Formal Modeling and Analysis of Multi-Rogue Backoff Manipulation Attacks in Unlicensed Networks

Jordi Navarrette, Subash Shankar, Xiaojie Zhang, Saptarshi Debroy
City University of New York
Email: {*jnavarr, sshankar, xiaojie.zhang6, saptarshi.debroy*}@*hunter.cuny.edu*

***Abstract*—Security vulnerabilities that are unique to unlicensed (secondary) networks have been well studied in literature. However, the nature and impact of traditional wireless network threats, such as backoff manipulation when applied to secondary networks, require further investigation in particular for multiple rogue station scenarios. In this paper, we perform modeling and analysis of multi-rogue backoff manipulation attack strategies in secondary wireless networks using the PRISM probabilistic model checker. Our secondary network implementation in PRISM includes scenarios where: a) sub-band (channel) occupancy by licensed (primary) nodes follows an ON-OFF model with parameters derived from real measurement data and b) the secondary network consists of up to three rogue secondary stations out of eight total with all following CSMA/CA like contention process for channel access. Unlike honest secondary stations, the rogues carry out a backoff-manipulation strategy of selecting a backoff timer that deviates from the backoff-selection process mandated by the secondary network. Unlike simulation based analysis, our analysis using PRISM model checker considers all possible combinations of system parameters and *proves* that for any set of primary ON-OFF parameters and for any density of rogues in the network, a fixed backoff selection (instead of random) maximizes the channel access probability of a particular rogue irrespective of other rogues' selection strategy. The results from this work will help generate deeper understanding of medium access threat landscape of secondary networks and foster design of more resilient access control strategies.**

***Index Terms*—Formal methods, PRISM, backoff manipulation attacks, dynamic spectrum access, unlicensed users.**

I. Introduction

The spatial and temporal under-utilization of radio spectrum have motivated a paradigm shift from static towards dynamic spectrum management where unlicensed (secondary) networks comprising of non-license holding secondary users/stations can 'borrow' idle spectrum from the primary license holders (users) without causing harmful interference to the latter. Such secondary networks are required to continuously monitor the presence of primary users on licensed sub-bands (channels) and opportunistically access the unused or under-utilized sub-bands [1], [2]. As shown in Figure 1, this entire process comprises of four distinct but inter-dependent stages: a) channel sensing often using cognitive radios, b) channel availability decision making based on statistical models, c) available channel access by secondary users, and d) data transmission through accessed channel. As licensed channels are made available to the secondary users, they are expected to adhere to the regulations pertaining to all the stages of unlicensed access.

In most cases, the channel sensing, decision making, and channel usage are strictly regulated by Federal Communications Commission (FCC) with harsh consequences for anyone who violates them. However, regulations about channel access among secondary users in many cases fall under the purview of the secondary network administrator/controller with relaxed compliance requirements leading to regulatory constraints that are not always being strictly enforced. This is especially true for secondary networks that are distributed in nature, such as [3], [4]. This is due to the fact that in such use cases there is no central entity to oversee the channel access control process and thus the secondary users resort to contention based medium access control (MAC) protocols. This results in some rogue secondary users actively manipulating the channel MAC contention process for selfish and malicious purposes that can propagate to the entire network with cascading effects.

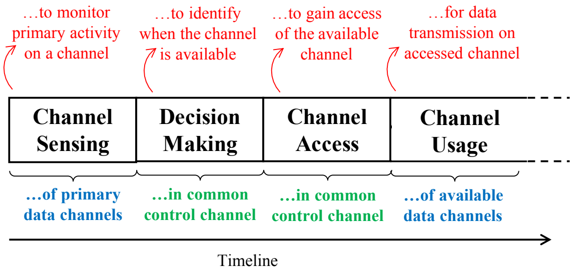
…to monitor primary activity on a channel
…to identify when the channel is available
…to gain access of the available channel
…for data transmission on accessed channel
Channel Sensing
Decision Making
Channel Access
Channel Usage
…of primary data channels
…in common control channel
…in common control channel
…of available data channels
Timeline

Fig. 1: Different stages of unlicensed secondary usage of licensed sub-bands/channels

One of the most prominent ways of gaining unfair advantage during contention is backoff manipulation attack. Backoff manipulation attacks are denial-of-service (DoS) attacks on wireless networks where rogue stations (users) choose a very small value for minimum contention window aiming to unfairly win the contention process and thereby monopolize channel access. Backoff manipulation attacks are also feasible in secondary networks where contending secondary users use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) based MAC protocol for channel contention. Although in the last decade many notable works [5], [6], [7] have studied generic wireless network-like backoff manipulation attacks, few have delved into modeling secondary network specific backoff manipulation attacks that maximize rogue user's channel access probability. At the same time, exploration and modeling of such attack behavior when multiple such rogue agents are present (in the network) also remain uncharted waters.

In this paper, we use the PRISM probabilistic model checker to compute the probability of channel access by rogue secondary stations when the primary user is not using the channel (i.e., the channel is in OFF state) in the presence of multiple rogue in the secondary network. The number of secondary stations range from four to eight, with the number of rogue secondaries ranging from zero to three. Rogues carry out a backoff manipulation strategy, deviating from the backoff selection process specified by the secondary CSMA/CA inspired contention based MAC protocol. Our results indicate that rogue behavior does improve the probability of success, with particular selections giving an overwhelming advantage. With two rogues, certain combinations in terms of backoff selection are shown to substantially reduce the probability of success for any honest secondary station in a network, while results for three rogues reinforce the optimality of such selection strategies observed in scenarios with fewer rogues. *Unlike simulation, our PRISM model checker implementation takes into account all possible unfoldings of the contention process, which is made possible both by utilities of the tool, and the modeling techniques applied.* Although the overall results corroborate with early works on backoff manipulation attacks, our unique formal methods based approach is able to *prove* that a fixed backoff selection rogue strategy leads to higher success even in multiple rogue scenarios.

The rest of the paper is organized as follows. Section II discusses the related work and motivation. Section III describes the PRISM implementation details. Section IV presents and discusses the results. Section V concludes the paper.

II. Related Work and Motivation

In this section we discuss the related work and motivation behind this work. First we discuss backoff manipulation attacks on IEEE 802.11 networks followed by the similar attacks in secondary networks. Finally, we discuss the applications of formal methods in network protocol verification.

Works such as [5], [6], [7], [8], [9] investigate backoff manipulation attacks in different types of wireless networks that are non-DSA. In [5], authors present backoff manipulation as one of the many ways of denying channel access to honest stations, whereas DOMINO [6] presents an analytical model of how such greedy behavior can be effectively detected with simulation results - both are considered seminal works on IEEE 802.11 networks. Works such as [7], [8], and [9] build upon DOMINO to design even more effective detection methods through statistical modeling and network deployed experiments. *However, no such works focus on modeling effective attack strategies for greater impact on the network. Most of the attack models used in such works are generic and may not prove very effective in a dynamic spectrum access setting. Furthermore, scenarios with multiple rogues and their effects are never explored, which is the focus of this paper.*

In recent years, notable works, such as [10], [11], [12], [13] explore the nature of backoff manipulation attacks in cognitive radio networks. In [10] authors propose a coordinated physical and MAC layer attack manifested through small backoff window selection. Authors use analysis and simulation to demonstrate the attack effects. Authors in [10] present a survey on security threats and detection techniques in cognitive radio networks where they discuss how generic wireless backoff manipulation attacks can be extended to secondary networks. Whereas in [12] and [13], authors propose DoS attacks called 'Off-sensing attacks' that affect the contention process among the secondary stations by manipulating their knowledge of licensed spectrum availability. Although it explores a derivative of backoff manipulation, the attack still exploits the inherent vulnerabilities of CSMA/CA contention process. *Overall, the scope of existing works towards backoff manipulation attacks in secondary network are limited in terms of optimizing attack strategy, as most of the works use analytical modeling with strong assumptions and thereby limit the real-world applicability. At the same time, almost all such works use Monte-Carlo simulations that only consider a limited number of scenarios with certain parameter combinations. Simulation is of course unable to provide guarantees, thus motivating our approach to use formal methods, and in particular model checking, to provide provable bounds over all possible executions.*

Although network protocol verification was one of the early driving forces behind model checking, the early projects involved verification of non-probabilistic systems (unlike the backoff manipulation attack) and effective probabilistic model checkers have appeared only over the last decade. One early work verifying similar probabilistic systems was by [14], who verified certain correctness properties of the CSMA/CA contention resolution protocol in IEEE 802.15.4 low-rate wireless personal area networks. Since then, there have been a few attempts to use formal methods to prove/analyze various properties of CSMA protocols. One such example is [15] who proved stability properties of wireless networked control systems' unslotted CSMA/CA protocol with 2-4 nodes. The only work that performs formal analysis of the backoff procedure CSMA/CA based MAC protocol in wireless sensor networks is performed in [16]. *However, we are not aware of any who have used formal methods for the backoff manipulation attacks in secondary networks that is our primary focus. Additionally, in the presence of multiple rogues (along with non-rogues) any realistic model must have enough nodes which leads to scalability challenges if meaningful results are to be expected. Our work presented here is thus guided by scalability concerns, both in terms of the underlying formalism and model abstractions.*

III. Approach

Our approach to this problem relies on model checking to formally model and prove properties of backoff manipulation attacks in a multi-rogue setting. The model checking approach to formal verification consists of codifying the behavior of a system as concurrent finite state machines (FSMs), and proving properties on all behaviors of the product machine resulting from their parallel composition [17]. FSM transitions may be deterministic or nondeterministic, with the latter allowing for states with several possible successors. Given a set of state machines, a model checker then constructs a representation (*i.e.*, the model) capturing all interleavings of the FSMs, and explores the model up to exhaustion for satisfaction, or violation, of specified properties. Specifications are given in a formal language distinct from the modeling language, which include not just the usual Boolean-valued operators, but others codifying temporal aspects, such as eventualities and the ordering of a sequence of events.

The primary problem with model checking is state space explosion, due largely to the exponential number of interleavings. One common approach alleviating state space explosion is the use of binary decision diagrams to represent model states and transitions *symbolically* instead of explicitly, which can in some cases expand the size of feasible models many orders of magnitude. Other notable optimizations and advancements have been developed, a particularly useful one to be discussed in Section III-A.

Typically, the investigator will produce a set of specifications for validating the correctness of the model — that is, to check that the system codified does exhibit the basic behavior intended, e.g. that state A always follows with state B, as is known to be the case. Thereafter, the model checker is run using specifications for verifying that desired behavior does occur, while undesired behavior does not.

A. Probabilistic Model Checking with PRISM

Probabilistic model checking is an extension of model checking where FSM transitions may be associated with probabilities, thereby facilitating the computation of, among many other related figures, probabilities for the satisfaction of specifications within a model. We use the most common probabilistic model checker, PRISM [18]. Its language for model description is based on the Reactive Models formalism [19], with support for numerous types of models: as with ordinary model checking, it permits both deterministic and nondeterministic behavior, while allowing for time to be modeled discretely and continuously, including with real-valued clock variables.

At the basic level, PRISM supports nonprobabilistic model checking of formulae in Linear Temporal and Computation Tree Logics (LTL and CTL, respectively). These logics are extended with the introduction of operators for computing (or verifying) probability (bounds), including for steady-state behavior of nonterminating processes. PRISM also provides a rewards mechanism that enables one to compute means for metrics on model behavior, while filters can be applied to restrict analyses to sets of states meeting user-defined criteria. PRISM also provides a powerful symmetry reduction option, which we exploit for multi-station scalability. Model components are organized into modules, which, once defined, can be used to instantiate other instances within the model. Given such a model, PRISM can exploit the symmetry among these modules to build a symbolic representation more efficiently, thus avoiding the exploration of equivalent traces. For our study, we chose discrete-time Markov chains (DTMCs), being the natural fit for slotted CSMA like protocols, while also exhibiting determinism, which greatly improves scalability.

B. Primary User Model

In our model, each primary user on a particular channel alternates between the ON and OFF state according to a 2-state Markov process.The activity process of primary user is expressed as a transition matrix:

$$\mathcal{P} = \begin{bmatrix} P_{ON \to ON} & P_{ON \to OFF} \\ P_{OFF \to ON} & P_{OFF \to OFF} \end{bmatrix}$$

For real values of transition probabilities, we use the data collected by RWTH Aachen Mobnets [20]. For our primary activity model, we use two TV primary sub-bands from the measurements dataset with the following center frequencies and ranges: 770 MHz (Range 20-1520 MHz) and 2250 MHz (1500-3000 MHz). Each measurement unit is a 6000×8192 matrix of primary (TV transmitters) power spectrum density (PSD) in dBm for 200KHz primary channel granularity. Figures 2(a) and 2(b) show PSD values of the two sub-bands for the entire time-sweep and their corresponding PSD thresholds (-107 dBm/200 kHz and -108 dBm/200 kHz) derived from their respective means. By comparing the PSD values with the threshold we determine the primary ON and OFF states in the bands. We then use the comparison results to estimate transition probabilities between ON and OFF states for the sub-bands. We denote $P_{i \to j}$ as the probability that a channel transits from state i to state j and apply well-known likelihood estimator for the transition probability [21] as:

$$P_{i \to j} = \frac{\#\text{transitions from state } i \text{ to state } j}{\#\text{number of } i \text{ states}}$$

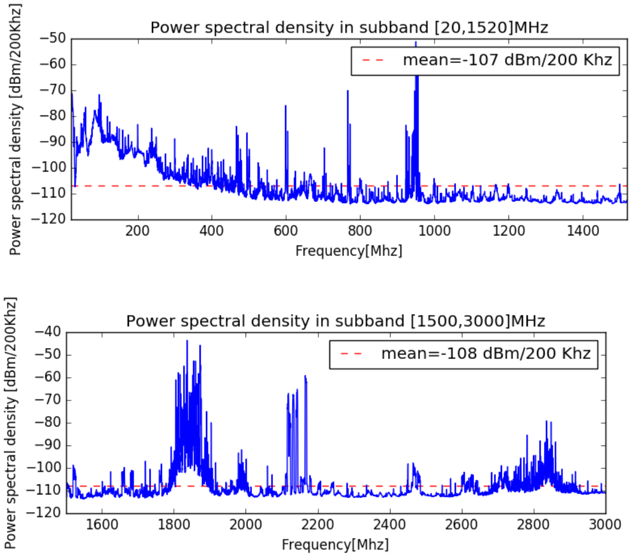

Fig. 2: RWTH Mobnets dataset power spectral densities in two primary sub-bands with respective thresholds

By applying this method, the primary ON and OFF transition probabilities for the two sub-bands used from our primary model are calculated as,

$$\mathcal{P}_{[20,1520]} = \begin{bmatrix} 0.9087 & 0.0913 \\ 0.0404 & 0.9596 \end{bmatrix}$$

$$\mathcal{P}_{[1500,3000]} = \begin{bmatrix} 0.8513 & 0.1487 \\ 0.0553 & 0.9447 \end{bmatrix}$$

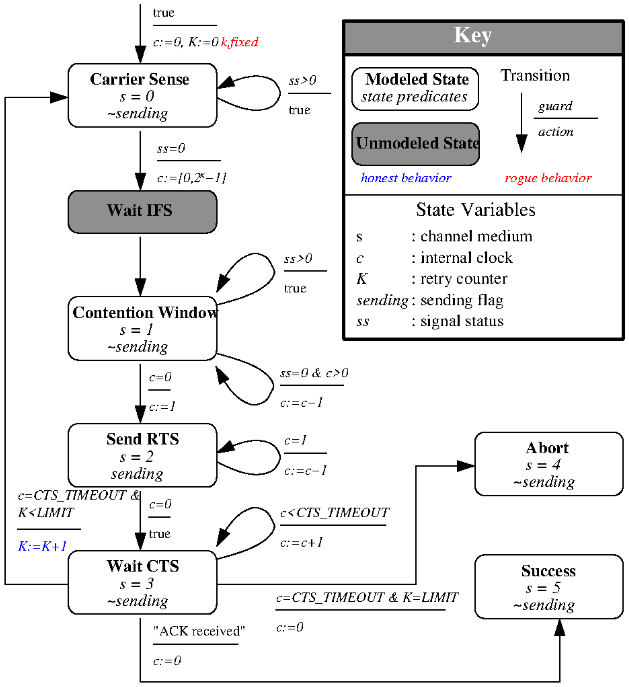

Fig. 3: The secondary rogue and non-rogue CSMA/CA based contention process

C. Secondary Contention Protocol

Figure 3 illustrates the finite state machine depicting our CSMA/CA like secondary contention protocol. In our model the secondary protocol is triggered by the primary going to the OFF state with all secondary stations (rogue and honest) contending to access the available channel. For the purpose of this work, several abstractions (from IEEE 802.11 CSMA/CA) were employed in order for the model to mimic contention process in notable secondary MAC protocols, such as [4], [22] and also for our computations to be tractable for larger numbers of stations. These abstractions occur both within the secondary station modules, and in their interaction through a shared medium with the primary station. To begin, we view the arrival of a clear-to-send (CTS) message as successful access of the channel by a secondary, and do not model the frame transmission. As soon as a secondary station reaches the success state, or all secondaries reach the abort state, the model reaches a sink state, halting any further progress.

Next, all interframe space (Wait IFS), such as DIFS and SIFS occurring are eliminated to reduce state space. Additionally, if a secondary station is on its last retry, and it is determined that the secondary will fail on this attempt, then that secondary immediately transitions into the abort state. This trims the state-space by a slight amount, while also allowing for probabilities computed regarding failure to accurately reflect that a station was on its way to abort, even though it would not have yet reached the designated abort state otherwise. These abstractions enable us to verify systems with up to eight stations, with the number of retries limited to three. While the number of retries in particular may seem rather low compared to the true retry limit of 15, later we will show that fairly definitive results can be derived with this value. A major source of state space explosion lies in selecting the random backoff value. Thus we model a different state machine that uses conditional probabilities to emulate this selection while producing completely equivalent behaviors. This avoids the associated state-space increase entirely, at the cost of some extra computation time.

Outside of the secondary station modules, the time for transmissions are parameterized by constant multipliers of time slots, each representing 51.2 μs. For our study, we establish the propagation time as amounting to one time slot, the roundtrip time as double that, and the CTS timeout as double the last. All behaviors within the protocol that are based on these parameters are defined in terms of them in the model. A single three-valued channel variable is used to capture the communication medium. Messages, and their propagation through the medium, are not themselves modeled. Instead, activity along the medium is captured through idle, low and high (abnormal) values — once the latter value is attained, any communication on the channel before inactivity is characterized as abnormal, indicating a garbled message. Our contention protocol does not model IEEE 802.11 CSMA/CA acknowledgements (ACK) from intended receivers to the contending stations, i.e., potential senders. Successful reception of an ACK is reflected by inactivity along the channel within one roundtrip-time of a request-to-send (RTS) message being transmitted. At any time step, the primary may probabilistically (not nondeterministically) issue an ON signal, causing all secondaries which have not yet aborted to reset, keeping their current value for number of retries.

Rogue secondary station modules occur as little modifications to those of honest secondary stations - they are given fixed values for their K (i.e., number of retries in Figure 3), which are parameterized in the model by constants. As such, rogue secondaries never reach an abort state, as their K values never change, and so never reach the limit. Nevertheless, they still choose random backoff values from 0 to $2^K - 1$ upon reaching the contention window, and wait the full CTS timeout before retrying. Our model is deterministic and follows discrete time steps. There is a single initial state, where the primary node is OFF and all secondary stations are in their carrier sense state (with $K = 0$ if not fixed). With nondeterminism, we could have any subset of the stations begin their communication attempts at any time step, in order to capture the dynamic nature of shared-medium communication. However, the results from PRISM would be returned as bounds for all possibilities, and given the wide range of different behaviors, we opted for precise probabilities for each possible scenario, over more comprehensive yet possibly wide-ranging bounds.

D. Specifications

For all models, we expect (and validated) the following behaviors, stated in English and PRISM's temporal logic specification language, where `P<=0 [spec]` checks that the probability of satisfying `spec` is (at most) 0:

- When the primary does turn on, all secondaries that have not aborted do reset. (That is, stop sending, return to carrier sense, and reset their internal clocks.)
  ```
  P<=0 [F (p=1 & (X (s1<5 & ... & sR<5 &
  ((0<s1 & s1<4)|...|(0<sR & sR<4))))))]
  ```
- Secondaries are only sending in their sending states. (That is, the sending variable is only on in the sending state.)
  ```
  P<=0 [F (sending1 & s1!=2)]
  ```
- Secondaries that have aborted or succeeded remain in that state.
  ```
  P<=0 [F (s1=4 & (F s1!=4))]
  P<=0 [F (s1=5 & (F s1!=5))]
  ```
- Only one secondary may succeed.
  ```
  P<=0 [F (s1=5 & (s2=5 | ... | sR=5))]
  P<=0 [F (sR=5 & (s1=5 | ...))]
  ```
- The channel only carries a signal when a secondary is sending.
  ```
  P<=0 [F (ss > 0 & !sending1 & ... &
  !sendingR)]
  P<=0 [F (ss = 0 & !s1=5 & ... & !sR=5 &
  (sending1 | ... | sendingR))]
  ```

Additionally, when there are rogue secondary stations, we expect that those modules never reach an abort state. [1]

Having established that these behaviors are captured by our model, we check the following probabilities, where `P=? [spec]` queries for the probability that `spec` is satisfied:

- The probability of success for any secondary in the model, and the same probability *without* any secondary aborting.
  ```
  P=?[F (s1=5 | ... | sR=5)]
  P=?[!(s1=4 | ...) U (s1=5 | ... |
  sR=5)]
  ```

[1] We also considered the property that there is eventual success whenever there is a rogue. When there are two rogues, this is not necessarily the case, as will be seen. However, when there is one rogue, PRISM will compute a 100% probability of eventual success for some secondary, even as the specification will *fail* when considered nonprobabilistically. The issue is that the primary, as mentioned, may turn on at any time step, thwarting any potentially successful sequence of states. However, the probability for the primary turning on and of staying on diminishes geometrically, so that the probability of no secondary ever reaching the success state shrinks to 0.

- For models with rogue secondaries, the probability of a rogue succeeding, as well as succeeding without another secondary aborting.

```
P=?[F (sR=5)]
P=?[!(s1=4 | ...) U sR=5]
```

The reason we computed those probabilities of success without aborts is as follows. It may occur that one station succeeds due to one or more of the other stations aborting. Given that our model is only tractable for a low retry limit, these aborts are effectively premature. Thus, any difference in the probability of success and success without an abort represents scenarios where an honest secondary could have still succeeded. We use this difference to give an upper bound for the true probability of success for an honest secondary, in the following way: since the behavior of the honest secondaries is symmetric, we may take this difference and distribute this equally to the probability of any honest secondary's success within the model. Similarly, the probability of success by a rogue without an abort gives a lower bound for the true probability of success by a rogue secondary.

As mentioned earlier, PRISM offers a reward mechanism, which can be used for computing means. Within each module, those transitions which occur with the passage of one time slot are labeled with the identifier "time". On one hand, this synchronizes the timed actions of all the modules. On the other, this is used to increment a reward for counting the number of time slots that have elapsed, and can be used to compute a mean for any certain (as in, 100% probable) event.

As it happens, symmetry reduction does *not* support the computation of rewards, and we observed discrepancies between the reported values for reduced and unreduced versions. However, by comparing the values from unreduced models to those generated with symmetry reduction, we were able to observe a useful pattern that allows us to gauge the extent of the error for those larger models that could not be approached without reduction.

IV. Results and Discussions

Our specifications validating model correctness passed with little to no time for models of all sizes. The following results took over 3000 computing hours on a workstation with a 4-core Xeon CPU (3.6-3.9 GHz) and 64GB RAM. The longest computation itself took over 520 hours – this is with the help of symmetry reduction, which in this most extreme case, reduced the sizes of the state space and number of transitions by factors of roughly 300 each. The first set of results presented use the primary ON-OFF model values of parameter set $\mathcal{P}_{[20,1520]}$ of the first sub-band.

A. No rogues

As seen in Table I, with no rogues, the probability of any secondary succeeding decreased gradually, from about 0.994 with four secondary stations, to about 0.976 with eight secondary stations. This probability can be divided among the symmetric honest secondaries to get their individual probability of success, which is very nearly the reciprocal of the number of secondaries. We note that the probability of success without any station aborting drops significantly, from 0.914 with four secondary stations, to 0.524 with eight secondary stations. This indicates that the probability of eventual success would be even higher, given a greater retry limit.

TABLE I: Probabilities of Success with No Rogues

No. of Secondaries	4	5	6	7	8
Eventual Success	0.9940	0.9921	0.9885	0.9834	0.9765
Without Abort	0.9139	0.8346	0.7295	0.6215	0.5238

B. One Rogue

With a single secondary rogue as shown in Table II, we can see the effectiveness of each fixed value for K across increasing numbers of stations. Keeping K at 0, which specifies immediately trying once inactivity is detected in the carrier sense state, is the poorest choice: not only is the probability of success relatively low (ranging from 0.327 to 0.466), but there is a significant difference from the corresponding probability without an abort occurring (growing from 0.015 to 0.17 with seven stations). This indicates that, given more retries, other secondaries may still succeed. While this rogue secondary is retrying immediately as described, it still leaves a window for other stations to succeed as it waits the CTS timeout.

TABLE II: Probabilities of Success with One Rogue

K	# Secondaries	4	5	6	7	8
0	Rogue succ.$\leq$	0.3273	0.4017	0.4449	0.4658	0.4746
	Rogue succ.$\geq$	0.3124	0.3439	0.3297	0.2937	
	Honest succ.$\leq$	0.2292	0.1640	0.1341	0.1177	
	Honest succ.$\geq$	0.2242	0.1496	0.1110	0.0890	0.0751
	Mean time	29.99	34.99	40.16	< 73.9	
1	Rogue succ.$\leq$	0.6742	0.6699	0.6745	0.6803	0.6857
	Rogue succ.$\geq$	0.6547	0.6316	0.6138	0.5980	
	Honest succ.$\leq$	0.1151	0.0921	0.0772	0.0670	
	Honest succ.$\geq$	0.1086	0.0825	0.0651	0.0533	0.0449
	Mean time	21.21	23.27	25.29	< 41.6	
2	Rogue succ.$\leq$	0.8754	0.8722	0.8707	0.8698	0.8692
	Rogue succ.$\geq$	0.8705	0.8632	0.8560	0.8492	
	Honest succ.$\leq$	0.0432	0.0342	0.0288	0.0251	
	Honest succ.$\geq$	0.0415	0.0319	0.0259	0.0217	0.0187
	Mean time	15.51	16.22	16.98	< 27.4	
3	Rogue succ.$\leq$	0.5631	0.5521	0.5484	0.5473	0.5471
	Rogue succ.$\geq$	0.5538	0.5338	0.5168	0.5014	
	Honest succ.$\leq$	0.1487	0.1166	0.0966	0.0831	
	Honest succ.$\geq$	0.1456	0.1120	0.0903	0.0755	0.0647
	Mean time	22.68	25.16	27.69	< 48.9	

The optimal value for K is observed as 2, with probabilities of success staying near 0.87 and decreasing slightly with increasing numbers of stations. The corresponding probabilities without aborts only differ by up to 2%, in the seven station model. This indicates that a value of 2 for K gives fairly dependable chances of success for the rogue. The values computed for the mean number of time slots further support this: it would seem that by choosing such a value, the rogue manages to avoid early collisions by other stations, while giving it short enough backoff times to acquire the channel.

C. Two Rogues

The analyses for two rogue scenarios are divided between situations where the rogues have the same value for K, and those where they have different values. In the latter case, we only examine scenarios where the values differ by 1 with fairly insightful results.

1) Same Value for K: In Table III we show that when both rogues have $K = 0$, neither one is able to succeed, and only honest rogues are able to acquire the channel — this occurs with probabilities decreasing from 0.935 to 0.819 as the total number of secondaries increases from four to eight. As the probability of success is not 1, no mean can be computed for the

TABLE III: Probabilities with Two Rogues, Same K

K	# Secondaries	4	5	6	7	8
0	Rogue succ. =	0.0000	0.0000	0.0000	0.0000	0.0000
	Honest succ. $\geq$	0.4676	0.3031	0.2196	0.1695	0.1364
1	Rogue succ. $\leq$	0.3977	0.3860	0.3829	0.3832	0.3851
	Rogue succ. $\geq$	0.3813	0.3607	0.3461	0.3351	
	Honest succ. $\leq$	0.1187	0.0929	0.0770	0.0660	
	Honest succ. $\geq$	0.1023	0.0760	0.0586	0.0467	0.0383
	Mean time	21.60	23.17	24.86	< 34.0	
2	Rogue succ. $\leq$	0.4261	0.4239	0.4247	0.4257	0.4264
	Rogue succ. $\geq$	0.4232	0.4170	0.4109	0.4041	
	Honest succ. $\leq$	0.0768	0.0553	0.0445	0.0384	
	Honest succ. $\geq$	0.0739	0.0507	0.0377	0.0297	0.0245
	Mean time	16.65	17.86	< 22.5	< 27.3	
3	Rogue succ. $\leq$	0.3786	0.3700	0.3674	0.3668	0.3666
	Rogue succ. $\geq$	0.3756	0.3631	0.3535	0.3443	
	Honest succ. $\leq$	0.1244	0.0913	0.0733	0.0623	
	Honest succ. $\geq$	0.1214	0.0867	0.0663	0.0533	0.0533
	Mean time	18.67	20.47	< 26.2	< 32.3	

TABLE IV: Probabilities with Two Rogues, Different K

K	# Secondaries	4	5	6	7	8
0	Rogue succ. $\leq$	0.0824	0.1000	0.1100	0.1155	0.1178
	Rogue succ. $\geq$	0.0782	0.0847	0.0791	0.0691	
1	Rogue succ. $\leq$	0.6811	0.6730	0.6806	0.6908	0.6995
	Rogue succ. $\geq$	0.6633	0.6326	0.6126	0.5959	
	Honest succ. $\leq$	0.1293	0.0942	0.0771	0.0670	
	Honest succ. $\geq$	0.1182	0.0757	0.0524	0.0388	0.0305
	Mean time	20.32	22.98	22.42	< 36.2	
1	Rogue succ. $\leq$	0.3335	0.3263	0.3246	0.3252	0.3267
	Rogue succ. $\geq$	0.3297	0.3175	0.3093	0.3031	
2	Rogue succ. $\leq$	0.6008	0.5998	0.5978	0.5955	0.5933
	Rogue succ. $\geq$	0.5977	0.5936	0.5874	0.5808	
	Honest succ. $\leq$	0.0363	0.0296	0.0258	0.0232	
	Honest succ. $\geq$	0.0328	0.0247	0.0194	0.0159	0.0133
	Mean time	15.28	15.98	< 19.2	< 22.6	
2	Rogue succ. $\leq$	0.6321	0.6366	0.6402	0.6422	0.6430
	Rogue succ. $\geq$	0.6298	0.6306	0.6278	0.6220	
3	Rogue succ. $\leq$	0.2305	0.2204	0.2163	0.2146	0.2138
	Rogue succ. $\geq$	0.2291	0.2168	0.2087	0.2023	
	Honest succ. $\leq$	0.0706	0.0509	0.0409	0.0351	
	Honest succ. $\geq$	0.0687	0.0476	0.0359	0.0286	0.0239
	Mean time	15.93	17.05	< 21.2	< 25.5	

number of time slots until success. It is evident from Table III that the best choice, again, occurs with $K = 2$, and we can even observe some non-monotonicity in the probabilities of success: they decrease slightly from 0.4261 (for each rogue) with four stations to 0.4239 with five stations, and then inch back up to 0.4264 with eight stations. This non-montonicity is also observed with $K = 1$, but with lower probabilities of success, while the probabilities of success were strictly decreasing, though slightly, as the number of stations increases when $K = 3$.

2) Different Values for K: With differing Ks, the possible combinations examined were with K set to 0 and 1, to 1 and 2, and to 2 and 3. In the first case, the rogue with $K = 0$ rogue starts off with a success probability lower than that of a rogue acting honestly when there are only four stations total, but steadily outperforms honest rogues as the number of stations increases. The rogue with $K = 1$ enjoys a success rate near 70% for all station counts. In the latter two cases, the station with $K = 2$ achieves success rates of about double that of with $K = 1$ and triple that of with $K = 3$ for all station counts. In the latter case, honest secondaries have success rates decreasing from 0.069 to 0.029 as the number of stations increase. In the former case, honest secondaries start with success rates of 0.033 to less than 0.015.

TABLE V: Probabilities of Success with Three Rogues

K	# Secondaries	5	6	7
1	Rogue succ. $\leq$	0.2373	0.2315	0.2305
	Rogue succ. $\geq$	0.2276	0.2106	0.1976
2	Rogue succ. $\leq$	0.3390	0.3347	0.3319
	Rogue succ. $\geq$	0.3320	0.3200	0.3090
	Honest succ. $\leq$	0.0542	0.0498	0.0461
	Honest succ. $\geq$	0.0423	0.0330	0.0264
	Mean time	19.34	< 22.9	< 26.9
1	Rogue succ. $\leq$	0.2848	0.2796	0.2793
	Rogue succ. $\geq$	0.2780	0.2643	0.2543
2	Rogue succ. $\leq$	0.4668	0.4666	0.4650
	Rogue succ. $\geq$	0.4615	0.4554	0.4472
3	Rogue succ. $\leq$	0.1712	0.1646	0.1612
	Rogue succ. $\geq$	0.1682	0.1581	0.1506
	Honest succ. $\leq$	0.0462	0.0407	0.0370
	Honest succ. $\geq$	0.0386	0.0297	0.0236
	Mean time	17.45	< 20.2	< 23.4
2	Rogue succ. $\leq$	0.2738	0.2698	0.2695
	Rogue succ. $\geq$	0.2657	0.2515	0.2390
	Honest succ. $\leq$	0.1015	0.0818	0.0708
	Honest succ. $\geq$	0.0893	0.0635	0.0479
	Mean time	21.25	< 25.9	< 31.2
2	Rogue succ. $\leq$	0.3462	0.3451	0.3459
	Rogue succ. $\geq$	0.3408	0.3321	0.3227
3	Rogue succ. $\leq$	0.1542	0.1458	0.1429
	Rogue succ. $\geq$	0.1506	0.1371	0.1274
	Honest succ. $\leq$	0.0839	0.0663	0.0568
	Honest succ. $\geq$	0.0767	0.0547	0.0414
	Mean time	19.14	< 22.9	< 27.2

D. Three Rogues

As shown in Table IV, the analysis for three rogue scenarios is performed for four situations, each having at least one rogue with $K = 2$: 1) one rogue has $K = 1$ and the other two have $K = 2$; 2) the rogues take different values of 1, 2, and 3; 3) all the rogues take the same value; and 4) one rogue has $K = 3$ and the other two have $K = 2$. These situations were chosen, as $K = 2$ was shown to lead to the highest probability of success, while $K = 0$ was shown to lead to very low probability of success in the presence of other rogues. Because the number of honest stations is lower, symmetry reduction was not as effective in reducing computational intensity, so data was only obtained for station count from 5 to 7.

Once again, it can be seen that rogues having $K = 2$ generally achieve higher probabilities of success. The slight caveat to this is when all rogues choose this value, in which case no single rogue can improve their probability of success by having their K set otherwise, and the probability of success is even lower than a rogue with $K = 1$ when the three rogues choose different values. At the same time, when all rogues choose $K = 2$, honest secondaries have a substantial bump in their probability of success, and we can see an increase in the mean time taken until some secondary station succeeds.

E. Second Primary Parameter Set

As mentioned earlier, all previous results were obtained using the first set of primary ON-OFF model parameters, i.e., $\mathcal{P}_{[20,1520]}$. When the second set of parameters (parameter set $\mathcal{P}_{[1500,3000]}$.) were used, probabilities of success generally decreased, but by amounts averaging less than 0.13%. In general, the higher probability of the primary switching ON led to slightly poorer performance by honest secondaries and rogues with $K = 2$, likely due to the higher incidence of would-be successful requests being abandoned due to a switch. Exceptions to this include when two rogues chose $K = 0$, in which case the performance of honest secondaries was slightly improved. Otherwise, no significant changes in behavior arise.

F. Summary of Results

With multiple rogues, we observed the highest probability of success for a rogue when there are two, with one rogue choosing $K = 0$, and the other, $K = 1$. This can be interpreted as an elementary coordinated backoff manipulation attack strategy, where the rogue with the lower value essentially disrupts the attempts made by other secondaries, allowing for the other rogue to acquire the channel. Following the trend as the number of stations increases, it would appear that this may not be as successful with a more realistic number of retries, as the probability of having an honest secondary abort (after only three retries) increases gradually.

This aside, superior outcomes generally occur when rogues participate with a strategy of K fixed at 2, and this holds across all numbers of rogues and stations studied. The advantage is substantial when no other rogues occur, or when they choose other fixed values for K. This suggests that the rogue(s) can benefit from avoiding earlier collisions by spending a modest amount of time in the contention window. This corroborates with the results from early works on backoff manipulation attacks on wireless networks that argued that smaller K values lead to higher rogue success. At the same time, our results *prove* that rogue strategies with $K = 2$ have higher success rate than other K values even when multiple rogues are present in the network trying to maximize individual channel access success probabilities.

V. Conclusions and Future Work

In this paper, using PRISM probabilistic model checker, we performed modeling and analysis of multi-rogue backoff manipulation attack strategies for multi-rogue setting. Using model parameters derived from real measurement data, our results prove (unlike simulation based analysis) that for any set of primary ON-OFF parameters and for any density of rogues in the network, a fixed backoff selection (instead of random) maximizes the channel access probability of a particular rogue irrespective of other rogues' selection strategy. The results from this work will help generate deeper understanding of medium access threat landscape of secondary networks and foster design of more resilient access control strategies.

In future, aside from exploring the current model with other combinations of fixed K, we aim to explore situations with more rogues. In this study, we set the value for the propagation time to 1 time slot, from which the values for roundtrip and CTS timeout follow. This can be altered to reflect different network topologies, although this will also diminish the scalability afforded by symmetry reduction. As mentioned, our current model also does not include the second backoff time waiting period, but it may be possible to model this without too much penalty, although this is not without its challenges. It is possible to apply a probability distribution to the initial state of a model. With some appropriate data, we will be able to more accurately model real-world behavior, though how this will affect the efficiency of computation cannot be immediately ascertained.

Applying the different types of models made available in PRISM, nondeterminism will be incorporated to permit secondaries to become active at any stage in the contention process. Probabilistic timed automata have also seen popular use in this area, and having real-time clocks will extend this investigation to unslotted CSMA/CA like contention process.

Finally, we plan on identifying and analyzing collaborative strategies that rogues may use to improve their success rates. At the same time, in the future we intend to explore the vulnerabilities of other non-contention based secondary MAC protocols applied in a small-cell setting and analyze attack strategies. The results from this work and future directions will help generate deeper understanding of medium access threat landscape of secondary networks and foster design of more resilient access control strategies.

References

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, S. Mohanty, "Next generation/-dynamic spectrum access/cognitive radio wireless networks: A survey," *Journal of Computer Network*, vol. 50, pp. 2127-2159, 2006.

[2] S. Debroy, S. Bhattacharjee, M. Chatterjee, "Spectrum Map and its application in Resource Management in Cognitive Radio Networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 1, no. 4, pp. 406-419, 2015.

[3] S. Bhattacharjee, S. Debroy, M. Chatterjee, "Quantifying Trust for Robust Spectrum Fusion in Distributed Multi-channel Cognitive Radio Networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 2, pp. 138-154, 2017.

[4] S. Debroy, S. De, M. Chatterjee, "Contention based Multi-channel MAC Protocol for Distributed Cognitive Radio Networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2749 - 2762, 2014.

[5] J. Bellardo, S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", *Proc. of USENIX Security*, 2003.

[6] M. Raya, J-P. Hubaux, I. Aad, "DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots", *Proc. of ACM MobiSys*, 2004.

[7] S. Radosavac, J. S. Baras, I. Koutsopoulos, "A framework for MAC protocol misbehavior detection in wireless networks", *Proc. of ACM WiSec*, 2005.

[8] A. A. Cardenas, S. Radosavac, J. S. Baras, "Evaluation of Detection Algorithms for MAC Layer Misbehavior: Theory and Experiments", *IEEE Transactions of Networking*, vol. 17, no. 2, April 2009.

[9] A. L. Toledo, X. Wang, "Robust Detection of MAC Layer Denial-of-Service Attacks in CSMA/CA Wireless Networks", *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, September 2008.

[10] W. Wang, Y. Sun, H. Li, Z. Han, "Cross-Layer Attack and Defense in Cognitive Radio Networks", *Proc. of IEEE Globecom*, 2010.

[11] A. G. Fragkiadakis, E. Z. Tragos, I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks", *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, First Quarter 2013.

[12] M. Hossain, J. Xie, "Off-sensing and Route Manipulation Attack: A Cross-Layer Attack in Cognitive Radio based Wireless Mesh Networks", *Proc. of IEEE INFOCOM*, 2018.

[13] M. Hossain, J. Xie, "Hide and Seek: A Defense Against Off-sensing Attack in Cognitive Radio Networks", *Proc. of IEEE INFOCOM*, 2019.

[14] M. Fruth, "Probabilistic Model Checking of Contention Resolution in the IEEE 802.15.4 Low-Rate Wireless Personal Area Network Protocol," *Proc. of ISoLA*, 2006.

[15] Bo Wu, Michael D. Lemmon, Hai Lin, "Formal Methods for Stability Analysis of Networked Control Systems With IEEE 802.15.4 Protocol," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 5, pp. 1635–1645, September 2018.

[16] H. Zayani, K. Barkaoui, R. Ben Ayed, "Probabilistic verification and evaluation of Backoff procedure of the WSN ECo-MAC protocol", *International Journal of Wireless & Mobile Networks*, vol. 2, no. 2, May 2010.

[17] E. M. Clarke, Orna Grumberg, Doron Peled, *Model Checking*, MIT Press, 1999.

[18] Marta Kwiatkowska, Gethin Norman, David Parker, "PRISM 4.0: Verification of Probabilistic Real-time Systems", *Proc. of CAV*, 2011.

[19] R. Alur, T. Henzinger, "Reactive Modules," *Formal Methods in System Design*, vol. 15, no. 1, pp. 77–48, 1999.

[20] RWTH Aachen University Static Spectrum Occupancy Measurement Campaign - https://download.mobnets.rwth-aachen.de/fileadmin/Documentation/Metadata.pdf

[21] S. Geirhofer, L. Tong, B. M. Sadler, "Dynamic spectrum access in WLAN channels: empirical model and its stochastic analysis," Proc. of TAPAS, 2006.

[22] S. Jha, U. Phuyal, M. Rashid, V. Bhargava, "Design of OMCMAC: An opportunistic multi-channel MAC with QoS provisioning for distributed cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3414 - 3425, October 2011.

[23] M. Kwiatkowska, G. Norman, D. Parker "Symmetry Reduction for Probabilistic Model Checking," *Proc. of CAV*, 2006.