THE SPREAD OF WI-FI ROUTER MALWARE REVISITED

Hamdi Kavak
Daniele Vernon-Bido

Modeling, Simulation, Visualization & Eng. Dept.
Old Dominion University
1300 Eng. & Comp. Sciences Bldg.
Norfolk, VA 23529, USA
{hkava001, dvern001}@odu.edu

Jose J. Padilla
Saikou Y. Diallo
Ross J. Gore

Virginia Modeling Analysis & Simulation Cent.
Old Dominion University
1030 University Boulevard
Suffolk, VA 23435, USA
{jpadilla, sdiallo, rgore}@odu.edu

ABSTRACT

A study by Hu et al. [2009, PNAS, 106(5)] projected that a targeted malicious attack on Wi-Fi routers could infect a region in two days. The study also argued that the use of WPA security protocol in 60-70% routers would practically prevent such epidemics. This paper revisits their model with current Wi-Fi router data from WiGLE.net and a refined data selection method. We examine the temporality and scale of the malware spread applying these two updates. Despite ≈88% WPA adoption rate, we see a rapid malware spread occurring in a week and infecting ≈34% of all insecure routers (≈5.4% of all) after two weeks. This result is significantly higher than the original study projection. It occurs due to the increased use of Wi-Fi routers causing a more tightly connected graph. We argue that this projected risk can increase when current vulnerabilities introduced and connected devices are considered. Ultimately, a thorough consideration is needed to assess cybersecurity risks in Wi-Fi ecosystem and evaluate interventions to stop epidemics.

Keywords: cyber security, malware epidemiology, agent-based simulation.

1 INTRODUCTION

Since its inception in the late 90s, Wi-Fi technology has been adopted by a wide range of products in the residential and commercial arena. Nowadays, almost any internet-capable device is shipped with Wi-Fi connection capabilities supporting the growth of Wi-Fi routers (Wi-Fi 2016). In the U.S. only, there were over nine million public Wi-Fi hotspots as of 2014 not counting residential and commercial private routers (iPass 2016). Due to this widespread adoption and the potential of compromising connected devices, Wi-Fi routers provide a target-rich environment for cyber criminals.

Attackers can directly gain control of Wi-Fi routers by exploiting misconfigurations of the device (Viehböck 2011) or flaws in wireless protocol (Sanatinia, Narain, and Noubir 2013). Alternatively, an attacker can setup a public trap Wi-Fi router and expect people to connect it for free internet (Li et al. 2016). Once a user is connected to a compromised or trap Wi-Fi router, the attacker can conduct several types of attacks such as man-in-the-middle attack, redirection to a malicious website to infect the user, or conduct denial-of-service attack using the infected Wi-Fi router (Tsow et al. 2016; Sanatinia, Narain, and Noubir 2013). In other words, security of Wi-Fi routers has implications beyond the device itself. In fact, a compromised Wi-Fi router can potentially attack nearby routers especially in densely populated areas and epidemic-like malware spread situation may occur (Milliken, Selis, and Marshall 2013).

SpringSim-CNS 2017, April 23-26, Virginia Beach, VA, USA; ©2017 Society for Modeling & Simulation International (SCS)

There is a growing body of literature investigating such malware spread scenarios. Hu et al. (2009), for instance, simulates the spread of a hypothetical Wi-Fi router malware using real-world router locations and security flaw rates. Utilizing a SIR (Susceptible-Infected-Recovered) model, they examine the spatiotemporal spread of the malware within selected urban areas in the U.S. Their results show that the rate of unsecure protocol usage and configuration in Wi-Fi routers play an important role in the spread of malware as well as the population density of cities (also reported by Milliken, Selis, and Marshall 2013). Sanatinia, Narain, and Noubir (2013) also investigate a Wi-Fi malware spread scenario for some neighborhoods in Boston, MA. Like Hu et al., they use a SIR model and real world Wi-Fi router data. However, Sanatinia et al.'s model differs from Hu et al. in terms of the consideration of vulnerabilities in Wi-Fi routers and protocols. Despite this fact, dynamics of their model are similar and their results follow a similar rapid spread of malware.

These studies expose a cybersecurity risk that is not investigated with current conditions. We aim to create a research initiative to investigate cybersecurity risks associated with Wi-Fi network ecosystem not only considering Wi-Fi routers but also mobile devices connected to them. Outcome from the research aims to address questions for government policy-makers with regards to Wi-Fi network ecosystem security. This is considered analogous to health officials making regulations and incentivizing about vaccination. In our case, the issue is not diseases but malwares and regulations would be the rules that enforce or suggest certain security measures to be adopted.

To address such an important initiative, we start by revisiting the malware spread model developed by Hue et al. (2009) with current Wi-Fi router data and a refined data selection method. We presently examine whether the time and scale of malware spread changes due to current conditions. As in Hue et al. (2009), our study uses publicly available data by WiGLE (www.wigle.net) and utilizes a SIR epidemiology model to simulate the propagation of malware through the Wi-Fi network. We consider the same weaknesses (e.g. default and poor password selection and wired equivalent privacy (WEP) flaws). We present details of our model in section 2 and provide results in section 3. We conclude with a discussion on the validity of our model and potential improvements for future work.

2 METHODS

Our approach can be summarized in three steps. *First*, we construct an agent-based simulation model based on Hu et al. (2009). Details of the original model, its interpretation for this revisit case, and simulation parameterization is reviewed in section 2.1. *Second*, we collect data from WiGLE for Wi-Fi router network construction. Details of this dataset and our refined data selection method are given in section 2.2. *Third*, we simulate the model with parameters provided in Hu et al. (2009) and report time and scale of malware epidemic in section 3.

2.1 Simulation Model

The SIR approach has originally been used to model the spread of epidemic diseases in both equation- and agent-based models (Connell, Dawson, and Skvortsov 2009). In this approach, each letter of SIR represents a health state called Susceptible, Infected, and Recovered respectively. In equation based models, each letter represents the fraction of the population belonging to those health states. In agent based models, an individual is considered in only one of these three health states and can transition to another based on the nature of disease. Such models are successfully used to assess health risks related to the speed and scale of epidemics. The same approach also has long been successfully applied in cybersecurity research to model the spread of malwares over a network of computers (Murray 1988). Hu et al. (2009) develop one of the first and comprehensive applications of the SIR model on the spread of a malware targeting Wi-Fi routers as explained in the following section.

2.1.1 Hu et al. model

The Hu et al. model has attributes and a behavior rule for router agents. In terms of attributes, each router is defined with *a health state*, *a password strength*, *an encryption usage*, and *location coordinates* (latitude and longitude). Health state is designated as I for the infected health state; S_{nopass}, S_{pass1}, S_{pass2}, and S_{WEP} for the susceptible health state; and R and R_{hidden} for the recovered health state. Additional health states is used to represent the variety of setting can be found in real world. For password strength attribute, four possible values are considered: *default*, *easy*, *hard*, and *unbreakable*. For encryption usage attribute, four values are considered: *none*, *WEP*, *WPA*, and *WPA2*. For the behavioral rule, routers with Infected (*I)* health state try to infect nearby reachable routers.

Initially, all Wi-Fi routers are assigned to one of four states: S_{nopass} (no encryption, default password), S_{pass1} (no encryption, user set password), S_{WEP} (WEP encryption), or R (WPA or WPA2 encryption) according to their real-world usages. A router can only transition to another health state when there is an attack by a nearby infected (I) router within R_{int} distance . Assuming there is an active attack, Figure 1 shows the health state transition dynamics described as follows:

- Routers with WPA or WPA2 encryption levels are considered immune to any attacks.
- Routers with health state S_{nopass} are directly infected after 5 minutes.
- S_{pass1} routers with a user set passwords are first attempted to be cracked using a small dictionary of ≈65,000 words that takes 6 to 15 minutes to infect. When this fails, the router transitions to health state S_{pass2}.
- Those routers health state S_{pass2} are attempted to be cracked using a large dictionary with approximately a million words that takes 400 to 1000 minutes to infect.
- When both small and large dictionary attacks fail for a router, it becomes immune and transition to R_{hidden} health state.
- Routers with health state S_{WEP} are first attacked to crack their encryption that is assumed to be successfully applied within 2,880 to 5,760 minutes. Once the WEP protection is cracked, the router assumed to be a non-encrypted router with a user set password.

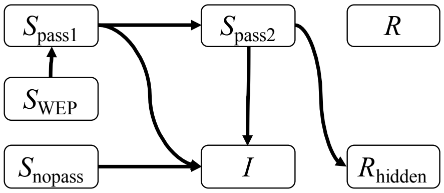


Figure 1: Health state transition dynamics (recreated from Hu et al. [2009]).

The numbers in these transitions rules are derived from related cyber security studies (Klein 1990; Yan et al. 2000; Bittau, Handley, and Lackey 2006) as noted by Hu et al. (2009). Besides the above transition rules, there are several assumptions pertaining to the attack process in general. First, when obtaining a list of reachable nearby routers, the model do not consider altitude. It means that routers in the same building can be considered closely located even though distance between them might be greater than R_{int}. Second, an infected router can only attack one router at a time therefore simultaneous attacks are not allowed. Third, an infected router keeps attacking the same router until it infects or fails. Fourth, an infected router attacks nearby routers with the lowest observable security level. In other words, routers with no encryption is assumed to be having the lowest observable security level compared to the ones with WEP encryption.

2.1.2 Our Interpretation of the Hu et al. Model

While the original model is described in detail, we come across sections that require further consideration. These considerations are related to choosing a method among alternatives and making additional assumptions that are not explicit in the original document.

For their model, Hu et al. provide two types of state transition methods: (1) probability-based and (2) time- and rule-based. The former method generates transition probability rates using empirical studies with regard to different attack types considered. For instance, transitioning from S_{WEP} to S_{pass1} is given as 0.001 for the average scenario. We do not consider this method because all probabilities need to be re-calculated when new vulnerabilities added to the model. The addition of new vulnerabilities in a future study is among expansions we aim to make. Therefore, we use the latter method that only requires the range of attack time length and rules that trigger these attacks.

We also make several assumptions in the attack process. We assume that when a router is under attack, no other router can attack the same router, inspired by the non-simultaneous attack assumption made in the original model. When a router fails to infect a nearby router, we make sure that the failed router is removed from the potential attack list. However, it is likely that same failed router could be attacked by another infected router because we do not assume a global coordination mechanism for the malware. For the same reason, we reset a router's health state to very first state when an attacker fails so other potential attackers could try infecting too. Lastly, when choosing a router with weakest security setting, we remove routers with health state R so we do not have to check them again later.

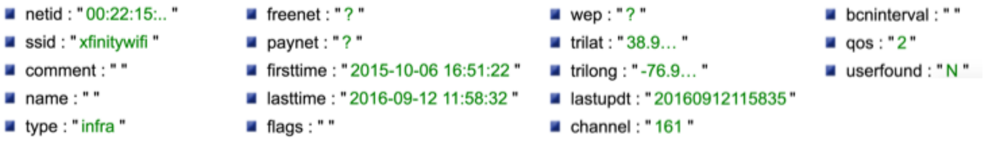
2.1.3 Simulation Parameters

As in model details, we make assumptions regarding initial parameters of the model.

- When distributing routers among S, I, and R classes, we easily follow Hu et al. Routers employing WPA or WPA2 encryption are assigned R health state while routers with WEP encryption assigned S_{WEP} health state. For unencrypted routers, we assign 50% of respective routers to each class of S_{nopass} and S_{pass1} as proposed by the original model.
- Password strength setting of routers is not as straightforward. The original model reports two conflicting methods for initializing non-encrypted routers. The assignment of 50% of non-encrypted routers to S_{nopass} would automatically require these router to have *default password strength* per definition of the health state. However, Hu et al. also mention that they use the fraction of routers keeping their default connection name (SSID) as a proxy for assigning routers a *default password strength*. As they do not elaborate nor mention anywhere in the annex, we do not consider this assumption in our initialization process and use the former one.
- We use the same analogy as Hu et al. when setting password strength for all routers except the ones with health state to S_{nopass}. 25% of these routers are assigned *easy password strength* that can be cracked using the small dictionary attack, additional 11% are assigned *hard password strength* that can be cracked using the large dictionary attack while remaining passwords are considered *unbreakable*.
- For the attacking process, router reception range R_{int} is an important factor determining the tightness of Wi-Fi router graph. The original paper evaluates distances ranging from 15 meters to 100 meters and use 45 meters in their report. Therefore, we also use R_{int}=45m in our model for comparability of the results.
- Lastly, we assume that attack time lengths in section 2.1.1. is uniformly distributed in given ranges.

2.2 Dataset

We use WiGLE (wigle.net) as our data source for Wi-Fi router locations and corresponding encryption usages. As of the report of our study, WiGLE contains over 304 million Wi-Fi router records worldwide from over 4 billion observations made by contributors. Mainly this data is collected through volunteer wardriving – collection of Wi-Fi device information using antennas in a moving vehicle (https://www.wardriving.com). Each Wi-Fi router in WiGLE is designated by several attributes (Figure 2) including latitude and longitude, which allows us to retrieve the data for a given area.



- netid : "00:22:15:.. "
- ssid : " xfinitywifi "
- comment : " "
- name : " "
- type : " infra "
- freenet : " ? "
- paynet : " ? "
- firsttime : " 2015-10-06 16:51:22 "
- lasttime : " 2016-09-12 11:58:32 "
- flags : " "
- wep : " ? "
- trilat : " 38.9… "
- trilong : " -76.9… "
- lastupdt : " 20160912115835 "
- channel : " 161 "
- bcninterval : " "
- qos : " 2 "
- userfound : " N "

Figure 2: An example WiGLE record.

To collect the WiGLE data, we used their official API by providing a rectangular frame that covers our target area, Washington D.C. We later identify the Wi-Fi router data that fall within the official boundary of Washington D.C. Initially, that corresponds to 759,750 records as of December 18, 2016. Like any other crowd-sourced effort, WiGLE data requires certain preprocessing and cleaning steps in order to improve the quality of the data. Hu et al. applies the following three steps to process the data.

1. Clear routers marked as 'probe' by WiGLE.
2. Limit number of router to 20 records for the same latitude and longitude location.
3. Redistribute routers in Φ degrees direction (Φ : Uniform[0, 2π]) and r meters (r : Uniform[0, R_{int}]) distance to eliminate strong street pattern in data locations.

In our case, we start with records that are entered since 2011 or updated after 2015. This is needed to eliminate potentially unused Wi-Fi router data because WiGLE goes back to the early 2000s. We eliminate 107,194 records (≈14.11%) and have 652,556 records before applying Hu et al.'s three-step data processing approach. Unlike Hu et al., we only find one probe network so we do not perform first step. We apply the second step and identify 405 latitude-longitude points reporting over 20 Wi-Fi routers (some points have more than 300 records). In this way, we eliminate 6360 records (≈0.97%). Lastly we apply the third step and redistribute router locations. As the final size, we identify 646,196 records as depicted in Figure 3.

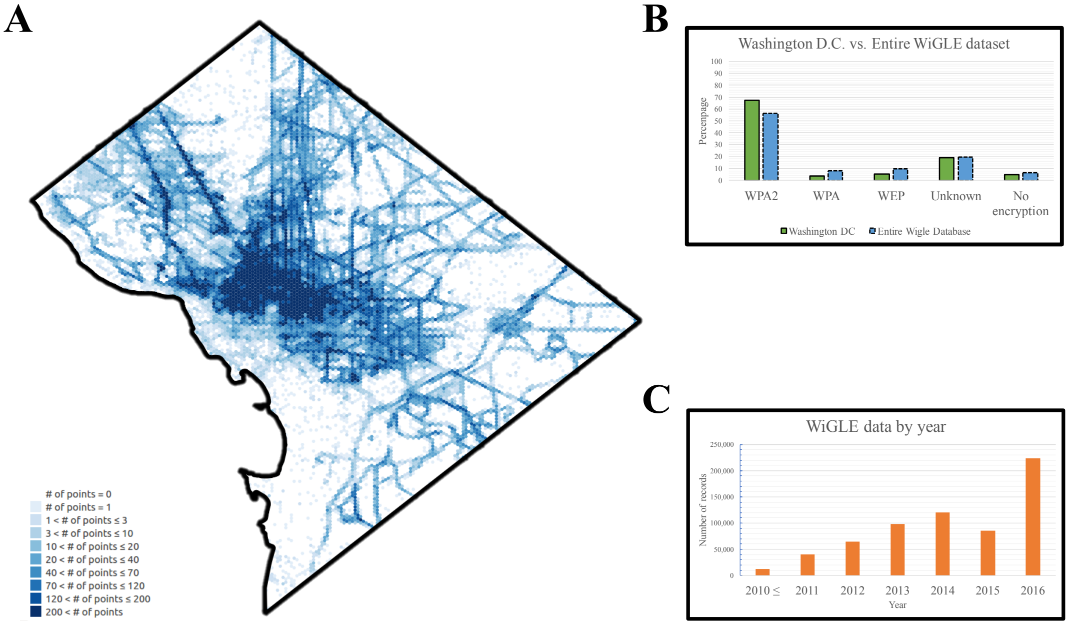


Figure 3: Three view of clean WiGLE dataset for Washington D.C. (A) Spatial density distribution. (B) Encryption usage percentages. (C) Number of data points by year.

Despite the redistribution of routers, there is still strong visual correlation with street patterns. This suggests using some alternative approaches to redistribute routers. When it comes to spatial density, the downtown area of Washington D.C. is very densely populated with Wi-Fi routers. This is expected as previous studies report similar spatial distributions. Regarding encryption usage, there is a high usage (over 67%) of WPA2 encryption method while there is still 3.8% to 5.1% usage of other methods. WPA-based encryption usage is at least doubled compared to Hu et al. (2009). ≈19% of records have an unknown encryption usage. The original model do not report how they handle records with unknown encryption usage. We identify two possible workarounds: ignore unknowns or reassign them an encryption usage based on known ones. Either way, we end up having a relative prevalence of ≈88% WPA or WPA2 encryption usage. According to Hu et al. (2009), our model should have an attack rate close to zero. Attack rate, according to Hu et al., is the fraction of infected routers (f_I) of all routers (N) but recovered ones (R), f_I / (N-R).

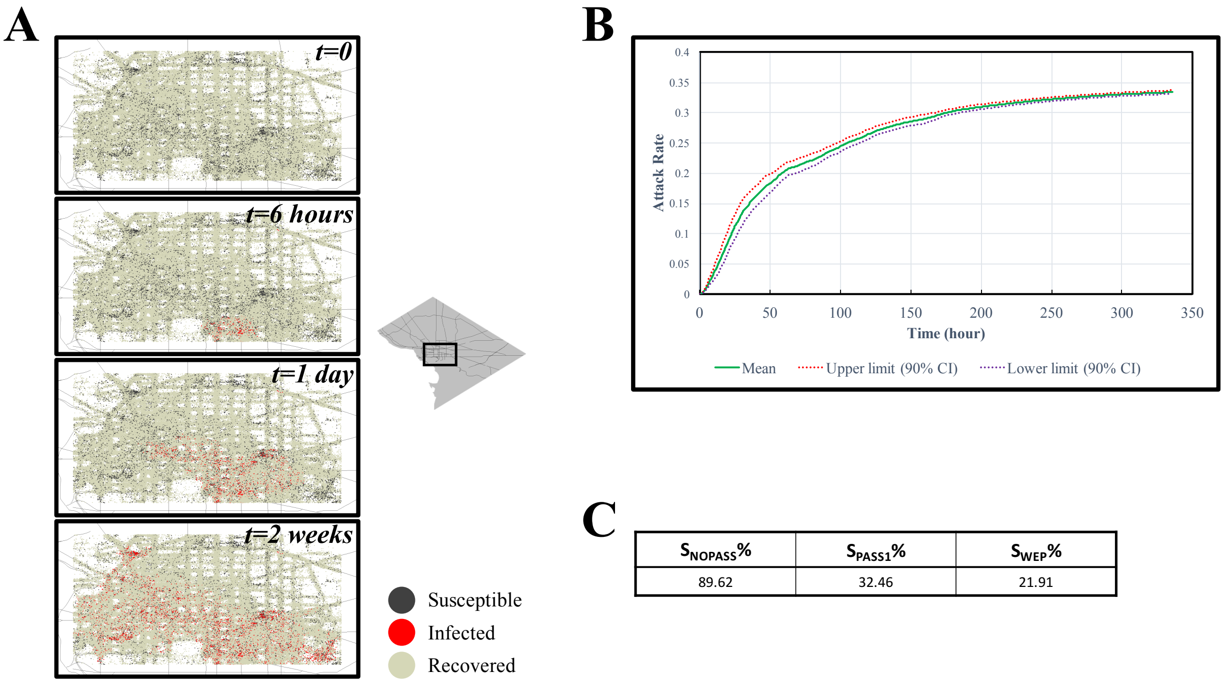
3 RESULTS

We setup our simulation model in MASON (Luke et al. 2005) using the attack lengths described in the original model (section 2.1.1.) and other parameters given in section 2.1.3. Hu et al. (2009) run their simulation model with a special subset of routers that are called 'giant network' – a network piece with largest number of nodes. They also report that such a network piece is mostly located in downtown areas of each cities. We visually identify a densely covered rectangular area in downtown Washington D.C. (between two latitude-longitude points 38.9198, -77.0125 and 38.8937, -77.0544) and consider this area as our 'giant network' piece.

Based on the wireless reception distance of R_{int}=45m, we generate a network with 225,421 nodes (83.88% WPA2, 4.15% WPA, 4.91% WEP and 7.06% non-encrypted), the average degree of 316.6, and the maximum degree of 1065 using five random redistribution of the original Wi-Fi router locations. Highest numbers recorded in Hu et al. (2009) were 50,084 nodes, average degree of 20.3, and maximum degree of 154 for Chicago, IL. Our network statistics are four to fifteen times higher than Hu et al.'s network statistics that can be related to two reasons. One potential reason is that Wi-Fi routers became more prevalent within the past eight years. This is a valid reason based on recent statistics (iPass 2016). Another potential reason could be related to the time filtering criteria we assumed even though we picked networks generated or updated in recent years. We discuss this criteria in the next section.

By using the above identified network of agents, we run the model with 10 replications, each lasting 4032 steps (5 minute/step) covering two weeks of a malware spread scenario. In order to propagate the spread, we infect 5 random Wi-Fi routers with health states S_{nopass} or S_{pass1}. Figure 4 illustrates some important results from the simulation runs. With regard to the spatial distribution of agents (Figure 4A), our results suggest a widespread distribution of malware especially among non-encrypted routers with default password. The first 48 hours represent an epidemic critical time. We see another spread (while slower) increasing the attack rate until the end of the first 160 hours (≈seventh day). Here the attack rate is the fraction of infected routers (f_I) of all routers (N) but recovered ones (R), f_I / (N-R). The second spread occurs mainly due to the infection of non-encrypted with non-default passwords and WEP-encrypted routers because it takes longer to infect these two types of routers.

After the seventh day, the attack rate gets stable with a trend suggesting a slight increase. This is the point where the epidemic is no longer as effective. Our results also suggest that (see Figure 4 C), almost all non-encrypted routers with default password are infected at the end of two-week period while about one third of non-encrypted routers with non-default password and a quarter of WEP-based ones are infected. Eventually we report an average attack rate of 33.44% at the end of two week period. It can be argued that the routers with WEP encryption would be infected with higher percentage due to the increased processing power that would shorten infection time. Since we use empirical values given in Hu et al., we will consider recent infection times in a future study.



S_{NOPASS}%	S_{PASS1}%	S_{WEP}%
89.62	32.46	21.91

Figure 4: Simulation results at a glance. (A) Snapshots from the spread of the malware at different points in time, taken from one simulation run. (B) A time series graph showing the attack rate using multiple simulation runs. (C) Final infection rates of different susceptible classes of agents as the average of multiple simulation runs.

We compare our results with Hu et al.'s for *the attack rate growth* (the malware progression depicted in Figure 4B) and *final attack rate projection based on encryption adoption*. (1) In terms of the attack rate growth, our results resemble Seattle, Boston, Chicago and Indiana results with a rapid then slightly slower growth occurring in the first seven days and very slow growth in the remaining seven days. While there is a slight difference in attack rate growth number with these cities, their final attack rate reaches ≈34% matching with ours. (2) In terms of final attack rate projections, however, our results differ from the original study. In the original study, Hu et al. examined how different rate of secure encryption use would change the final attack rate. According to this examination, Hu et al. projects less than one percent final attack rate when secure encryption usage is over 80%. In our case, secure encryption use is almost 88%; however, our model predicts ≈34% final attack rate. This difference occurs because number of nodes in our network of routers is more than four times higher and the average degree is approximately fifteen times higher than Hu et al.'s. Therefore, this tightly connected larger network we gathered allows a malware to spread despite the increased usage of secure protocols. It is important to note here that the attack rate metric introduced by Hu et al. puts emphasis on unsecure networks so our projections are comparable to all cities in Hue et al. except New York City (≈54% attack rate). It would be more appropriate for our case to define a metric to reflect both secure and unsecure Wi-Fi networks. Simply, we can define such a global attack rate metric as the fraction of infected routers among all Wi-Fi routers (f_I/N). In this case, our average global attack rate would be calculated ≈5.4%. We also calculate the global attack rate for Hu et al.'s model and get the rate of 24% as an average of all cities. This metric reflects the spatial epidemic seen in our model (Figure 4A).

4 DISCUSSION AND CONCLUSION

In this paper, we revisited the Wi-Fi malware epidemiology model by Hu et al. (2009) with current Wi-Fi usage data from WiGLE and a refined data selection method. Our model generated a tightly connected network which was not present at the same scale in the original study. Average degree distribution, for instance, is more than fifteen times higher than the original study. As a result, despite the prevalence of secure encryption usage, our model predicts a relatively rapid epidemic occurring in seven days that eventually infects almost one third of the insecure Wi-Fi routers in two weeks. This unexpected result can be discussed in terms of three aspects that shed light into future studies.

- First, it is observed that model predictions depend on the number of Wi-Fi routers and their density forming tight/sparse network. In this study, we introduced a time filtering method that select routers added since 2011 or updated since 2015 to get currently active Wi-Fi routers in the area. If we had chosen a more conservative assumption of considering routers added since 2014 instead of 2011, we would have ≈24% less nodes. We do not calculate other network statistics but it is worth investigating the influence of different time filtering values. Apart from the time filtering approach, one can develop an algorithm that takes into account of spatially nearby records and street patterns to find most recently active routers. Having a street map of the area, this process would include (1) assigning each data point (or group of points added at the same time) a streets edge, (2) finding the last time that street edge is updated, and (3) eliminating records that are outdated. Ultimately, both methods need to be tested by acquiring a ground truth dataset and triangulating it with WiGLE. This might be costly as it requires personal data collection.
- Second, we argue that Hu et al. could not predict current spread because their model is only tested with the data collected at the time of their study. In other words, their model do not project the growth of Wi-Fi usage that may happen in future months and years. When we address the first point, we could gather representative WiGLE data at different points in time (e.g., 2015, 2014 etc.). Based on these data points and their spatiotemporal growth rate, we can develop a projection model that can be used for policy-making.
- Third, we suggest an update to the original model due to time passed since then. First area of updates are to the epidemic model portion. A current model needs to account for current vulnerabilities. Two present current vulnerabilities are (1) the weaknesses in WPA encryption key handling mechanism that allows an attacker to crack the protocol and (2) the flaw in the Wi-Fi Protected Setup (WPS) mechanism present in current routers. Sanatinia, Narain, and Noubir (2013) partly address this vulnerability but their model is only tested in a small area. Further, we need to update the original model in term of times needed to perform certain attacks. This is especially important to project epidemic spread speed properly. Second area of updates to the original model is in the processing of WiGLE data. In addition to finding a reliable router data selection mechanism (as discussed earlier), we need an algorithm that could be used to redistribute the location of Wi-Fi routers because visual inspection of redistributed data Based on Hu et al. shows that we still have majority of routers located on the streets. We propose that the assignment of routers to nearby building footprints would make routers originate within buildings, not on the roads. This can help creating a more realistic Wi-Fi network. Further, the assumption of all non-encrypted Wi-Fi routers are insecure is a bold assumption as Sanatinia, Narain, and Noubir (2013) reports that half of non-encrypted Wi-Fi routers in their study area belong to institutions that have secondary password protection mechanisms. Dismissing this fact might exaggerate the scale of the epidemic. Lastly, the original study assumes that more than 20 Wi-Fi routers at the same location is not realistic thus limit them to 20. While it might be a justifiable case at the time of their study, there is a need to re-identify this number based on current use of Wi-Fi technology. We note that this number could even vary by the location where urban areas would have higher number while rural areas would have lower.

In addition to the points discussed above, the spread of Wi-Fi router malware is still a fertile area for new models. Current studies either consider just devices (Sarat, and Terzis 2007; Wang et al. 2009) or Wi-Fi router networks (Hu et al. 2009; Sanatinia, Narain, and Noubir 2013). We identified no Wi-Fi malware spread model considering the devices (e.g., mobile devices) connected to Wi-Fi routers. It is our hypothesis that the inclusion of mobile devices such as smartphones can act as catalyst for malware spread. Vulnerabilities in smart phones, for instance, can facilitate an increased attack surface as individuals travel and connect to different Wi-Fi routers. Ultimately, such models can be realized using human mobility as a proxy for mobile device movements.

NOTES

Supplemental material is available on GitHub at https://github.com/hamdikavak/wi-fi-malware-spread-revisited

ACKNOWLEDGMENTS

This material is based on research sponsored by the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)) under agreement number FAB750-15-2-0120. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

We thank Wigle.net for providing increased API usage limits to access the data.

DISCLAIMER

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)) or the U.S. Government.

REFERENCES

Bittau, Andrea, Mark Handley, and Joshua Lackey. 2006. "The Final Nail in WEP's Coffin." In *Proceedings - IEEE Symposium on Security and Privacy*, 2006:386–400. doi:10.1109/SP.2006.40.

Connell, Russell, Peter Dawson, and Alex Skvortsov. 2009. "Comparison of an Agent-Based Model of Disease Propagation with the Generalised SIR Epidemic Model." *Defense Science and Technology Organisation*. Vol. DSTO-TR-23. http://handle.dtic.mil/100.2/ADA510899.

Hu, Hao, Steven Myers, Vittoria Colizza, and Alessandro Vespignani. 2009. "WiFi Networks and Malware Epidemiology." *Proceedings of the National Academy of Sciences of the United States of America*. 106 (5): 1318–23. doi:10.1073/pnas.0811973106.

iPass 2016. "Wi-Fi Growth Map". http://www.ipass.com/wifi-growth-map/index.html. Accessed Dec. 19, 2016.

Klein, Daniel V. 1990. "Foiling the Cracker: A Survey Of, and Improvements To, Password Security." *Proceedings of the 2nd USENIX Security Workshop*, 5–14.

Li, Mengyuan, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu, and Na Ruan. 2016. "When CSI Meets Public WiFi: Inferring Your Mobile Phone Password via WiFi Signals." In *23rd ACM Conference on Computer and Communications Security*, 1068–79. Vienna, Austria. doi:10.1145/2976749.2978397.

Luke, Sean, Claudio Cioffi-Revilla, Liviu Panait, Keith Sullivan, and Gapriel Balan. 2005. "MASON: A Multiagent Simulation Environment." *Simulation* 81: 517–27. doi:10.1177/0037549705058073.

Milliken, Jonny, Valerio Selis, and Alan Marshall. 2013. "Detection and Analysis of the Chameleon WiFi Access Point Virus." *EURASIP Journal on Information Security* 2013 (1): 2. doi:10.1186/1687-417X-2013-2.

Murray, W. H. 1988. "The Application of Epidemiology to Computer Viruses." *Computers and Security* 7 (2): 139–45. doi:10.1016/0167-4048(88)90327-6.

Sanatinia, Amirali, Sashank Narain, and Guevara Noubir. 2013. "Wireless Spreading of WiFi APs Infections Using WPS Flaws: An Epidemiological and Experimental Study." *2013 IEEE Conference on Communications and Network Security, CNS 2013* 2011: 430–37. doi:10.1109/CNS.2013.6682757.

Sarat, Sandeep, and Andreas Terzis. 2007. "On Using Mobility to Propagate Malware." In *5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*. IEEE. doi:10.1109/WIOPT.2007.4480052.

Tsow, Alex, Markus Jakobsson, Liu Yang, and Susanne Wetzel. 2006. "Warkitting: The Drive-by Subversion of Wireless Home Routers." *Journal of Digital Forensic Practice* 1 (3): 179–92. doi:10.1080/15567280600995832.

Viehböck, S., 2011. Wi-Fi protected setup pin brute force vulnerability. *CERT Vulnerability Note VU*, *723755*.

Wang, Pu, Marta C González, César A Hidalgo, and Albert-lászló Barabási. 2009. "Understanding the Spreading Patterns of Mobile Phone Viruses." *Science* 324 (5930): 1071–76.

Wi-Fi 2016. "Wi-Fi Alliance History". http://www.wi-fi.org/who-we-are/history. Accessed Dec. 19, 2016.

Yan, Jianxin, Alan Blackwell, Ross Anderson, and Alasdair Grant. 2000. "The Memorability and Security of Passwords – Some Empirical Results." *Technical Report-University Of Cambridge Computer Laboratory*, 1–11. doi:10.1109/MSP.2004.81.

AUTHOR BIOGRAPHIES

HAMDI KAVAK is a Ph.D. candidate in the Modeling, Simulation, and Visualization Engineering Department at Old Dominion University (ODU). He received his master's degree in Modeling and Simulation from ODU. His research focuses on data-driven agent-based simulations with an emphasis on human mobility and cyber security. His email address is hkava001@odu.edu.

JOSE J. PADILLA is Research Assistant Professor at VMASC at Old Dominion University. He is the lead of the Human Dynamics Lab at the Center. His research focuses on the understanding and modeling of problem situations. Ongoing research focuses on methodological development for M&S of human behavior using social media data and agents; simulating users, insider threats and hackers for cybersecurity; and designing and developing platforms for simulation development and data capture. His email address is jpadilla@odu.edu.

DANIELE VERNON-BIDO is a Ph.D. candidate at the Virginia Modeling Analysis and Simulation Center at Old Dominion University. She received her B.S. in Computer Science (1987) from Brooklyn College, her M.S. in Computer Information Systems from Boston University (Brussels, Belgium) and her M.S. in Modeling and Simulation (2013) from ODU. Her email address is dvern001@odu.edu.

SAIKOU Y. DIALLO is a Research Associate Professor at the Virginia Modeling, Analysis and Simulation Center (VMASC) of the Old Dominion University (ODU). He received his M.S. in Modeling and Simulation (2006) and his Ph.D. in Modeling and Simulation (2010) from ODU. His research focuses on the theory of interoperability as it relates to model-based data engineering and web services for M&S applications. He is currently the co-chair of the Coalition Battle Management Language drafting group, an M&S IEEE standard development group. His email address is sdiallo@odu.edu.

ROSS J. GORE is a research assistant professor at the Virginia Modeling, Analysis and Simulation Center of Old Dominion University. He holds a doctorate of philosophy (Ph.D.) and a master's degree in computer science from the University of Virginia and a bachelor's degree in computer science from the University of Richmond. His research focuses on verification and validation as well as the mining of public data sources to inform models and simulations. His email address is rgore@odu.edu.