aperiodic and a limiting stationary distribution $\pi = (\pi(0) \cdots \pi(K))$, always exists.

[1]One can also consider a case where the attacker always eavesdrop on K paths. Although the analysis approach in that case will be similar, the actual calculations will be different.

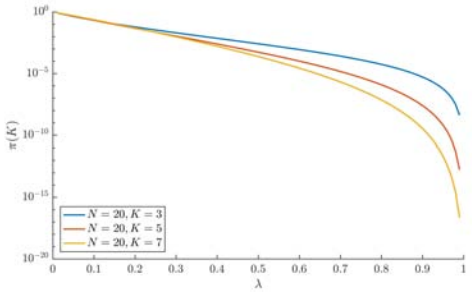

Figure 3: Numerical results for $\pi(K)$ as a function of λ for $N = 20$ and different values of K for the case C1.

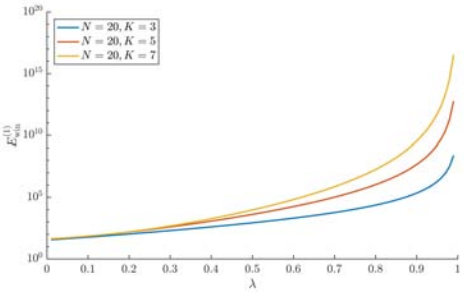

Figure 4: Numerical results for $E^{(1)}_{\text{win}}$ as a function of λ for $N = 20$ and different values of K for the case C1.

3 SECURITY ANALYSIS

We use two security measures related to the success criteria of the attack.

Expected number of compromise

Consider the system over a period of T time steps, starting from state 0. The expected number of times that the system is in a compromised state, that is the attacker can learn the communicated message, is an important security measure. Note that one can use coding strategies [6] to spread information over longer sequences, and so estimating the number of compromise will provide the required parameter for encoding .

Theorem 3.1. *For an MTD game with transition matrix M and stationary distribution $\pi = (\pi(0), \pi(1), \cdots, \pi(K))$, where K is the winning state, L_T, the expected number of times the adversary wins in the first T time steps, assuming that the game starts with the $\mathbf{0} = (1, 0, \cdots, 0)$ distribution, is less than $T \cdot \pi(K)$.*

It is easy to prove this theorem using similar arguments discussed in [3]. In our numerical computation we use $\pi(K)$, the winning probability in the stationary state, to represent this security measure.

Expected number of steps to first time win

Expected number of steps to first time compromise is an important measure for defender to estimate unbreakability of the system, and for the attacker to estimate the work (in terms of the number of time steps, that could be translated into attacker's cost) needed to break the system. This measure can be analytically calculated using the following theorem. Proof is omitted because of space.

Theorem 3.2. *Consider an MTD game with transition matrix M. Let v_j denote the expected number of times to reach the state K (the winning state) for the first time if the game M has started with state j. We have*

$$\boldsymbol{v} = \boldsymbol{r} + \tilde{M}\boldsymbol{v}, \tag{4}$$

where $\boldsymbol{r}(j) = 1$ for all $j \in \{0, \cdots, K-1\}$, and $\tilde{M}$ is the same matrix as M with the last (K^{th}) row removed .

4 NUMERICAL RESULTS

We used the results of Section 3 to calculate $\pi(K)$ and $E^{(1)}_{\text{win}}$ for different choices of N, K, λ and μ. To calculate $E^{(1)}_{\text{win}}$, we used the results of Theorem 3.2 and employed the linear equation solver (`linsolve`) of MATHLAB to solve the set of equations $\boldsymbol{v} = \boldsymbol{r} + \tilde{M}\boldsymbol{v}$ for each parameter set. For large values of K, M becomes near-singular and an exact solution cannot be found. This explains the choice of $K < 10$ in our graphs. To calculate $\pi(K)$ we used MATLAB eigenvector analysis function (`[V,D]=eig(M')`) to find for the stationary distribution π where $\pi M = \pi$.

The case C1

For fixed N and K, as λ increases $\pi(K)$ decreases. For fixed N and λ, when K increases, $\pi(K)$ decreases. Both these imply better security as expected from more dynamic systems (Figure 3).

Figure 6 and Figure 7 show that for fixed N and λ, increase in K results in the reduction of $\pi(K)$ and increase in $E^{(1)}_{\text{win}}$; and so better security. However, this gain in security diminishes after K reaches a threshold. In this last case almost all paths are target paths and so attacker's chance of correctly guessing is high. The thresholding behaviour suggests using higher K (and so higher system cost) will not have a substantial effect on security.

The figures also show that for fixed K as λ increases, $\pi(K)$ decreases. For example, for $N = 20$, $K = 3, 5$, and 7, for all $\lambda \geq 0.6$ we have $\pi(K) \leq 10^{-3}$ (see Figure 3).

Figure 4 shows that for given parameters N and K, increasing λ increases security of the game. Moreover, we can observe that $E^{(1)}_{\text{win}}$ behaves linearly in the log graphs of Figure 4 as λ increases and it increases more rapidly for higher λ's. Therefore, the risk-taking attacker in this case needs exponentially longer time to compromise the system with increasing λ.

We also observe that for given N and λ, as K increases, after a certain threshold value, $\pi(K)$ increases. For example for $N = 20$, $K = N - 1 = 19$ and $\lambda = 0.2$, this threshold is $\pi(K) = 0.57$ (see Figure 6). For $\lambda > 0.5$; however, even for $K = N - 1$, $\pi(K)$ remains small (very close to zero). The same behaviour, also exists for $E^{(1)}_{\text{win}}$: the expected value for the first win of the adversary decreases as K increases for given N and λ; however, this decrease in the security of the communication is negligible if λ is sufficiently large (see Figure 7).

The case C2

Extensive numerical computation for the case C2 shows that, similar to the case C1, the defender achieves better security by choosing higher λ's.

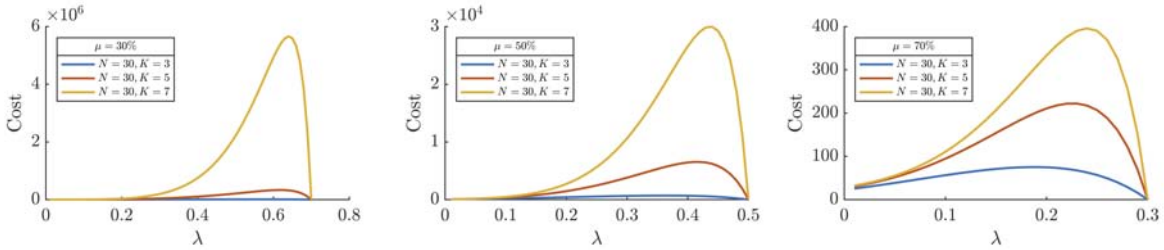

Figure 5: The Cost of being risk-averse in terms of $E^{(1)}_{\text{win}}$ as a function of λ for $N = 30$ and different values of K, and μ.

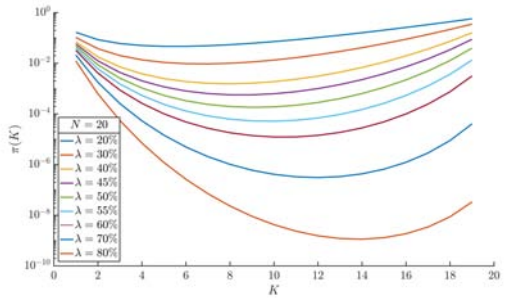

Figure 6: Numerical results of $\pi(K)$ as a function of K for $N = 20$ and different values of λ.

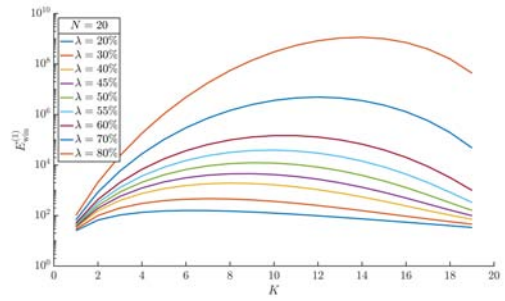

Figure 7: Numerical results of $E^{(1)}_{\text{win}}$ as a function of K for $N = 20$ and different values of λ.

5 UTILITIES

There are costs and gains associated with the defender's and the attacker's actions. In the following we estimate the cost of being a risk-averse adversary.

Estimating the cost of being risk-averse. A risk-averse adversary will use an attack rate below $1 - \lambda$ and so, with probability $1 - \lambda - \mu$ there is no action from the attacker. Intuitively, no action means that the attacker will have a reduced success chance in breaking security. This can be quantified by the larger expected number of time steps to win for the first time. By defining the cost of being risk-avers as $RiskAverseCost = E^{(1)}_{\text{win}}(\mu, \lambda) - E^{(1)}_{\text{win}}(\mu = 1 - \lambda, \lambda)$ for a risk-averse adversary with probability of moving μ, we can graph the behaviour of this cost (penalty) as a function of $\lambda < 1 - \mu$.

Figure 5 shows that smaller μ (being more risk-averse) will have higher costs, and as μ increases, the cost decreases. However, as defender increases λ, the available attack rate of the attacker $(1 - \lambda)$ decreases and after a certain threshold value of λ, the cost of being risk-averse decreases and becomes 0 when $\lambda = 1 - \mu$.

6 CONCLUDING REMARKS

Using diversity and dynamicity property has been widely used in security systems [2, 4, 5, 8]. To our knowledge, our work is the first to use an MTD framework [3] in a post-quantum cryptographic setting. Our construction not only provides long term security in comparison with using a shared secret key to encrypt the communication with a secure symmetric encryption algorithm such as AES, that is considered quantum-safe, but allows ciphertexts to be stored and attacked offline.

Our approach can be seen as *coordinated* path hopping where the sender and receiver share a random source, and thus achieve a high communication rate. Uncoordinated path hopping was considered in [1] and communication protocols with information theoretic security were constructed. The communication rate of these constructions; however, is very low.

There are many open questions such as considering more complex set of actions for the players, and incorporating the cost and gain of actions to refine the model.

REFERENCES

[1] Hadi Ahmadi and Reihaneh Safavi-Naini. 2014. Multipath private communication: An information theoretic approach. *arXiv preprint arXiv:1401.3659* (2014).
[2] Richard Colbaugh and Kristin Glass. 2012. Predictability-oriented defense against adaptive adversaries. In *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. 2721–2727. https://doi.org/10.1109/ICSMC.2012.6378159
[3] Hoda Maleki, Saeed Valizadeh, William Koch, Azer Bestavros, and Marten van Dijk. 2016. *Markov Modeling of Moving Target Defense Games.* https://eprint.iacr.org/2016/741.pdff.
[4] Nicholas Nethercote and Julian Seward. 2007. Valgrind: A Framework for Heavy-weight Dynamic Binary Instrumentation. In *Proceedings of the 28th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI '07)*. ACM, New York, NY, USA, 89–100. https://doi.org/10.1145/1250734.1250746
[5] Hamed Okhravi, Thomas Hobson, David Bigelow, and William Streilein. 2014. Finding Focus in the Blur of Moving-Target Techniques. *IEEE Security Privacy* 12, 2 (Mar 2014), 16–26. https://doi.org/10.1109/MSP.2013.137
[6] Michael O. Rabin. 1990. The information dispersal algorithm and its applications. In *Sequences*. Springer, 406–419.
[7] Oded Regev. 2009. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)* 56, 6 (2009), 34.
[8] Kevin Scott and Jack Davidson. 2001. *Strata: A Software Dynamic Translation Infrastructure.* Technical Report. Charlottesville, VA, USA.
[9] Nick Statt. 1997. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* https://arxiv.org/abs/quant-ph/9508027.
[10] Xiangyun Zhou, Lingyang Song, and Yan Zhang. 2013. *Physical Layer Security in Wireless Communications.*