Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 7805408, 10 pages
https://doi.org/10.1155/2018/7805408

Research Article

Gleer: A Novel Gini-Based Energy Balancing Scheme for Mobile Botnet Retopology

Yichuan Wang, Yefei Zhang, Wenjiang Ji, Lei Zhu, and Yanxiao Liu

Xi'an University of Technology, Xi'an, China

Correspondence should be addressed to Yichuan Wang; chuan@xaut.edu.cn

Received 6 March 2018; Accepted 17 April 2018; Published 15 May 2018

Academic Editor: Kim-Kwang Raymond Choo

Mobile botnet has recently evolved due to the rapid growth of smartphone technologies. Unlike legacy botnets, mobile devices are characterized by limited power capacity, calculation capabilities, and wide communication methods. As such, the logical topology structure and communication mode have to be redesigned for mobile botnets to narrow energy gap and lower the reduction speed of nodes. In this paper, we try to design a novel Gini-based energy balancing scheme (Gleer) for the atomic network, which is a fundamental component of the heterogeneous multilayer mobile botnet. Firstly, for each operation cycle, we utilize the dynamic energy threshold to categorize atomic network into two groups. Then, the Gini coefficient is introduced to estimate botnet energy gap and to regulate the probability for each node to be picked as a region C&C server. Experimental results indicate that our proposed method can effectively prolong the botnet lifetime and prevent the reduction of network size. Meanwhile, the stealthiness of botnet with Gleer scheme is analyzed from users' perspective, and results show that the proposed scheme works well in the reduction of user' detection awareness.

1. Introduction

With the improvement of integrated-circuit technology, smartphones begin to provide better support for applications and services. Since users are increasingly exploiting smartphones for sensitive transactions (especially online shopping and banking), these mobile devices contain more sensitive and privacy information than legacy computer. Their unique features, including mobility, portability, and wide connectivity options, also play a significant role in promoting the rapidly growing popularity of smartphones. However, due to the lack of sufficient security and privacy protection mechanisms, smartphones are inevitably becoming the hot target of hackers. Among these threats from hackers, the mobile botnet [1] (evolved from traditional botnet) is the most destructive one, which not only steals user's privacy, but also attacks other network devices (e.g., DDOS). The motivation of this work is to shed light on potential botnet threats that are targeting smartphones. Since there are differences between computer and smartphone in many aspects, such as system structure and communication mode, existing techniques against computer botnets may not be applicable to mobile botnets. Thus, in the paper, we propose a Gini-based energy balancing scheme for defending mobile botnet attack, which can promote security researchers to investigate and develop new countermeasures before mobile botnets become a major threat [2].

The botnet life-cycle can be divided into six stages: botnet conception, botnet recruitment, botnet interaction, botnet marketing, attack execution, and attack success [3]. In the first stage, after confirming the motivation for creating a botnet, the following steps are processed for implementing the desired botnet. Various aspects should be carefully considered in this step, especially those regarding bot infection and botnet communications. From botmasters' perspective, improving the stealthy and robust of mobile botnet becomes the key objective in design process, while understanding the deployment strategy of a mobile botnet is critical for defending against malicious attacks on network in runtime from operators' perspective. Recently, there exist many literatures focused on mobile botnet communications design. Singh et al. [4] developed a mobile botnet on the basis of node popularity and leveraged publicly available data to demonstrate that the Bluetooth technology can be used as

C&C channel in a mobile botnet. Zeng et al. [5] proposed a mobile botnet that makes the most of mobile services and is resilient to disruption, utilizing SMS message for C&C and imitating the P2P fashion in the PC world. It is finally demonstrated that the structured architecture is a best choice for the mobile botnet topology. And in [6], Chen et al. proposed a novel multiple-push service based botnet, which significantly outperforms existing push-styled mobile botnet by exploring the design space of exploiting such services.

In the design process, the botnet architecture is the key decision, which determines the operation of subsequent element and thus the whole body of botnet [7]. The mobile botnet node, i.e., smartphone, constitutes the main component of mobile botnet architecture. The mobile botnet composed of smartphones is similar to sensor networks (SNs) in the architecture. (1) Topology design: their architecture can be centralized, distributed, or hybrid. Since the centralized scheme may encounter a single-point-of-failure, and distributed one is with high communication cost, most works on mobile botnet topology design are based on heterogeneous multilayer [8, 9], similar to cluster division of SNs. (2) Node management: due to the constrained power of smartphone and sensor, designing a node management scheme to reduce the node energy consumption and lowering the atomic network energy gap are in need. However, due to the fact that there exist some differences in constituent nodes and practical significance, the SNs management scheme cannot be applied to mobile botnet directly, such as low-energy adaptive clustering hierarchy (LEACH) and stable election protocol (SEP).

In view of the mobile botnet features and differences mentioned above, in this paper, we propose a region command and conquer (C&C) server selection scheme. At each start of operation cycle, we firstly divide smartphones of an atomic network into two categories according to their remaining capacity by the dynamic energy partitioning threshold. Then, the Gini coefficient is introduced to evaluate the power gap of nodes in the atomic network. Finally, the above coefficient values are leveraged to adjust and assign the selection probability to each type. Experimental results indicate that our proposed scheme can narrow the power gap of nodes in the atomic network and lower the reduction rate of network scale simultaneously. Meanwhile, the diversity of mobile network energy distribution at each experimental stage can lower the awareness of users effectively, which is beneficial to the concealment of mobile botnet. Therefore, the defensive strategies, which target the mobile botnet designed based on Gleer, should consider comprehensive factors instead of single factor like node power and use machine learning to explore potential insecurity features to detect the mobile botnet.

The rest of the paper is organized as follows: Section 2 describes the current researches on the mobile botnet topology and some cluster-head selection schemes for SNs; Section 3 shows the proposed C&C server selection scheme; Section 4 shows the experiment and result analysis; Section 5 presents the overall conclusions of this paper.

2. Related Work

2.1. Mobile Botnet Model. Different from legacy botnets, mobile botnets have to address new challenges from the unique features of mobile Internet and smartphones. More precisely, smartphones typically are with limited battery power, computation, and communication capabilities. If a bot consumes too much power, network traffic, or computation resource, then it will cause owner's awareness immediately. Many researches solve this problem by allocating hardware resources. For example, Chen et al. [10] proposed a novel cloud-based technology to overcome existing issues of mobile botnets. Meanwhile, due to the similarity between mobile botnets and SNs, we can also derive the network topology management scheme in SNs as follows. (1) The limited energy: despite being battery-operated, it may be unrealistic to recharge them due to either the inhospitable terrain for sensors or the high-mobility for smartphones. As such, the network lifetime maximization is of prime importance for SNs and mobile botnets [11]. (2) Cooperation [12]: they both involve a large number of nodes. Despite constrained capability of single node due to its limited energy capacity and communication capabilities, the collaboration among hundreds of nodes could offer unlimited possibilities. (3) High confidentiality: as SNs have been widely used in military, industrial, and health-care applications, the data transmitted among sensors are typically with significant values similar to the delivery in the mobile botnet for botnet controller. Thus, a secure communication with high confidentiality is perquisite [13].

It follows that SNs and mobile botnets share common goals: lifetime prolonging, coverage extension, seamless integration, and high reliability. Since data communication is basically an energy-intensive activity, the distribution of communication load among sensors contributes to their energy-consuming equilibration [14]. Currently, there are many existing works [15–19] with respect to clustering nodes to balance energy depletion and extending network lifetime further. Typically, nodes are divided into groups, and then a specific one is selected as the CH, similar to the hybrid scheme in the mobile botnet. In [20], a typical structure is designed, showed as in Figure 1, where the multilayer heterogeneous mode is favored, and the basic composition is atomic network which likes cluster in sensors. In Figure 1, the botmaster generates and sends commands to C&C servers, which distributes received commands to some region C&C servers further. Next, by analyzing each command, the region C&C server controls some bots to execute it, i.e., with a similar functionality to the cluster head (CH) in SNs.

2.2. Cluster-Head Selection Scheme. In the clustering procedure, selecting a CH for each cluster is of vital significance. Since CHs are responsible for aggregating reports from cluster members and then forwarding collected messages to the sink, they would consume more energy than non-CH nodes. For network retopology, the CH selection is always designed to be dynamic; e.g., LEACH [15] switches the CH role among nodes based on a prior optimal probability.

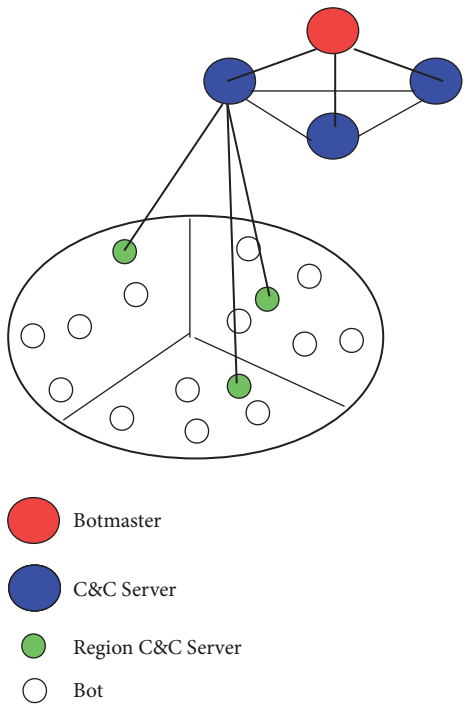


Figure 1: Mobile botnet logical topology.

Moreover, HEED [17] selects CH according to a hybrid of node residual energy and a secondary parameter, such as the distance between nodes or node degree. Furthermore, SEP [16] and P-SEP [18] are heterogeneity-aware protocols, introducing a fixed value α to represent the initial energy capacity difference ratio between two levels of deployed nodes.

To balance energy consumption, a cluster-head periodicity is favored in the atomic network. The selection used in SNs, nevertheless, does adapt to mobile botnet, with main factors as follows. (1) Mobile botnets need high stealthiness. The abnormal can be more easily awarded by a smartphone than a sensor; e.g., smartphone users are more sensitive to energy consumption. Thus, a fixed ratio (introduced in LEACH) between the remaining capacity and node selection probability cannot be applied to mobile botnets directly. Due to the difference between initial energy of nodes, a fixed value α introduced in SEP does not fit the mobile botnet scene. (2) Traditional CH selection schemes do not consider network energy gap, which may increase the network reduction rate. (3) There exist differences in component nodes and practical significance, so the selection scheme should necessitate a combination of their feathers. In view of these factors, we propose an energy balancing CH selection scheme based on Gini coefficient (Gleer). In particular, the energy partitioning threshold, i.e., α-value, is introduced, to categorize nodes of an atomic network into two groups: energy-sufficient node and energy-deficient node. Then, Gini coefficient is leveraged as an indicator to estimate botnet energy gap, as well as adjusting and optimizing the selection probability for each type.

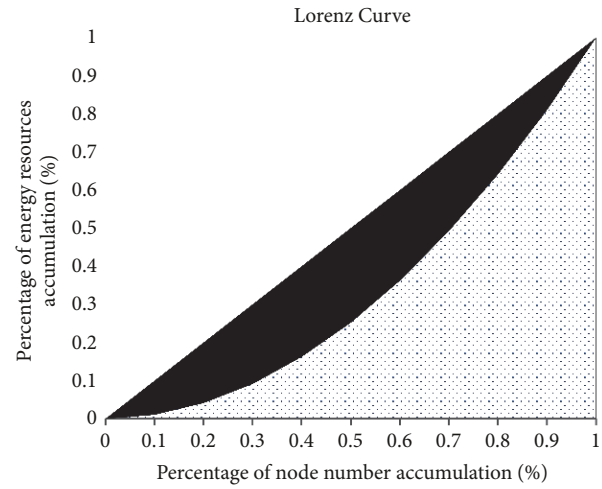


Figure 2: Lorenz Curve.

3. The Model

3.1. Gini Coefficient for Cluster-Head Selection. Gini coefficient was proposed by famous Italian economist C. Gini on the basis of the Lorenz curve in 1912 and has been deemed as a comprehensive index prevailing in the world showing the inequality degree of income distribution [21]. In this paper, it has been used as the main indicator widely. Figure 2 shows the Gini coefficient intuitively referring to the proportion of area A divided by A + B. In our work, we regard each node in an atomic network as a resident and its surplus energy as the current resident income and introduce the Gini coefficient as the measurement index for energy difference degree. As such, Figure 2 can be explained as follows: A is the area surrounded by actual Lorenz curve and energy absolute no difference curve, and A + B is the surrounded area by absolute no difference curve and absolute difference curve. Here, the Lorenz curve qualitatively reflects the energy difference degree roughly.

The calculation of Gini mean deviation was given as follows:

$$\Delta = \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{\left|x_j - x_i\right|}{n(n-1)}, \quad 0 < \Delta < 2u, \tag{1}$$

where Δ is the Gini mean deviation; $|x_j - x_i|$ is an absolute value of any pair of income sample deviation; n is the sample size; and u is the average income. Since Δ is obviously a monotone increasing function of income inequality, Gini stipulated

$$G = \frac{\Delta}{2u}, \quad 0 \le g \le 1 \tag{2}$$

as a measure of income inequality. According to (1) and (2), we can have

$$G = \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{\left|x_j - x_i\right|}{2n(n-1)u}. \tag{3}$$

Equation (3) offers a direct calculation method for Gini coefficient valued between 0 and 1, and the smaller, the more fair and the bigger the more unfair. Since this formula just involves the arithmetic operation of income data, this estimation method can be used unconditionally in theory without errors [22, 23]. Based on the Lorenz curve and the calculation method, a simple formula was put forward by Jianhua [24] as follows:

$$G = 1 - \frac{1}{n}\left(2\sum_{i=1}^{n-1} W_i + 1\right). \tag{4}$$

From the above calculation, it follows that n nodes are permuted from small to large according to their remaining energy, and W_i denotes the proportion of the accumulated energy of the first node to i node in all the nodes resources.

3.2. Proposed Scheme

3.2.1. Energy Partitioning Threshold. Considering the numerical diversity of smartphone residual capacity, we introduce an energy partitioning threshold α and divide nodes of an atomic network into two types, namely, energy-sufficient node and energy-deficient node, based on the comparison between α and the remaining energy of each node. To ensure that all nodes exhaust at approximately the same time, the nodes with more energy should be CHs more often than those with less energy, so the α-value should be set greater than energy mean. Suppose that $n \in N$ represents the number of smartphones with nonzero power. The remaining power of node i is E_i, $i = 1, \ldots, n$, and the value of partition coefficient $k \in [0, 1)$, $k \in R$ decides the range of α from the average to maximum energy of nodes; namely,

$$\alpha = \frac{\sum_{i=1}^{n} E_i}{n} + k \cdot \left(\max\left(E_i\right) - \frac{\sum_{i=1}^{n} E_i}{n}\right). \tag{5}$$

3.2.2. Classification and Statistics. Formula (6) is utilized to classify each node: $m_i = 1$ represents the remaining energy of node i which is larger than α; otherwise, the value is smaller than α. Table 1 shows the total number and energy for each node category.

$$m_i = \begin{cases} 1, & \dfrac{(E_i - \alpha) + |E_i - \alpha|}{2} > 0, \\ 0, & \dfrac{(E_i - \alpha) + |E_i - \alpha|}{2} = 0. \end{cases} \tag{6}$$

3.2.3. Regulating CH Selection Probability. Sort nodes based on their residual energy in ascending order and calculate Gini coefficient (G-value) of the current mobile botnet energy situation by Formula (4). According to the provisions of the relevant organization of United Nations [25], the Gini coefficient below 0.2 denotes the income absolute average; 0.2 to 0.3 denotes relative average; 0.3 to 0.4 denotes relatively reasonable; 0.4 to 0.5 denotes the income inequality relatively large; more than 0.5 denotes a huge income gap. Theoretically, there is a warning threshold, which is upper-bounded by 0.4 empirically; beyond 0.4, the society would be not in harmony, such as regional unbalance, rural and remote poverty, discrimination, hostility, crime, and environmental degradation [26, 27]. Since the surplus energy of each node is regarded as resident income, to balance node energy consumption and lower network size reduction rate, we use $G = 0.4$ as the dividing line to regulate the cluster-head selection probability following Table 2, where P_S and P_D, respectively, represent the total selection probability for each category.

Table 1: Classification and statistic for each category.

	Nodes number	Energy
Sufficient	$K_S = \sum_{i=1}^{n} m_i$	$K_S = \sum_{i=1}^{n} m_i$
Deficient	$K_D = n - K_S$	$E_{totD} = \sum_{i=1}^{n} \cdot E_i - E_{totS}$

Table 2: Total selection probability.

	P_S	P_D
$G < 0.4$	$\dfrac{E_{totS}}{E_{tot}}$	$\dfrac{E_{totD}}{E_{tot}}$
$G \geq 0.4$	$\dfrac{1}{2} + \dfrac{\lvert E_{totS} - E_{totD}\rvert}{2E_{tot}}$	$1 - P_S$

3.2.4. Calculating the Selection Probability for Each Node. To prevent the defender from detecting botnet and hide the nodes selection rule, the selection probability is identical between nodes of the same kind. The actual selection probability for each category is, respectively, represented by P_{SA}, P_{DA}.

$$\begin{aligned} P_{SA} &= \frac{P_S}{K_S} \\ P_{DA} &= \frac{P_D}{K_D}. \end{aligned} \tag{7}$$

4. Model Analysis

In [28], Tremblay et al. presented an easy-to-use battery model applicable to dynamic simulation. Figure 3 shows one of the typical lithium battery consumption curves for smartphones. Due to the similarity of smartphone users belonging to the same time zone, for example, most users are accustomed to charging smartphones fully at night and terminating charging between 6:30 and 8:00 a.m., therefore, if phones are approximately homogeneous, then they have almost the same capacity of lithium battery, application software, and usage habits. We can thus infer that the battery consumption curve of their smartphones is almost the same. Then, the remaining power of a smartphone at a certain time follows normal distribution. To analyze the performance of Gleer directly, we conduct experiments in MATLAB testbed and expand the experiment to atomic network with G-value larger than 0.4. The initial node number is represented by n.

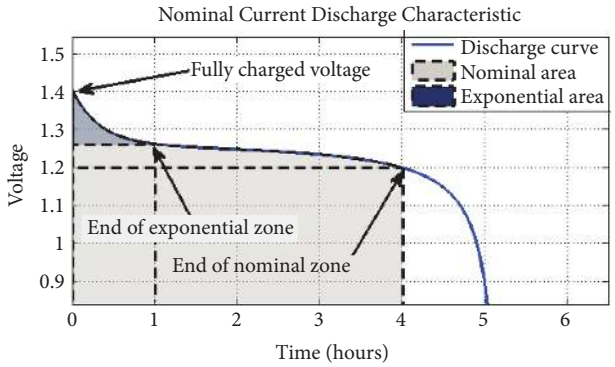


Figure 3: A typical discharge curve.

(1) Since CH nodes consume much more energy than normal ones, the atomic network should perform the CH selection process periodically to prevent the reduction of botnet size. Figure 4 shows the variation of Gini coefficient throughout the botnet lifetime. From Figure 4, it reveals that LEACH shows a significant increase, while Gleer is nearly stable. Meanwhile, it is obvious that Gleer outperforms LEACH in terms of lowering energy gap. That is, the proposed scheme could benefit the energy balance distribution of mobile botnet.

(2) Figure 5 represents the G-value versus the partition coefficient (k). As Figure 5(a) shows, when the initial sample and experiment conditions are identical, the energy distribution (G-value) almost remains unchanged with partition coefficient (k-value). Since k-value is an important parameter of Gleer scheme, the diversity of mobile botnet can prevent defenders cracking its internal rules and benefit the stealthiness of mobile botnet. Figure 5(b) also reveals the relationships between different initial conditions. From Figures 5(a) and 5(b), it follows that there exists a certain range for the multiexperiments with the same sample. However, boundaries emerge with different initial samples.

5. Simulation

NS-3 is an open-source and widely used network simulation platform [29] for networking research; it contains many models which simulate the packet data networks working and performing scene and provides a simulation engine for users to conduct simulation experiments. In this section, NS-3 platform is used to validate our model.

For simplicity, we only consider one cell as an atomic network with multiple nodes, and the base station is responsible for the connections between these nodes and the C&C server. Based on the models in [30] provided by NS-3, we build the network topology as shown in Figure 6. The battery model parameter for each node is from [28, 31], and Table 3 shows the detailed simulation configuration. The main task of this simulation is to select a node in the cell to be the region C&C server.

(1) Figure 7 shows mobile botnet performance in terms of energy node survival rate, energy consumption ratio, energy consumption ratio differences, and energy consumption ratio differences cumulative sum. With identical initialization (i.e., $n = 50$, G-value = 0.473), it can be observed from Figure 7(a) that the mobile botnet with Gleer scheme has larger lifetime than that with LEACH scheme. Since the proposed scheme involves the botnet energy distribution, it could benefit the prevention of botnet scale reduction caused by improper node selection. Figures 7(b), 7(c), and 7(d) show the energy consumption comparison; since Gleer contributes to the maintenance of botnet size and the lowering of number of death nodes, it can save much more energy and execute much more attacks with limited energy resources.

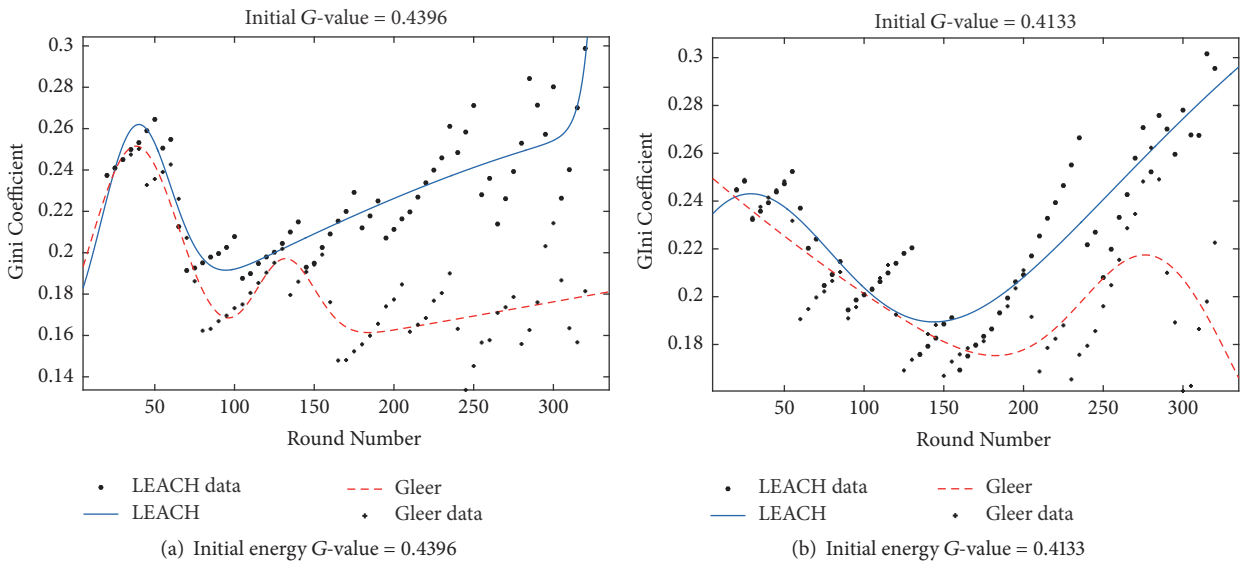
Table 3: NS-3 simulation configuration.

Name	Configuration
UE nodes	50
ENB nodes	1
Data rate between EPC and C&C server	100 G/s
Delay	0.01
App protocol	TCP
Packet size	1280
Simulated interval	2 s
Initial energy	100~31752 J
Initial Cell Voltage	3.45 A
Normal nodes current draw	2~4 A
Cluster nodes current draw	5~8 A
Nominal cell voltage	3.3 V
Exp Cell Voltage	3.6 V
Rated Capacity	2.45 Ah
Nom Capacity	1.1 Ah
Exp Capacity	1.2 Ah
Internal Resistance	0.145 Ohms

(2) For some abnormal cases, for example, strange SMS with a website URL linked to virus and emails with an attachment cheating, the intuition for smartphones users to judge whether a cell phone is safe is to observe the battery power variation. In order to show users' view obviously, the simulation is conducted six times with the same initial user group ($n = 50$, G-value = 0.437) and k-value ($k = 0.5$), and six users are picked randomly to observe their energy consumption. As Figure 8 shows, when the simulation reaches 30 s, there exists an energy bound for No. 4 user, ranging from $2.8 * 10^4$ J and $2.92 * 10^4$ J. For No. 25 user, the energy of six simulations is almost the same. And for No. 5 user, the time of arriving at the lowest energy varies. From these simulation results, it is observed that one user (infected by the mobile botnet with the proposed scheme) cannot judge whether his smartphone is abnormal or not, by analyzing the energy consumption. The energy consumption diversity across users shows that our proposed scheme can improve the stealthiness of mobile botnet effectively.

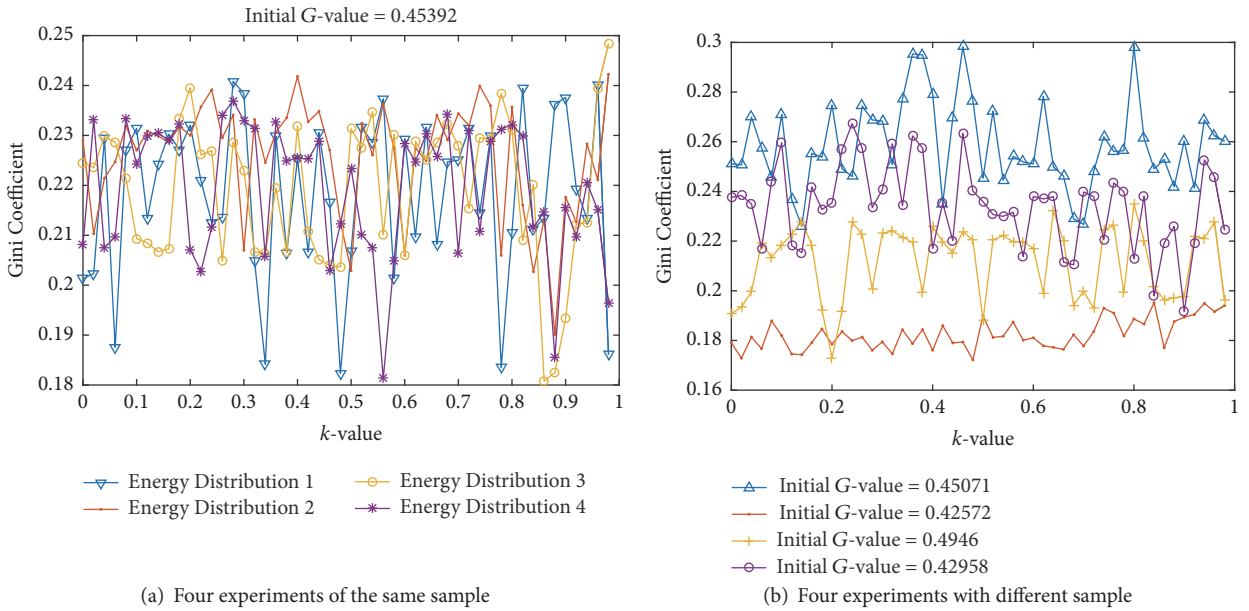
6. Defensive Strategies

As described in [32], smartphones not only provide capabilities of legacy computers, but also offer a large number of



(a) Initial energy G-value = 0.4396 (b) Initial energy G-value = 0.4133

Figure 4: The relationship between the G-value and round number.



(a) Four experiments of the same sample (b) Four experiments with different sample

Figure 5: The relationship between the G-value and k-value under different conditions.

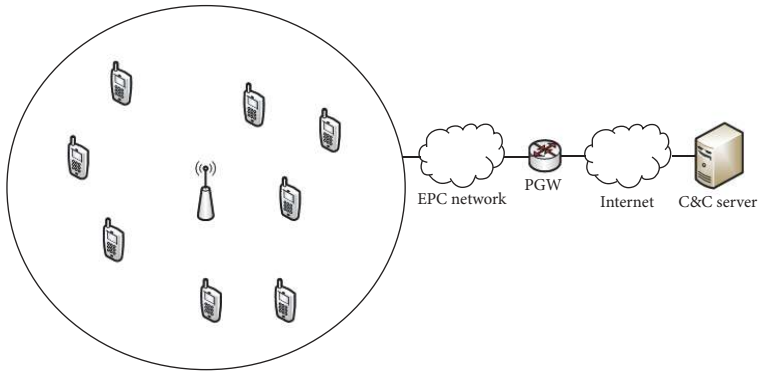


Figure 6: Simulation topology network.

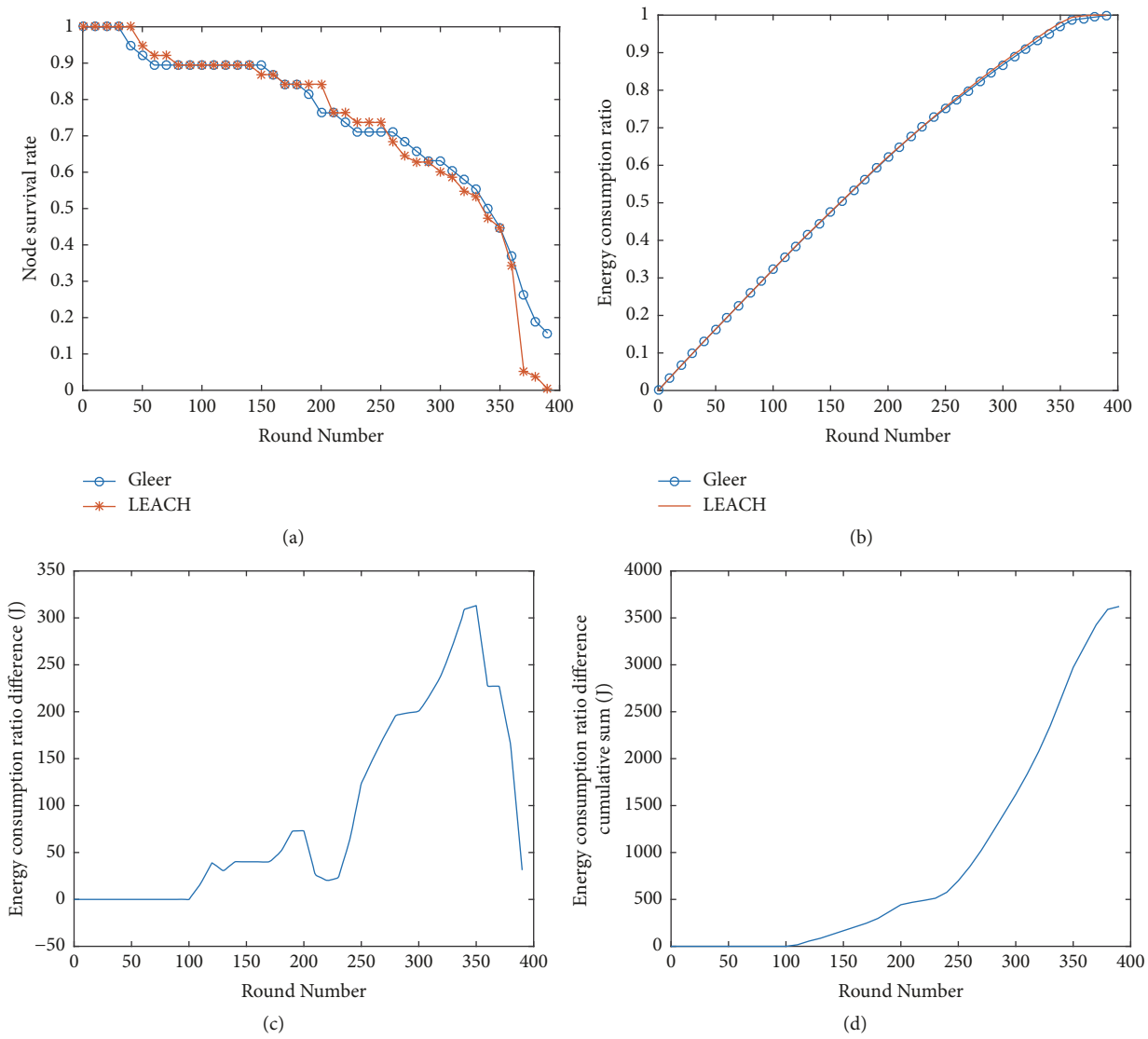


Figure 7: The comparison of node survival rate and energy consumption ratio.

connectivity options, i.e., IEEE 802.11, Bluetooth, and GPRS. In addition, smartphones have stronger personalization. Thus, detection methods, such as traffic detection [33, 34], with good effects to computer world may not be applicable to mobile botnet. Different from computers, smartphones are characterized by limited resources, e.g., CPU and memory. Among these characteristics, the battery is predominant for users to discover the abnormal of their smartphones.

In Gleer, node energy consumption is closely related to botnet structure and energy distribution, which significantly lowers the probability that defenders can observe or disrupt networks. For one node, the probability to be CH is related to the botnet energy gap and division line, rather than its remaining energy. Legacy detection methods, such as power consumption [35] and application signature analysis [36], are unlikely to help protect cellular providers against such activity. Therefore, based on the characteristics of Gleer, exploring features with a combination of unsupervised (clustering) and supervised (classification) machine learning is more appropriate, e.g., the feature extraction from battery usage statistics and attack model. The main steps can be summed up as collecting enough data, analyzing their intrinsic characteristics, adjusting learning algorithms, and finding their internal relations further.

7. Conclusion and Future Work

In this paper, we proposed a new CH selection scheme (Gleer) for heterogeneous multilayer mobile botnet. We first utilized the dynamic energy partitioning threshold α to categorize atomic network nodes into two groups. Then, we introduced the Gini coefficient to estimate the current power gap of nodes and regularized the probability of becoming the region C&C server for each kind node based on the above gap coefficient value. The experimental results show that the proposed scheme works well in narrowing the gap than traditional ones. In order to confirm our results more accurately, we

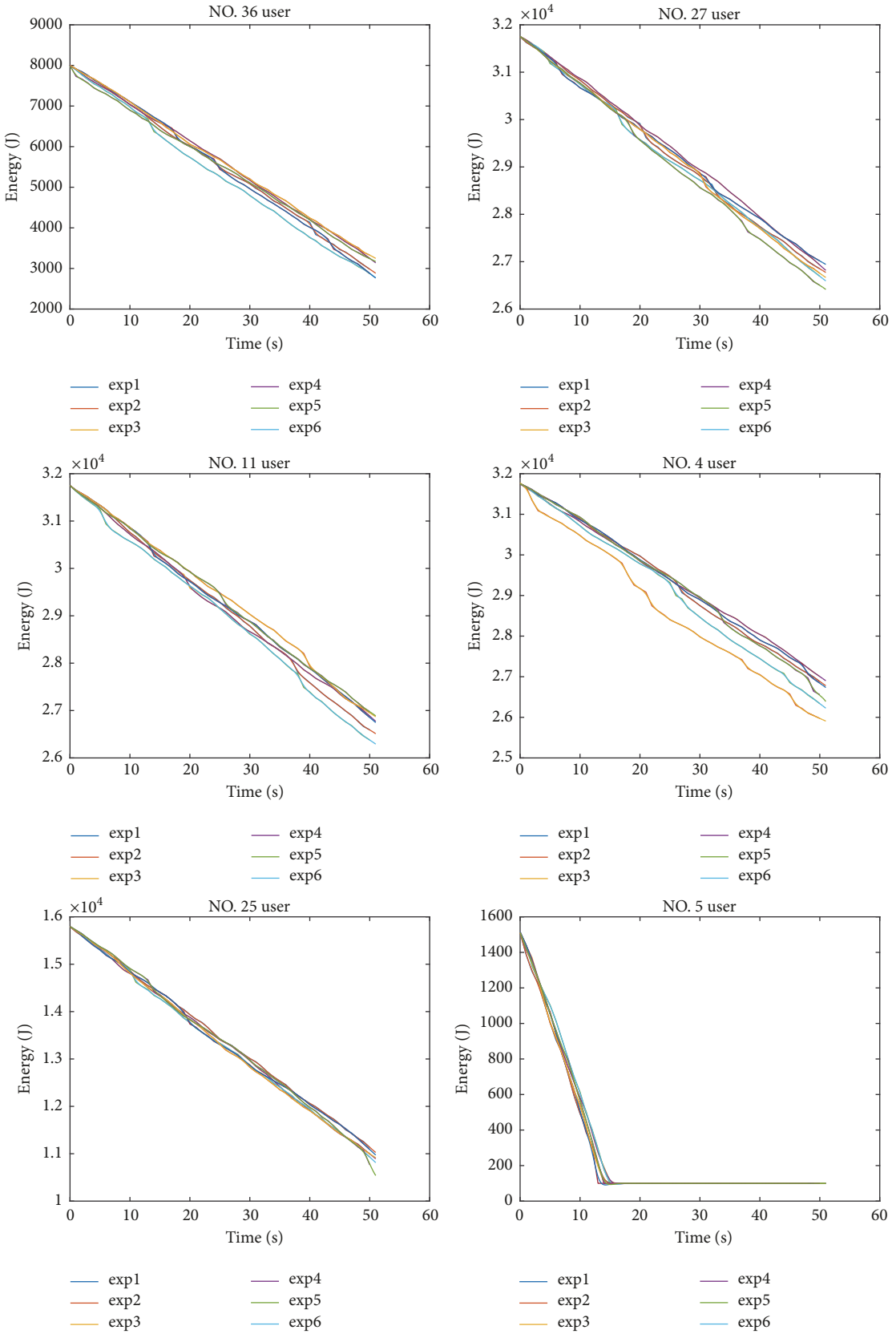


Figure 8: The relationship between the energy and time.

compared Gleer and LEACH in the NS-3 network simulation platform, and the results demonstrate that the mobile botnet with the proposed scheme has longer lifetime and save more energy; that is, the botmaster can execute more attacks with limited energy resources. Meanwhile, we also analyzed the diversity of network energy distribution with different conditions and show the energy consumption variation in users' perspective. And results show that the proposed scheme can maintain the performance diversity of the botnet energy distribution, which benefits the concealment of the mobile botnet.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper is supported by the National Natural Science Foundation of China (61602376, U1334211, U1534208, 61602374, and 61702411), Natural Science Foundation of Shanxi Province (2017JQ6020), Science Technology Project of Shaanxi Education Department (16JK1573), Ph.D. Research Startup Funds of Xi'an University of Technology (112-256081504), College Research Funds of Xi'an University of Technology (112-451016007), National Foundation of China (U1534208), and Science and Technology Innovation Project of Shanxi Province (2015KTZDGY0104).

References

[1] I. Vural and H. Venter, "Mobile Botnet detection using network forensics," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 6369, pp. 57–67, 2010.

[2] J. Milosevic, F. Regazzoni, and M. Malek, "Malware threats and solutions for trustworthy mobile systems design," *Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment*, pp. 149–167, 2017.

[3] R. A. Rodriguez-Gomez, G. Macia-Fernandez, and P. Garcia-Teodoro, "Survey and taxonomy of botnet research through life-cycle," *ACM Computing Surveys*, vol. 45, no. 4, Article ID 2501659, 2013.

[4] K. Singh, S. Sangal, N. Jain, P. Traynor, and W. Lee, "Evaluating Bluetooth as a medium for botnet command and control," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 6201, pp. 61–80, 2010.

[5] Y. Zeng, K. G. Shin, and X. Hu, "Design of SMS commanded-and-controlled and P2P-structured mobile botnets," in *Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec'12*, pp. 137–148, usa, April 2012.

[6] W. Chen, X. Luo, C. Yin, B. Xiao, M. H. Au, and Y. Tang, "Muse: Towards robust and stealthy mobile botnets via multiple message push services," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 9722, pp. 20–39, 2016.

[7] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 446–471, 2013.

[8] L. Cao and X. Qiu, "ASP2P: An advanced botnet based on social networks over hybrid P2P," in *Proceedings of the 22nd Wireless and Optical Communications Conference, WOCC 2013*, pp. 677–682, chn, May 2013.

[9] A. Malatras, E. Freyssinet, and L. Beslay, "Mobile Botnets Taxonomy and Challenges," in *Proceedings of the European Intelligence and Security Informatics Conference, EISIC 2015*, pp. 149–152, gbr, September 2015.

[10] W. Chen, X. Luo, C. Yin, B. Xiao, M. H. Au, and Y. Tang, "CloudBot: Advanced mobile botnets using ubiquitous cloud technologies," *Pervasive and Mobile Computing*, vol. 41, pp. 270–285, 2017.

[11] Chu, I. Shao, C. Y. Lien et al., "A Survey of Localization in Wireless Sensor Network," *International Journal of Distributed Sensor Networks*, vol. 1, pp. 385–391, 2012.

[12] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, "Wireless sensor network virtualization: A survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 553–576, 2016.

[13] J. Zhao, "Topological properties of secure wireless sensor networks under the q-composite key predistribution scheme with unreliable links," *IEEE/ACM Transactions on Networking*, vol. 25, no. 3, pp. 1789–1802, 2017.

[14] M. Rathee and S. Kumar, "Quantum inspired genetic algorithm for multi-hop energy balanced unequal clustering in wireless sensor networks," in *Proceedings of the 9th International Conference on Contemporary Computing, IC3 2016*, ind, August 2016.

[15] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.

[16] G. Smaragdakis, M. Ibrahim, and A. Bestavros, "SEP: A Stable Election Protocol for clustered heterogeneous wireless sensor networks," in *Proceedings of the International workshop in San Patrignano*, Citeseer, 2004.

[17] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366–379, 2004.

[18] P. G. V. Naranjo, M. Shojafar, H. Mostafaei, Z. Pooranian, and E. Baccarelli, "P-SEP: a prolong stable election routing algorithm for energy-limited heterogeneous fog-supported wireless sensor networks," *The Journal of Supercomputing*, pp. 1–23, 2016.

[19] M. Jan, P. Nanda, M. Usman, and X. He, "PAWN: A payload-based mutual authentication scheme for wireless sensor networks," *Concurrency Computation*, 2016.

[20] G. Geng, G. Xu, M. Zhang, Y. Guo, G. Yang, and W. Cui, "The design of SMS based heterogeneous mobile botnet," *Journal of Computers*, vol. 7, no. 1, pp. 235–243, 2012.

[21] J. Han, Q. Zhao, and M. Zhang, "China's income inequality in the global context," *Perspectives in Science*, vol. 7, pp. 24–29, 2016.

[22] Y. Jiye, J. Shen, H. Ye et al., "Gini coefficient constraint method for making monthly trade schedule of directly dispatched thermal power generation units," in *Proceedings of the 2016*

IEEE PES Asia Pacific Power and Energy Engineering Conference, APPEEC 2016, pp. 2000–2006, chn, October 2016.

[23] Hoque, A. Anisul, and J. A. Clarke, "On variance estimation for a Gini coefficient estimator obtained from complex survey data," *Communications in Statistics Case Studies Data Analysis & Applications*, vol. 1, no. 1, pp. 39–58, 2015.

[24] Z. Jianhua, "An convenient method to calculate Gini coefficient," *Journal of Shanxi Agricultural University: Social Science Edition*, vol. 6, no. 3, pp. 275–278, 2007.

[25] D. Wu, G. Zeng, L. Meng, W. Zhou, and L. Li, "Gini coefficient-based task allocation for multi-robot systems with limited energy resources," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 155–168, 2018.

[26] Z. Fang, J. Zhu, and R. Deng, "Estimating Gini Coefficient Based on Hurun Report and Poverty Line," *Open Journal of Statistics*, vol. 03, no. 03, pp. 167–172, 2013.

[27] F. Teng, J. He, X. Pan, and C. Zhang, "Metric of carbon equity: Carbon Gini index based on historical cumulative emission per capita," *Advances in Climate Change Research*, vol. 2, no. 3, pp. 134–140, 2011.

[28] O. Tremblay, L.-A. Dessaint, and A.-I. Dekkiche, "A generic battery model for the dynamic simulation of hybrid electric vehicles," in *Proceedings of the IEEE Vehicle Power and Propulsion Conference (VPPC '07)*, pp. 284–289, IEEE, Arlington, Va, USA, September 2007.

[29] S. G. R. Prasad, R. Vivek, J. Mungara, and E. J. Sebastian, "NS3 simulation studies for optimized neighbour discovery in 6LoWPAN networks," in *Proceedings of the 3rd IEEE International Symposium on Wireless Systems within the IEEE International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS-SWS 2016*, pp. 15–18, deu, September 2016.

[30] W. Li, X. Ma, J. Wu, K. S. Trivedi, X.-L. Huang, and Q. Liu, "Analytical Model and Performance Evaluation of Long-Term Evolution for Vehicle Safety Services," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 1926–1939, 2017.

[31] C. M. Shepherd, "Design of Primary and Secondary Ceils: II. An Equation Describing Battery Discharge," *Journal of The Electrochemical Society*, vol. 112, no. 7, pp. 657–664, 1965.

[32] Y. Wang, K. Streff, and S. Raman, "Smartphone security challenges," *The Computer Journal*, vol. 45, no. 12, Article ID 6269870, pp. 52–58, 2012.

[33] J. Zhang, R. Perdisci, W. Lee, X. Luo, and U. Sarfraz, "Building a scalable system for stealthy P2P-botnet detection," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 1, pp. 27–38, 2014.

[34] Q. Yan, Y. Zheng, T. Jiang, W. Lou, and Y. T. Hou, "PeerClean: Unveiling peer-to-peer botnets through dynamic group behavior analysis," in *Proceedings of the 34th IEEE Annual Conference on Computer Communications and Networks, IEEE INFOCOM 2015*, pp. 316–324, hkg, May 2015.

[35] L. Liu, G. Yan, X. Zhang, and S. Chen, "VirusMeter: Preventing your cellphone from spies," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 5758, pp. 244–264, 2009.

[36] T. Oh, S. Jadhav, and Y. H. Kim, "Android botnet categorization and family detection based on behavioural and signature data," in *Proceedings of the 6th International Conference on Information and Communication Technology Convergence, ICTC 2015*, pp. 647–652, kor, October 2015.