KASU JOURNAL OF MATHEMATICAL SCIENCES (KJMS) VOL. 2, ISSUE 2, December 2021
ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms

KASU JOURNAL OF MATHEMATICAL SCIENCES

Epidemic Based Modelling For the Mitigation of IoT Botnet Propagation at Equilibrium Point

Mohammed Ibrahim

Department of Computer Science, Kaduna State University

E-mail: mohammed.ibrahim@kasu.edu.ng

Abstract

In mitigating Internet of Things (IoT) botnet propagation, infected nodes are recovered via vaccination or patching,however, recovered nodes are liable to the same malware reinfections since bots often tide with the new exploits. Hence, in the absence of effective vaccines or treatment, it is realistic to mitigate IoT botnet propagation using an epidemic modelling approach. While current mitigation models in IoT botnets propagation do not take into account the efficiency of the of the infected nodes, In this paper, an epidemic based model (Infectious-Abandoned-Forensic (IoT-SIAF)) model is proposed. IoT-SIAF is a model inspired by the epidemic models to select or abandon infected nodes in mitigating botnet propagation. In addition to other influential factors, the IoT-SIAF model takes into consideration the memory availability of the infected nodes to determine its suitability for classification as an object of forensic interest. Furthermore, we demonstrate the capability of the IoT-SIAF model in mitigating at botnet equilibrium points.

Keywords: Abandon, Bots, Forensic, Infections, IoT, IoT-SIAF, Memory, Mitigation, Nodes, Propagation.

1. Introduction

The issues of IoT botnets threats and its emergence in the late 2016s have justified the need, for not only studying its mode of propagation but how to mitigates and establish facts from its attack surface. Mirai as publicly and popularly known botnet in the late 2016s has deceived more than 600,000 IoT devices to spread itself and cause a series of large-scale DDoS Attacks (Antonakakis et al., 2017). IoT botnets like Mirai execute infection through an attacker or botmaster (controller) not the bot itself, the infected bot is just an IoT device that is running a bot program and prepares to receive various commands, analyze and execute the attack in addition to the information gathered about the target nodes (Ji et al., 2018). Such infected bots can similarly be used to further propagate a malware attack to its nearby network and/or other internet nodes (Koroniotis,et al., 2019). Hence, with such a destructive attack on the increase, it is clear that security and forensics of the IoT infrastructure should become a priority for research (Koroniotis,et al., 2019). Also, Mirai botnet targeted camera with weak password vulnerabilities written in their read only memory

(ROM) and can not be cleared once infected (Ji et al., 2018). Besides, Mirai uses worm-based propagation techniques (Acarali, et al., 2019) to transmits attacks to the neighboring nodes. However, with consideration to IoT wireless sensor-based network, worm-attacks exploiting memory-related vulnerabilities can compromise the entire network without breaking protocols (Gu and Noorani, 2008). Also, with the diversity of sensor nodes architecture for program and data storage (Gu and Noorani, 2008), taking von Neumann sensor nodes architecture as a basis of our research. Von Neumann sensor node architecture considered both the instruction and data to be stored in the same memory space. Consequently, this will enable the attacker to transfer execution control where the mal-packet is being stored. In addition to the processing of the attacker's instruction, the bot memory can be exploited to scan information about the target nodes for onward propagation of the attack. Hence, isolating memory efficient bots and subjecting them to forensic analysis can not only provide data for forensic analysis but can similarly mitigate the propagation of the attack. On the other hand, Users, botnet controllers, IT Service providers, and law enforcement are part of the entity relationship in dealing with IoT botnet attacks (Gardner et al., 2017). The role of IT service providers is to provide forensic services to law enforcement, as such there is a need to identify and isolate the object of forensic interest (OOFI) during the mitigation of IoT botnet attack. However direct access to OOFI within the IoT domain may not always be possible (Mac Dermott et al., 2018).This is due to the challenges regarding the traces present on the physical devices during an attack, while traces were obtained from the device, these traces are either limited themselves to configuration settings or had limited persistence, mainly due to the limited storage availability (Servida and Casey., 2019). Also, the limited storage capability of the IoT devices will limit their ability to track and store detailed logs of their activity for forensic analysis (Alur et al., 2016).

In this complex situation, since it is difficult to isolate the object of forensic interest, the option of identifying and considering the next best thing (source of relevant evidence) may have to be taken (Oriwoh et al., 2013) . However, to the best of our knowledge, such a strategy to identify and isolate the next best thing in mitigating IoT botnet propagation has not been previously considered. Hence, in this paper, we are to consider memory efficient bots as the next best things since their capable of storing attacker's instructions as well as traces of information about the target nodes. Although there are existing models in studying IoT botnet propagation, few models (Gardner et al., 2017) and (Jerkins et al., 2018) are directed towards the mitigation of the menace. These models do consider intervention parameters such as user awareness and nodes immunization without consideration to the isolation of memory-efficient bots in mitigating the attack.

In this regard, based on Von Neumann's sensor node architecture, memory efficiency determines the amount of information a host sensor can hold, as such memory-efficient bots can hold significant information about target nodes for onward propagation of the attack. While studying IoT botnet propagation, (Yin et al., 2019) considered an interesting phenomenon of which the probability of computer infection increases as a result of the host computer receives several

disguised emails with viruses. This indicates the memory effect, and based on the memory effect of a node, a non-redundant memory features in IoT global botnet propagation process was introduced (Yin et al., 2019).

Also, to propagate the botnet attacks to the neighboring nodes, the infected nodes(bots) scan and forward information about the vulnerable nodes to the attacker or controller. This information includes the device IP address, port, username, and password (Ji et al., 2018). The attacker and the loader server implement the infection based on the information scanned by the bot (Ji et al., 2018). Hence, considering the amount of information stored in the bot memory, memory of the infected nodes will be attractive particularly for the mitigation and forensic analysis of IoT botnet attack.

Therefore, the objective of this paper is to develop an epidemic based model that can isolate memory-efficient bots as a strategy for the mitigation of IoT botnet propagation. Consequently, it will limit the attack propagation. The paper overview previous model on IoT botnet propagation, in section II, the proposed model is presented in section III, simulation results are presented in section in IV and finally conclusion is presented in section V.

2. Previous Models on IoT Botnet Propagation

With their modes of propagation similar to the spreading of infectious diseases. Various epidemic models were modified to represent the dynamic propagation of computer viruses, worms in wireless sensor network (WSN) and botnet propagation in IoT infrastructure. While many models (Mishra and Keshri, 2013), (Feng et al., 2015), (Khanh et al., 2016), (Wanget al., 2017), (Singh al., 2018)) concentrated on Worm propagation, (Ji et al., 2018), (Jerkins et al., 2018), (Acarali,et al., 2019) and (Gardner et al., 2017), (Farooq and Zhu, 2019) directed their work on dynamic propagation of IoT botnet, except (Farooq and Zhu, 2019) and (Jerkins et al., 2018) that considered the mitigation of the botnet propagation. With (Farooq and Zhu, 2019) proposing a device patching to prevent the botnet formation, (Jerkins et al., 2018) uses the techniques of inoculation epidemic to mitigate the propagation of the attack. Inoculation epidemic enhances the IoT population's resistance to malware and mitigates the damage from a harmful epidemic. This is achieved by developing an active acquired immunity in the susceptible population of IoT nodes (Jerkins et al., 2018).

To describe the effectiveness of the inoculation, an epidemic based model derived from the traditional Susceptible Infectious-Susceptible (SIS) model is used to incorporate a separate population of IoT devices. The separated IoT devices can be infected with the "harmless" virus and as such cannot be infected with the "harmful" virus. Hence, based on this technique, a model was proposed called a Susceptible infected/non-vulnerable-susceptible(SI/NS) (Jerkins et al., 2018). By analyzing the parameter of the model, the basic reproduction number R_o was obtained

to determine the expected number of secondary infections that result when an infected node is introduced into the susceptible population (Jerkins et al., 2018). R_o determine if an infection will die out or persist within the susceptible class of an IoT network. If $R_o < 1$, the infection will dies out, otherwise if $R_o > 1$, the infection will persist within IoT infrastructure.

The SI/NS model is dynamically represent using a system
of differential equations (1) below.

$$S = -\alpha SI - \gamma SN + \beta I + \delta N$$

$$I^{\cdot} = \alpha SI - \beta I$$
$$N = \gamma SN - \delta N \quad (1)$$

based on the stability analysis of the model, the basic reproduction number is obtained as

$$R_o = \alpha\delta/\gamma\beta$$

where
$\alpha =$ is the occurrence of new harmful infection
$\gamma =$ is the occurrence of new harmless infection
$\beta =$ infected machine become susceptible when they are rebooted
$\delta =$ non-vulnerable machine become susceptible again

Thereafter, based on the value of R0, both the disease free and disease-endemic equilibrium were determined. Numerical simulation is then designed and run with different chosen parameters' values to reflect the various behaviors of the model (Jerkins et al., 2018). Based on the simulation results, it was demonstrated that a well termed inoculation epidemic with a suitable infection vector would be capable of mitigating the damage associated with a large scale malware attack on the internet. However, as previously established that devices recovered through patching are similarly vulnerable to the same malware since bots frequently update with new exploits (Acarali,et al., 2019). Consequently, inoculation techniques can not be reliably used to mitigate IoT botnet propagation.
Hence, in the absence of effective vaccines or treatment, it is realistic to mitigate IoT botnet propagation by isolating the memory-efficient infected nodes.

3. Proposed Model

Rather than mitigating the infected nodes via vaccination or patching, we proposed the IoT Susceptible-Infected Abandoned-Forensic (IoT-SIAF) model to isolate memory-efficient bots in mitigating IoT botnet propagation. To isolate memory-efficient bots from infected nodes, it is paramount to consider not only parameters that can affect the propagation of the attack but those parameters that can distinguish between memory-efficient bot with the remaining bot from the infected nodes. In this regard, to build the model, the following steps are required:

A. Model Assumption

To understand the process of propagation and mitigation of IoT botnets respectively. Clear assumptions are stated as follows:

- Dynamic IoT wireless sensor based network with mobility of nodes, that is, nodes can be added/ remove from the network.
- A random network deployment.
- Homogeneous IoT sensor nodes with different memory status at a time.

With the established assumptions, we built an IoT-SIAF model by modifying the epidemic model S-I(Susceptible-Infectious), with add-on classes A and F to stand for abandoned and forensic nodes(Memory-Efficient bots) respectively. In this work, the object of forensic interest (forensic nodes) is defined as infectious memory-efficient bots with the capability of holding a large amount of traces of the attack for forensic analysis

B. Model Parameters and Notation

The model is built using four different classes, susceptible class S(t), Infectious class I(t), Abandoned class A(t) and forensic class F(t). In addition to these classes, other parameters are clearly defined in the Table 1 while the parameter values can be determine depending on the scenario at hand, it is essential to highlight some of the importance once as follows:

Table 1. Model Notation and Parameter Definitions

Notation	**Parametric Definition**
Ω	Scanning rate
B	Infection rate
λ	new nodes added to the network
θ	rate of losing neighboring nodes
T	rate of abandoning bots
Γ	rate of isolating bots
α	rebooting rate of abandoned bots
Δ	data loss rate of forensic nodes

C. Infection Rate

The infection rate of a botnet attack as in the case of Mirai, depends on the scanning rate ω of IP address and the successful probability $P_{robsucc(blast)}$ of blasting a password library of 62 records with unique blasting weight. Therefore, the infection rate can be determined using (2)below:

$$\beta = \omega \times P_{robsucc(blast)} \quad (2)$$

Upon identifying a potential victim, the bot entered into a brute-force login phase in which it attempted to establish a telnet connection using 10 username and password pairs selected randomly from a pre-configured list of 62 credentials (Antonakakis et al., 2017). Hence, the probability of successful blasting $P_{robsucc(blast)} = 0.72580$

D. Abandon Rate

To propagate further the attack, the botmaster directs bot to scan and send information about the target node, based on the information about the target, the memory-inefficient bots can be abandon using the equation (3) below:

$$\tau = (\frac{r_m}{r_i} \times \frac{I(t)}{S(t)} \times target\ Size) - 1 \quad (3)$$

Where r_m is the remaining memory space of the bot and r_i is the bot's initial memory space as adopted from the definition of memory efficiency of a sensor node [21]. The target size is the size of information acquired from a target nodes before it can be attack. The minimum target size to attack a node is 9 bytes.

E. Isolation Rate (γ)

In an attempt to isolate the bot from infected nodes, it is necessary to search for super spreaders bots. Super spreaders are bots with high memory that gathered a large amount of information about the target nodes, for the attacker to exploits and execute the attack. To isolate the super spreaders bot, we define the isolation rate γ as the probability compliment of the abandon rate τ. This is because, abandon rate transferred bots with low memory to the abandoned class, hence the isolation rate will target bots with high memory for onward transfer to the forensic class. Therefore, the isolation rate can be mathematically expressed as in (4) below:

$$\gamma = 1 - \tau \quad (4)$$

F. *Schematic Representation Of The Model*

To demonstrate the relationship among different classes and various parameters of IoT-SIAF model, the model is diagram mathematically represented in the Fig. 1 below

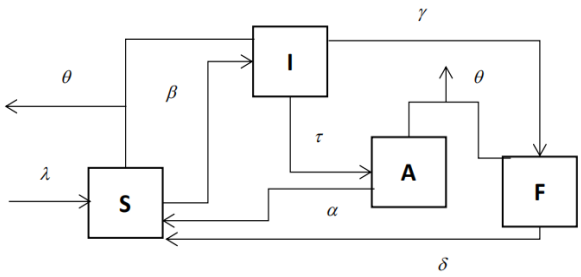

Fig 1. IoT-SIAF Schematic Representation

From Fig. 1 above, IoT-SIAF model consist of four classes, with infection parameter β transferring nodes from susceptible class S to the infections class I, the abandon rate τ transfer low memory bots to the abandonment class A, while α and δ transfer nodes from E and F to S respectively as a result of rebooting of bot and data loss. Finally, λ and θ signify the addition of new nodes and the removing of nodes from the neighboring device respectively. This dynamic process of transferring nodes from one state to another follows a system of differential equation given as in (5) below:

$$\frac{dS}{dt} = \lambda - \beta S(t)I(t) + \delta F(t) + \alpha A(t) - \theta S(t)$$
$$\frac{dI}{dt} = \beta S(t)I(t) - (\tau + \gamma + \theta)I(t)$$
$$\frac{dA}{dt} = \tau I(t) - (\theta + \alpha)A(t)$$
$$\frac{dF}{dt} = \gamma I(t) - (\delta + \theta)F(t) \qquad (5)$$

To understand the dynamic behavior of the model and the effect of changes of parameter values on IoT botnet propagation, (5) will be subjected to stability analysis. Stability analysis has been a technique used in most of the malware propagation models; the concept is generally to understand the steady-state effects of different parameters in the models.

G. Stability Analysis Of The Proposed Model

To study the stability of the IoT-SIAF model, the basic reproduction number R_0 which determines the number of secondary bots produced by a single (typical) infection in a completely susceptible population can first be obtained. R_0 often serves as a threshold parameter that predicts whether a botnet will spread in an IoT platform, to achieve this, we check the stability of the model at both the botnet-free and botnet-endemic equilibrium states.
To generate R_0 from the mathematical model (5), we considered states consisting of infectious parameter and applied a generation matrices to obtained R_0 as in the equation (6)

$$R_0 = \beta\lambda/(\theta(\tau + \gamma + \theta)) \quad (6)$$

If the value of $R_0 < 1$, the botnet propagation will be eliminated within the IoT wireless network and the proposed model will stabilized at botnet-free equilibrium, else if $R_0 > 1$, the botnet will propagate consistently within the IoT network and the proposed model will stabilize at botnet endemic equilibrium.

4. Results

To investigate the behavior of different IoT botnet infection scenario and validate the qualitative results of our IoT-SIAF model, we perform numerical simulation by programming the model using de Solve package [22] of R script. The numerical simulation is performed based on the parameters' values that can reflect the effect of our proposed model in mitigating the menace of IoT botnet propagation.

The simulation will consider different parameter values that are chosen to demonstrate the various possible behaviors of the proposed model when the value of $R_0 < 1$ and $R_0 > 1$ respectively.

Taking the parameter values ($\beta = 0.106, \lambda = 3.0,\ \delta = 0.075,\ \alpha = 0.06, \theta = 0.301,\ \tau = 0.301$ and $\gamma = 1 - \tau$), will enable us to have the value of our $R_0 = 0.8133 < 1$ close to $R_0 = 0.8138$ from the work of (Khanh et al., 2016). With the value of our R_0 closely related to that of (Khanh et al., 2016). We similarly took the exact value of the initial condition ($S(0) = 1.5,\ I(0) = 2.75,\ A(0) = 1.15$, and $F(0) = 0.01$) from SIQR model (Khanh et al., 2016). However, we replaced $Q(t)$ and $R(t)$ with $A(t)$ and $F(t)$ respectively. This because the work of (Khanh et al., 2016) shared some similarity with our work in an effort to quarantine infected nodes from the attack of worms in a wireless sensor network. Fig. 2 shows the number of bots (I) dying out from the IoT network, this satisfied the condition for botnet-free equilibrium state ($R_0 < 1$). The number of bots has decayed down to zero due to the isolation of the memory-efficient bots to the forensic class (F). In this regard, most of the susceptible nodes are prevented from being infected and also some abandoned bots that undergone the rebooting process have similar transferred to the susceptible class. Consequently, the entire propagation process stabilized at botnet-free equilibrium state.

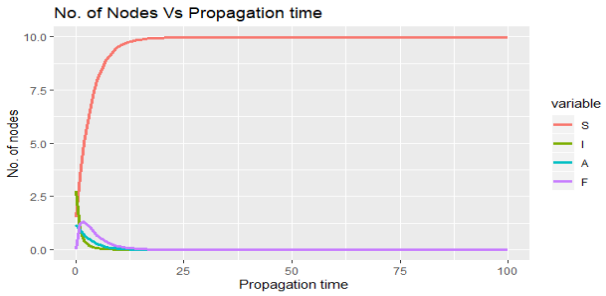

Fig 2. IoT-SIAF : Simulation results with $R_0 < 1$

On the other hand, Fig. 5 below shows the simulation results with the value of $R_0 > 1$. This has been achieved by setting the parameters' values for $(\lambda = 7,\ \delta = 0.075,\ \alpha = 0.06,\ \tau = 0.1,\ \theta = 0.295$ and $\beta = 0.105)$ and Initial conditions $(S(0) = 2.5,\ I(0) = 3.75, A(0) = 0.025$ and $F(t) = 4.0)$ SIQR model (Khanh et al., 2016). However, we similarly replaced $Q(t)$ and $R(t)$ with $A(0)$ and $F(0)$ respectively. The behaviors of the simulation match with the condition of $R_0 > 1$. It is shown that despite the isolation of the memory- efficient bots to the F class for forensic analysis, the botnet infection pickup to stabilized and persist within the IoT network. Nevertheless, the behavior of the simulation satisfied the botnet endemic equilibrium state, since all the nodes in various classes remain stable as time tends to infinity.

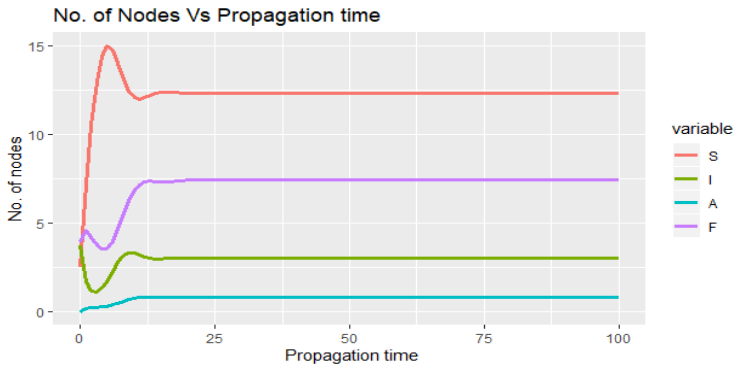

Fig 3. IoT-SIAF : Simulation results with $R_0 > 1$

5. Conclusion

In this paper, we explored the effect of isolating memory-efficient bots as a strategy in mitigating IoT botnet propagation. By isolating the memory-efficient bots at the botnet-endemic equilibrium state, our proposed IoT-SIAF model has effectively decreased the botnet infectious peak value and stabilized the attack propagation. Also, at the botnet-free equilibrium state, the proposed model suppressed the attack in such away that the number of the existing bots dies out from IoT network. Hence, it is deduce that the having a good parameters setting and isolating the most efficient bots from the network can mitigate botnet propagation.

References

Acarali D., M. Rajarajan, N. Komninos, B.B. Zarpelão,(2019). Modelling the Spread of Botnet Malware in IoT-Based Wireless Sensor Networks. *Security and Communication Networks*., vol. , pp. 1-13.

Alur R., E.Berger, A.W. Drobnis, L. Fix, K. Fu, G.D. Hager, D. Lopresti, K. Nahrstedt, E. Mynatt, S. Patel, and J. Rexford (2016). Systems computing challenges in the internet of things. arXiv preprint arXiv. 1604.02980.

Antonakakis, M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., Z. Durumeric, J. A. Halderman, L. Invernizzi, and M. Kallitsis, (2017). Understanding the mirai botnet. *in 26th USENIX Security Symposium (USENIX Security 17),* Vancouver, BC, Canada, pp. 1093–1110.

Farooq M.J. and Q. Zhu (2019). Modeling, analysis, and mitigation of dynamic botnet formation in wireless iot networks. *IEEE Transactions on Information Forensics and Security*, vol.14, pp. 2412-2426.

Feng L. L. Song, Q. Zhao, H. Wang (2015). Modeling and stability analysis of worm propagation in wireless sensor network . *Mathematical Problems in Engineering.* vol. 2015, pp. 1-8.

Gardner M.T., C. Beard, and D. Medhi (2017).Using SEIRS epidemic models for IoT botnets attacks. *In Proc. 13th International Conference on Design of Reliable Communication Networks*, Munich, Berlin, Germany, pp.62-69.

Gu Q. and Noorani, R. (2008).Towards self-propagate mal-packets in sensor networks, *in Proc. first ACM conference on Wireless network security* pp. 172-182.

Jerkins J.A. and J. Stupiansky (2018). Mitigating IoT insecurity with inoculation epidemics. In Proc.ACM SE '18: Southeast Conference,New York, NY, United States, pp. 608-615.

Ji, Y., L. Yao, S. Liu, H. Yao, Q. Ye, and R. Wang,(2018). The Study on the Botnet and its Prevention Policies in the Internet of Things. *22nd Int. Conf. Computer Supported Cooperative Work in Design*, Nanjing, China, May. 9-11, pp. 837–842.

Khanh N.H., (2016). Dynamics of a Worm Propagation Model with Quarantine in Wireless Sensor Networks. *Appl. Math*. vol.10, 2016, pp. 1739-1746.

Koroniotis, N., N. Moustafa, and E. Sitnikova,(2019). Forensics and deep learning mechanisms for botnets in Internet of Things: A survey of challenges and solutions. *IEEE Access*., vol. 7, pp.61764-61785

MacDermott, A., T. Baker, and Q. Shi, (2018). Challenges for the ioa era. *9th IFIP Int. Conf. on New Technologies, Mobility and Security (NTMS)*, Paris, France, Feb. 26-28.

Mishra B.K. and N. Keshri,(2013). Mathematical model on the transmission of worms in wireless sensor network. *Applied Mathematical Modelling*., vol. 37, pp. 4103-4111.

Oriwoh E., D. Jazani, G. Epiphaniou, and P. Sant (2013). Internet of things forensics: Challenges and approaches. *In Proc. 9th IEEE International Conference on Collaborative computing: networking, Applications and Worksharing*, Austin, TX, USA, pp. 608-615

Servida, F., and E. Casey(2019). IoT forensic challenges and opportunities for digital traces. Digital Investigation., vol. 28, pp.S22-S29.

Singh, A., A.K. Awasthi, K. Singh, and P.K. Srivastava (2018). Modeling and analysis of worm propagation in wireless sensor networks. *Wireless Personal Communications*, vol. 98, no. 3, pp.2535-2551.

Wang, T. Q. Wu, S. Wen, Y. Cai, H. Tian, Y. Chen, B. Wang,(2017). Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks. *Sensors*, vol.17, pp. 1-17.

Yin M., X. Chen, Q. Wang, W. Wang, and Y. Wang (2019). Dynamics on Hybrid Complex Network: Botnet Modeling and Analysis of Medical IoT. *Security and Communication Networks*. vol 2019; pp. 1-14.