International Journal of Internet, Broadcasting and Communication Vol.13 No.1 243-248 (2021)
http://dx.doi.org/10.7236/IJIBC.2021.13.1.243

IJIBC 21-1-29

Applying the Nash Equilibrium to Constructing Covert Channel in IoT

Jun-Won Ho

Associate Professor, Department of Information Security, Seoul Women's University, South Korea
jwho@swu.ac.kr

Abstract

Although many different types of covert channels have been suggested in the literature, there are little work in directly applying game theory to building up covert channel. This is because researchers have mainly focused on tailoring game theory for covert channel analysis, identification, and covert channel problem solving. Unlike typical adaptation of game theory to covert channel, we show that game theory can be utilized to establish a new type of covert channel in IoT devices. More specifically, we propose a covert channel that can be constructed by utilizing the Nash Equilibrium with sensor data collected from IoT devices. For covert channel construction, we set random seed to the value of sensor data and make payoff from random number created by running pseudo random number generator with the configured random seed. We generate $I \times J$ $(I \geq 2,\ J \geq 2)$ *matrix game with these generated payoffs and attempt to obtain the Nash Equilibrium. Covert channel construction method is distinctly determined in accordance with whether or not to acquire the Nash Equilibrium.*

Keywords: *Covert Channel, Nash Equilibrium, IoT, Sensor Data*

1. Introduction

As far as convert channel is concerned, game theory [1] has been usually used to analyze covert channels [2-4], to solve covert channel problem [5], and to discern covert channels [6]. Although these applications of game theory have merits of their own, they do not handle with direct use of game theory in the field of covert channel establishment. In order to extend the application field of game theory in terms of covert channel, we devise a covert channel setup technique based on the Nash Equilibrium, which is derived from utilizing sensor data in Internet of Things (IoT) devices.

Indeed, we developed a covert channel creation method that harnesses sensor data from IoT devices [7]. The key idea of our prior work [7] is to put to use the Sequential Probability Ratio Test (SPRT) under the assumption that sensor data can be randomly selected for the purpose of covert channel construction. Our work motivates from seeking other mechanism through which IoT sensor data can be deployed to establish covert channel between IoT devices. To fulfill that motivation, we come up with a new kind of covert channel setup scheme employing the Nash Equilibrium.

Manuscript Received: January. 13, 2021 / Revised: January. 17, 2021 / Accepted: January. 24, 2021
Corresponding Author: jwho@swu.ac.kr
Tel: +82-2-970-5607, Fax: +82-2-970-5981
Associate Professor, Department of Information Security, Seoul Women‘s University, South Korea

In the sections 2 and 3, we first briefly give an introduction to the work that are related to our proposed technique and then give an explanation of the details regarding to our proposed technique. Lastly, we bring to an end of our Nash Equilibrium based covert channel construction scheme.

2. Related Work

From the perspective that covert channel research field has been dissected for an extensive time period, researchers have devised many disparate types of covert channels [7], [8-10], [11], [12-21]. Additionally, game theory is utilized for the purpose of covert channel analysis [2-4], covert channel problem solving [5], covert channel recognition [6]. What crucially marks off our conceived covert channel from the existing covert channels is that the Nash Equilibrium is leveraged to set up covert channel in our constructed covert channel.

3. Covert Channel Creation by Applying the Nash Equilibrium to IoT Sensor Data

For the detailed description of our covert channel creation scheme, we consider two IoT devices *p* and *u.* Furthermore, we consider two player $I \times J$ matrix game such that two players are IoT devices *p* and *u*, $I \geq 2$, $J \geq 2$; Each player has payoffs of 0 and 1. We will use term of IoT device *p* (resp. *u*) with reference to covert channel setup process and use term of player *p* (resp. *u*) with respect to game theory. We assume that both IoT devices *p* and *u* use the same random seed of N_{rs} and the same pseudo random number generator of G_{pr}.

Let us contemplate a case in which IoT device *p* delivers a covert bit to IoT device *u.* Instead of actually sending a covert bit to IoT device *u*, IoT device *p* selects a set of sensor data indicating a covert bit and transmits it to IoT device *u*. Once receiving a set of sensor data from IoT device *p*, IoT device *u* interprets the received set of sensor data as that covert bit.

More specifically, we first denote a series of sensor data continuously measured by IoT device *p* by V_1, V_2, …. V_y ….. ($y \geq 1$). We also denote the number of sensor data in a set of sensor data as S_c. Namely, a set of sensor data is composed of S_c sensor data. The value of S_c is determined in line with the values of I and J: For instance, when $I = J = 2$, we have two player 2×2 matrix game. In this game, player *p* has four payoffs and player *u* also has four payoffs. Thus, 8 payoffs are needed for 2×2 matrix game. In addition, when $I = J = 4$, we have two player 4×4 matrix game. In this game, player *p* has sixteen payoffs and player *u* also has sixteen payoffs. Consequently, 32 payoffs are required for 4×4 matrix game. Finally, when $I = 3$ and $J = 2$, we have two player 3×2 matrix game. In this game, player *p* has six payoffs and player *u* also has six payoffs. Therefore, 12 payoffs are in need for 3×2 matrix game. In general, the number of payoffs required for $I \times J$ matrix game is $2IJ$. We let the number of sensor data in a set of sensor data be equivalent to the number of payoffs for $I \times J$ matrix game, viz. $S_c = 2IJ$ holds.

We extract a payoff from a sensor data V_q ($q \geq 1$) as follows: Player *p* first sets its random seed to the value of sensor data V_q, namely $N_{rs} = V_q$. Player *p* then obtains a random number stretching from 0.0 to 1.0 by running pseudo random number generator G_{pr} with random seed $N_{rs} = V_q$. If that random number is smaller than or equal to $\frac{1}{2}$, a payoff is set to 0. If that random number is larger than $\frac{1}{2}$, a payoff is set to 1. Player *u* also performs this procedure when to extract a payoff from a sensor data.

In $I \times J$ matrix game, the first half out of $2IJ$ payoffs belongs to player *p* and the second half out of $2IJ$ payoffs belongs to player *u*: For example, when $I = J = 2$, 8 payoffs are taken from 8 sensor data; the first 4 payoffs are player *p*'s payoffs and the remaining 4 payoffs are player *u*'s payoffs. In order to associate a covert bit with a payoff, we denote a payoff linking to a covert bit 0 by *0-payoff* and we denote a payoff linking to a covert bit 1 by 1-*payoff.* In $I \times J$ matrix game with $2IJ$ payoffs, IJ payoffs randomly chosen out of $2IJ$

payoffs are marked as 0-payoff and the remaining IJ payoffs are marked as 1-payoff. This distribution information of 0-payoffs and 1-payoffs is installed in both IoT devices *p* and *u*, letting both p and u have the same distribution information of 0-payoffs and 1-payoffs.

We also define *preference-bit* as a bit breaking a tie in the selection process of the Nash Equilibria leading to generation of a covert bit where the Nash Equilibria with 0-payoff and the Nash Equilibria with 1-payoff coexist in $I \times J$ matrix game: If preference-bit is configured to 0, a tie is breached in selection of the Nash Equilibria with 0-payoff, leading to generation of a covert bit 0. If preference-bit is configured to 1, a tie is breached in selection of the Nash Equilibria with 1-payoff, contributing to creation of a covert bit 1.

Now, we describe the process how to make a covert bit by utilizing a set of $2IJ$ sensor data. IoT device *p* gets $2IJ$ payoffs from $2IJ$ sensor data in accordance with the aforementioned payoff extraction procedure and forms a two player $I \times J$ matrix game with $2IJ$ payoffs; player *p* takes the first half of $2IJ$ payoffs and player *u* takes the second half of $2IJ$ payoffs.

A preference-bit is configured to 1 for the first time period E_1, it is then changed to 0 for the second time period E_2. A preference-bit is set to 1 for the third time period E_3, it is then changed to 0 for the fourth time period E_4. This switch between 1 and 0 is repeated for each time period. This preference-bit setup process is performed by both IoT devices *p* and *u*, hence they have the same preference-bit for each time period.

Let us consider the case in which IoT device *p* generates a covert bit 1 with a set of sensor data, F=V_1, V_2, …. V_{2IJ}.

(1) If the Nash Equilibria with 1-payoff exist while the Nash Equilibria with 0-payoff do not exist or if the Nash Equilibria with 1-payoff coexist with the Nash Equilibria with 0-payoff and preference-bit is set to 1, IoT device *p* regards V_1, V_2, …. V_{2IJ} as a covert bit 1.

(2) If any Nash Equilibrium does not exist and preference-bit is configured to 1 and the number of 1s counted in payoffs is not less than the number of 0s counted in payoffs, IoT device *p* then regards V_1, V_2, …. V_{2IJ} as a covert bit 1.

(3) Otherwise, IoT device *p* deletes the last sensor data from the sensor data set F and adds a new sensor data to the sensor data set F as the last element. IoT device *p* then repeats steps (1) ~ (3) with a newly constructed sensor data set F until F is thought of as a covert bit 1.

If IoT device *p* succeeds in getting sensor data set F that is deemed as a covert bit 1, it sends IoT device *u* each sensor data in sensor data set F sequentially.

Let us consider the case in which IoT device *p* generates a covert bit 0 with a set of sensor data, F=V_{c+1}, V_{c+2}, …. V_{c+2IJ}.

(4) If the Nash Equilibria with 0-payoff exist while the Nash Equilibria with 1-payoff do not exist or if the Nash Equilibria with 0-payoff coexist with the Nash Equilibria with 1-payoff and preference-bit is set to 0, IoT device *p* regards V_{c+1}, V_{c+2}, …. V_{c+2IJ} as a covert bit 0.

(5) If any Nash Equilibrium does not exist and preference-bit is configured to 0 and the number of 0s counted in payoffs is not less than the number of 1s counted in payoffs, IoT device *p* then regards V_{c+1}, V_{c+2}, …. V_{c+2IJ} as a covert bit 0.

(6) Otherwise, IoT device *p* deletes the last sensor data from the sensor data set F and adds a new sensor data to the sensor data set F as the last element. IoT device *p* then repeats steps (4) ~ (6) with a newly constructed sensor data set F until F is thought of as a covert bit 0.

If IoT device *p* succeeds in acquiring sensor data set F that is regarded as a covert bit 0, it sends IoT device *u* each sensor data in sensor data set F sequentially.

Upon receiving a set of sensor data from IoT device *p*, IoT device *u* performs the same covet bit generation process as IoT device *p* carried out in order to interpret the received set of sensor data as a covert bit 0 or 1. In this way, the Nash Equilibrium based covert channel is constructed between IoT devices *p* and *u*.

We illustrate how to generate a covert bit with two examples of 2×2 matrix games between player *p* and player *u*, as shown in Figures 1,2.

In Figure 1, we assume that preference-bit is set to 1 and a set of sensor data consists of $V_{20}, V_{21}, V_{22}, V_{23}, V_{24}, V_{25}, V_{26}, V_{27}$. Moreover, we assume that player *p*'s payoffs 0, 0, 0, 1 and player *u*'s payoffs 0, 1, 0, 1 are extracted from $V_{20}, V_{21}, V_{22}, V_{23}$ and $V_{24}, V_{25}, V_{26}, V_{27}$, respectively. Besides, we assume that (0, 0) in the first row of 2×2 matrix in Figure 1, (1, 1) are marked as 1-payoff, and (0, 0) in the second row of 2×2 matrix in Figure 1, (0, 1) are marked as 0-payoff. In 2×2 matrix game in Figure 1, there is one Nash Equilibrium such that player *p* 's payoff is 1 and player *u*'s payoff is 1. Since (1, 1) is indicated as 1-payoff, by step (1), sensor data set $V_{20}, V_{21}, V_{22}, V_{23}, V_{24}, V_{25}, V_{26}, V_{27}$ is regarded as a covert bit 1.

	Player u	
Player p	(0, 0)	(0, 1)
	(0, 0)	(1, 1)

Figure 1. 2×2 Matrix game with the Nash Equilibrium

In Figure 2, we assume that preference-bit is set to 0 and a set of sensor data consists of $V_{30}, V_{31}, V_{32}, V_{33}, V_{34}, V_{35}, V_{36}, V_{37}$. We assume that player *p*'s payoffs 0, 1, 1, 0 and player *u*'s payoffs 1, 0, 0, 1 are extracted from $V_{30}, V_{31}, V_{32}, V_{33}$ and $V_{34}, V_{35}, V_{36}, V_{37}$, respectively. Besides, we assume that (0, 1), (1, 0) placed in the first row of 2×2 matrix in Figure 2 are marked as 1-payoff and (1, 0), (0, 1) placed in the second row of 2×2 matrix in Figure 2 are marked as 0-payoff. There is no Nash Equilibrium in 2×2 matrix game in Figure 2. In this case, preference-bit is configured to 0 and the number of 0s counted in payoffs is equal to the one of 1s counted in payoffs, by step (5), sensor data set $V_{30}, V_{31}, V_{32}, V_{33}, V_{34}, V_{35}, V_{36}, V_{37}$ is regarded as a covert bit 0.

	Player u	
Player p	(0, 1)	(1, 0)
	(1, 0)	(0, 1)

Figure 2. 2×2 Matrix game without the Nash Equilibrium

4. Conclusion

In this paper, we develop a covert channel that can be built by utilizing the Nash Equilibrium: Two player games are obtained from a series of IoT sensor data and the Nash Equilibrium derived from two player games is geared toward covert channel setup between IoT devices.

Acknowledgement

This work was supported by a research grant from Seoul Women′s University (2020-0244).

References

[1] M. Maschler, E. Solan, and S. Zamir, Game Theory, Cambridge University Press, Second Edition 2020.
[2] S. Anand, S. Sengupta and R. Chandramouli, "An Attack-Defense Game Theoretic Analysis of Multi-Band Wireless Covert Timing Networks," 2010 Proceedings IEEE INFOCOM, San Diego, CA, 2010, pp. 1-9.
DOI: https://doi.org/10.1109/INFCOM.2010.5461976.
[3] J. Wang, W. Tang, X. Li and S. Li, "Optimal Strategy in Covert Communication based on Game Theory," 2019 IEEE/CIC International Conference on Communications in China (ICCC), Changchun, China, 2019, pp. 189-194.
DOI: https://doi.org/10.1109/ICCChina.2019.8855950.
[4] Malte Diehl, "Secure Covert Channels in Multiplayer Games," MM&Sec pp. 117-122, Sep. 2008.
DOI: https://doi.org/10.1145/1411328.1411350.
[5] A. S. Leong, D. E. Quevedo, and S. Dey, "A Game-Theoretic Approach to Covert Communications," https://arxiv.org/pdf/1911.00156.pdf.
[6] L. Hélouët, M. Zeitoun, A. Degorre, "Scenarios and Covert Channels: Another Game…," Electronic Notes in Theoretical Computer Science, 119 (2005), pp. 93–116. DOI: https://doi.org/10.1016/j.entcs.2004.07.010.
[7] J. Ho, "Covert Channel Establishment Through the Dynamic Adaptation of the Sequential Probability Ratio Test to Sensor Data in IoT," in IEEE Access, vol. 7, pp. 146093-146107, 2019.
DOI: https://doi.org/10.1109/ACCESS.2019.2945974.
[8] D. Evtyushkin and D. Ponomarev, "Covert Channels through RandomNumber Generator: Mechanisms, Capacity Estimation and Mitigations," In ACM CCS, 2016. DOI: https://doi.org/10.1145/2976749.2978374.
[9] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise (diskfiltration)," In European Symposium on Research in Computer Security, 2017.
DOI: https://doi.org/10.1007/978-3-319-66399-9_6.
[10] K. Block, S. Narain, and G. Noubir, "An Autonomic and Permissionless Android Covert Channel," In ACM WiSec, 2017. DOI: https://doi.org/10.1145/3098243.3098250.
[11] W. Qi, Y. Xu, W. Ding, Y. Jiang, J. Wang, and K. Lu, "Privacy Leaks When You Play Games: A Novel User-Behavior-Based Covert Channel on Smartphones," In ICNP, 2015. DOI: https://doi.org/10.1109/ICNP.2015.40.
[12] P. C. Ritchey and V. J. Rego, "Covert Channels in Combinatorial Games," In DISIO Workshop 2012. DOI: https://doi.org/10.4108/icst.simutools.2012.247733.
[13] R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, "Soundcomber: A Stealthy and Context Aware Sound Trojan for Smartphones," In NDSS, 2011.
[14] T. Heard, D. Johnson, and B. Stackpole, "Exploring a high-capacity covert channel on the Android operating system," In IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015. DOI: https://doi.org/10.1109/IDAACS.2015.7340765.
[15] S. Chandra, Z. Lin, A. Kundu, and L. Khan, "Towards a Systematic Study of the Covert Channel Attacks in Smartphones," In SecureComm, 2014. DOI: https://doi.org/10.1007/978-3-319-23829-6_29.
[16] J. Xiong, L. Xuan, T. Huang, and J. Zhao, "Novel Covert Data Channel in Wireless Sensor Networks Using Compressive Sensing," In Journal of Networks, vol. 7, no. 10, pp. 1523-1529, October 2012. DOI: https://doi.org/10.4304/jnw.7.10.1523-1529.
[17] A. Al-Haiqi, M. Ismail, and R. Nordin, "A New Sensors-Based Covert Channel on Android," In The Scientific World Journal, DOI: https://doi.org/10.1155/2014/969628, 2014.
[18] L. Deshotels, "Inaudible Sound as a Covert Channel in Mobile Devices," In WOOT, 2014. DOI: https://doi.org/10.5555/2671293.2671309.
[19] S. Cabuk, C. Brodley, and C. Shields, "IP covert timing channels: Design and detection," In ACM Conference on Computer and Communications Security, October 2004. DOI: https://doi.org/10.1145/1030083.1030108.

[20] S. Li and A. Ephremides, "A Network Layer Covert Channel in Ad-hoc Wireless Networks," In IEEE SECON, 2004. DOI: https://doi.org/ 10.1109/SAHCN.2004.1381906.
[21] C. Maurice, C. Neumann, O. Heen, and A. Francillon, "C5: cross-cores cache covert channel," In Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, 2015. DOI: https://doi.org/10.1007/978-3-319-20550-2_3.