2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID)

Security Assessment of Microfluidic Fully-Programmable-Valve-Array Biochips

Mohammed Shayan*, Sukanta Bhattacharjee†, Yong-Ak Song*†, Krishnendu Chakrabarty‡, and Ramesh Karri*
*New York University, †New York University Abu Dhabi, ‡Duke University
Email: mos283@nyu.edu, sb6538@nyu.edu, rafael.song@nyu.edu, krish@ee.duke.edu, rkarri@nyu.edu

***Abstract*—The fully-programmable-valve-array (FPVA) is a general-purpose programmable flow-based microfluidic platform, akin to the VLSI field-programmable gate array (FPGA). FPVAs are dynamically reconfigurable and hence are suitable in a broad spectrum of applications involving immunoassays and cell analysis. Since these applications are safety-critical, addressing security concerns is vital for the success and adoption of FPVAs. This study evaluates the security of FPVA biochips. We show that FPVAs are vulnerable to *malicious operations* similar to digital and flow-based microfluidic biochips. FPVAs are further prone to new classes of attacks - *tunneling* and deliberate *aging*. The study establishes security metrics and describes possible attacks on real-life bioassays.**

I. Introduction

Microfluidic technologies are a major driving force in miniaturizing laboratory-based biochemical protocols. They enable the implementation of basic fluidic operations into a tiny chip a few squares centimeter. These technologies are referred to as lab-on-a-chip (LoC) or biochip. Biochips are revolutionizing point-of-care diagnostics [1], DNA analysis [2], drug development [3], and bio-medical analysis [4].

A biochip platform enables microfluidic operations such as dispensing, mixing, and splitting. These, in turn, can be used to build more complex protocols for biochemical analysis [9]. [5]. Several biochip platforms have been proposed such as digital microfluidic biochip (DMFB) or continuous flow-based microfluidic biochip (CFMB). DMFB offers a general-purpose programmable fluidic platform in which discrete fluid droplets can be manipulated through electrical actuations [6]. Whereas, CFMBs are based on the continuous fluid flow through micro-channels and lack programmability.

CFMBs use pressure-driven micro-valves to control the fluid flow in a network of micro-channels. CFMBs are created for individual applications, similar to application-specific-ICs (ASICs). However, a programmable microfluidic device, analogous to an FPGA in VLSI, is desirable to reduce the cost of design/production. This has lead to the development of the Fully Programmable Valve Array (FPVA) [7].

An FPVA biochip is a two-dimensional array of fluid chambers. Each chamber in an FPVA is surrounded by up to four independently addressable valves to implement programmable interconnection of chambers (Fig. 1). One can configure valves to create an arbitrary channel network connecting the desired chambers. The chambers are used as vessels to hold and mix reagents [8]. To scale down the number of I/O pins, FPVAs use a multiplexer to control each of the valves. This offers a versatile programmable platform to implement a broad range of bioassays [7].

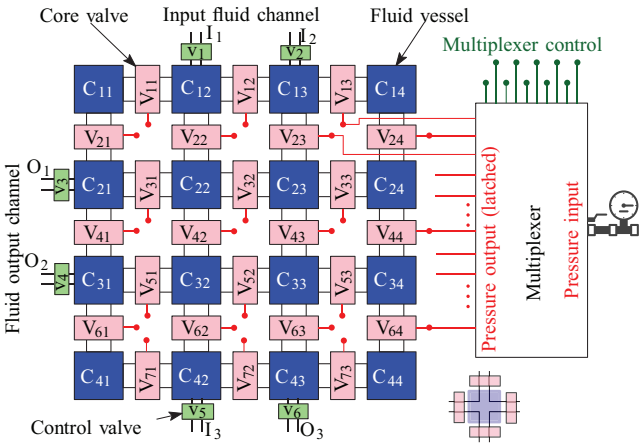

Fig. 1: Schematic of a fully programmable valve array biochip.

Security and trustworthiness of biochips are important as they are adopted in safety-critical applications like point-of-care diagnosis, drug discovery, and military applications. Recent works have shown that microfluidic biochip platforms are susceptible to attacks [9], [10]. FPVAs perform fluid operations similar to the CFMBs while offering programmability similar to digital microfluidic biochips (DMFBs). Thus, FPVAs are susceptible to attacks that apply to digital and flow-based microfluidic biochips. In this paper, we evaluate the security ramifications of the FPVA biochip by:

- showing that FPVAs are prone to malicious operations.
- presenting FPVA-specific tunneling and lifetime reduction attacks.
- launching simulated attacks on real-life cell-culture and immunoassay case studies implemented on the FPVA.
- defining security metrics to capture stealthiness of the attacks and susceptibility of FPVA implementations to the attacks.

The organization of the rest of this paper is as follows. Section II provides relevant background on CMFBs, FPVA platform, and biochip security. In Section III, we present the threat model and analyze various security threats to FPVA biochips. In Section IV, we present attacks on real-life bioassays. In Section V, we define the security metrics that capture the stealthiness of the attack, and conclude in Section VI.

2380-6923/19/$31.00 ©2019 IEEE
DOI 10.1109/VLSID.2019.00053

II. Background

In this section, we present the relevant background related to the continuous-flow microfluidic platform, FPVA, and recent work on microfluidic security.

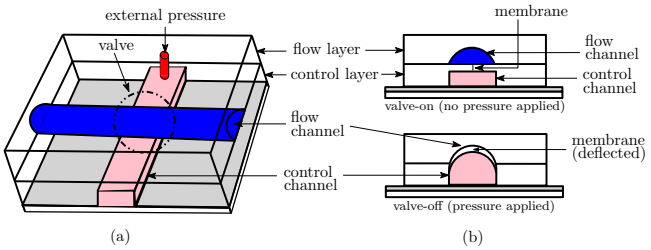

Fig. 2: Schematic of a two-layer microfluidic device: (a) top view and (b) cross-sectional view of valve states.

A. Continuous-Flow-Microfluidic Biochips

A CFMB consists of two layers of permanently etched micro-channels called the flow and the control layer, as shown in Fig. 2(a). At the intersection of the two layers, a "valve" is formed that can be controlled by an external pressure source. When the valve is pressurized, the flexible membrane of the control layer deflects deep into the flow layer blocking the fluid flow (ref. Fig. 2(b)). By controlling the opening/closing of the valves, complex fluid handling operations can be performed such as mixing, incubation, transportation, and storage [11].

B. Fully Programmable Valve-Array (FPVA) Biochip

Fig. 1 shows the primary building blocks of an FPVA biochip. *Fluid chambers* act as stop-gaps during channel formation and as temporary storage for the mix and incubate operations. The *core valves* surrounding these chambers can be individually controlled (open/close) by applying pressure inputs. A *multiplexer* is used to trim the number of pressure inputs in the FPVA biochip. *The control valves* control the flow of fluids into the flow network through the I/O channels. *External solenoid valves* guide the pressure discharge to the control valves and the multiplexer controls.

The implementation of a bioassay on an FPVA requires transforming each assay operation into one or more fluid operations supported by the FPVA [7]. Fig. 3 illustrates the design flow of a bioassay on the FPVA platform. Loading an input fluid is achieved by setting up a flow channel between the input fluid port to an output port and forcing the fluid through this channel. The flow channel is set up by regulating (i.e., opening/closing) the valves through the multiplexer control lines, which are in turn actuated through the solenoid switches by an external micro-controller.

A biochip may have manufacturing defects, which might contribute to operation-time failures. To expose such failures and to facilitate error recovery, the biochip cyber-physical system incorporates one or more sensors [12]. A CCD camera captures the images of a chamber to determine the presence/absence of fluid [12]. Pressure sensors at the flow I/O ports reveal the presence/absence of flow [13]. The feedback from the sensors allows for a robust and reliable assay implementation.

C. Previous Work

Previous work has shown that DMFBs are susceptible to operational attacks such as denial-of-service and result manipulation [14]. IP security threats in the supply chain due to the distributed design flow include overbuilding, reverse engineering, and counterfeiting [15], [14]. IP protection schemes have been proposed using physical unclonable functions [15] and bioassay locking [16]. One of the early countermeasures for tamper detection used randomized checkpoints [9]. To overcome the computational limitations of randomized checkpoints, a tamper-resistant pin mapping technique was proposed. This approach uses pin-constrained DMFB to make the stealthy modification of actuation sequence difficult [17]. Even with these measures, an attacker can escape detection with some probability. A micro-electrode-dot-array (MEDA) platform with a fine-grained integrated sensor modules offers strong proof of security [18], [19]. A threat model for CFMBs is discussed in [10]. The security solutions for DMFBs cannot be readily applied to CFMBs due to the inherent differences in the technologies.

III. Security Assessment

In this section, we present the threat model and describe attack scenarios that arise from the threat model.

A. Threat Model

The threat model elaborates the following six components:
Attacker: An attacker can be far away or be in proximity of the biochip. A remote attacker can be a competitor attempting to sabotage the reputation of the biochip designer. The proximity attacker can be an insider or an enemy trying to harm the end-user by denying service or manipulating biochip results.
Attack surface: The biochip is connected to the network for software updates and online processing of the results. A remote attacker can compromise the biochip controller software via the network interface. The proximity attacker can compromise the biochip results by inducing faults in the biochip.
Attack methods: A remote attacker can gain administrator credentials using malware such as Stuxnet [20]. The attacker reads and alters the actuation sequence. The proximity attacker can expose the valves to excess pressure or subject them to high-frequency actuations, deforming the valves and failing the biochip.
Assay monitoring: The state of the biochip can be monitored using sensors such as CCD camera and pressure sensors. Due to the practical constraints of a pattern-matching algorithm, the CCD camera can monitor a limited number of chambers in a cycle [9]. The pressure sensors monitor the presence of fluid at the output ports. This is used to determine the time taken by the fluid flow (*flow time*), which is a function of the fluid routing path.

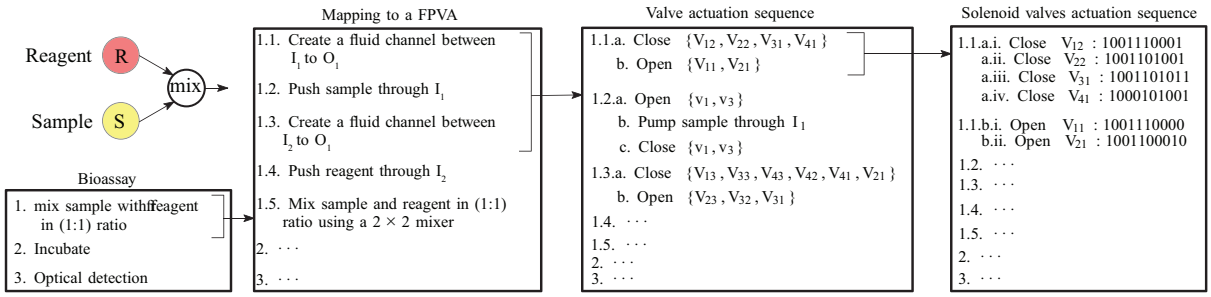

Fig. 3: An FPVA design flow consists of the mapping of bioassay description to fluidic operations on an FPVA biochip, which in turn maps to the core valve actuations, which further correspond to the solenoid actuations.

Attack constraints: The attacker aims to manipulate the results of the biochip in a stealthy and untraceable way. To do this, the attacker has to ensure that:

- The number of chambers whose states differ from the golden state, referred to as *deviant chambers*, are minimal (ideally zero). The number of deviant chambers increases the probability of detection by CCD camera sensors.
- The real-time fluid flow time should be identical to the expected golden flow time. The pressure sensors can detect a change in the flow time.

Trusted actors: The biochip designer is the defender. The defender trusts the biochip platform as it has been tested for manufacturing defects [13]. The end-user is also trusted.

B. Attack Classification

Programmable biochips are susceptible to tampering of the high-level control program and the low-level actuation sequence. These are called "actuation tampering" attacks [9], [21]. The actuation sequence encodes a sequence of fluidic operations such as dispense, transport, and mixing. Tampering of actuation sequence impacts the fluidic operations on the biochip. For an FPVA, we define three types of tampering: 1) **Transpose attack** modifies golden operations, e.g., the mixing ratio or swapping of flows. 2) **Tunneling attack** inserts extra actuations to create a new flow channels to dispense malicious fluids or contaminate flows. 3) **Aging attack** subjects the valves that are not participating in certain bioassay stage(s) to additional actuations. This reduces the biochip lifetime by failing these valves.

C. Attack Space

To demonstrate the consequences of a modified operation, let us consider an attack that modifies a dispense-mix operation:

Example 1. *Consider the bioassay described in Fig. 3, where the sample and the reagent are mixed in a (1:1) ratio on the FPVA of Fig. 1. The reagent (sample) is loaded by forming a fluid path from I_2 (I_1) to O_1 through chambers C_{21}, C_{22} (C_{11}, C_{12}). These are mixed in a 2×2 mixer, as shown in Figs. 4(a)-(c). Figs. 4(a)-(f) show the relevant segments of the FPVA in Fig. 1. One can tamper with the bioassay by mixing the sample and the reagent in (1:3) ratio (Figs. 4(c)-(e)). This can be done by altering the reagent path from I_2 to O_1 (Fig. 4(e)) in the mapping program, to pass through chambers C_{12}, C_{22}, C_{21}. The sample is loaded into chamber C_{11}. This causes an erroneous reaction and a wrong result. Pressure sensors at the output O_1 cannot catch this since the route length and the flow time are not modified.*

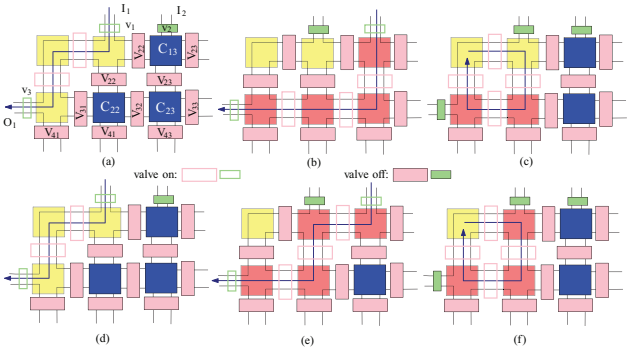

Fig. 4: Golden assay: (a) pushing a sample through I_1 to O_1, (b) pushing a reagent through I_2 to O_1, and (c) mixing the two fluids in (1:1) ratio using a 2×2 mixer. Tampered assay: (d) pushing a sample from I_1 to O_1, (e) pushing a reagent through a maliciously modified flow channel from I_2 to O_1, and (f) mixing the two fluids in (1:3) ratio using a 2×2 mixer.

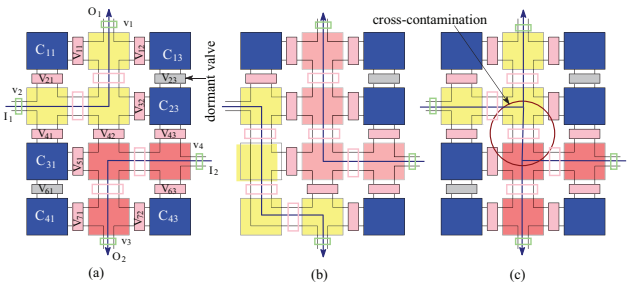

Fig. 5: (a) A FPVA routing two fluids. (b) A transpose attack. (c) A tunneling attack. Grey valves are susceptible to aging.

Transpose attack — Similar to modifying dispense and mix operations, one can manipulate the channels such that the

endpoints of two different flows are swapped as demonstrated in Example 2. Such attacks involving modifying the existing operations are called transpose attacks.

Example 2. *Consider the routing of two flows through two distinct channels between the same start and end points, as shown in Fig. 5(a). One can maneuver the valves to swap the endpoints. This is done by inverting the state of valves* V_{31}, V_{41}, V_{42}, V_{61}, V_{62}, V_{71} *in Fig. 5(b). Swapping increases the flow time for each flow by opening an extra valve relative to the original flows. The state of the chambers* C_{14}, C_{13} *in Fig. 5(b) are different from the golden flows in Fig. 5(a).*

Tunneling attack — Additional actuations can be inserted in the implementation leading to the formation of new channels between the existing channels. This way, two flows get in contact with each other, causing contamination. The insertion of new operations is called tunneling.

Example 3. *Consider the tunneling attack in Fig. 5(c). The attacker contaminates the flows by inverting the state of one of the shaded valves in Fig. 5(c). Opening a valve leads to mixing of the two flows, leading to contamination. Tunneling does not alter the flow time of the fluids as one can open a new valve after the channel is set up. The sensor readings of the chambers in Fig. 5(c) will be similar to the expected golden readings in Fig. 5(a). Therefore, it does not raise an alarm.*

Aging can degrade the lifetime of the FPVA by causing extra actuations in core valves and solenoid valves. An attacker can actuate in valves that are dormant - either temporarily or throughout a bioassay implementation. The core valves of FPVA biochip are made of a rubber-like material that has a short lifespan. These can be operated reliably only a few thousand times. A design for reliability approach minimizes the number of valve actuations for longer life [8]. An attacker can toggle the dormant valves, which escapes sensor detection.

Example 4. *The FPVA in Fig. 5(a) has 17 valves. Among them, the status of the two valves shaded in grey does not affect the assay implementation. The attacker can manipulate the status of these valves continuously, reducing the lifetime of the biochip and rendering it useless for (re)use for either other stages of the same bioassay or another bioassay. This does not change the flow time of each fluid as the extra valves can be toggled after the requisite channel formations. Further, status of all the chambers is the same as that of the golden.*

Solenoids are used to actuate the core valves through the multiplexer. To activate a core valve in an FPVA, one has to actuate the solenoid valves numerous times. The number of solenoid actuations depends on the order in which the valves are actuated and the addresses of the valves. In the example in Fig. 3, the opening of each core valve requires two-to-ten actuations of the solenoids. One may modify the actuation order of the core valves to increase the total number of solenoid actuations. This causes high-frequency activity in the solenoid valve, which in turn increases heat dissipation. This heat-induced stress ultimately breaks the solenoid valves [22].

IV. Case Study: Attacks on FPVA Cell Culture

We demonstrate attacks on the multiplexed cell culture implementation on an FPVA platform. We consider an 8×8 FPVA biochip that implements four independent cell culture experiments in duplicate (Fig. 7), i.e., eight experiments in total [7]. A brief description of the cell culture protocol is given in the following steps:

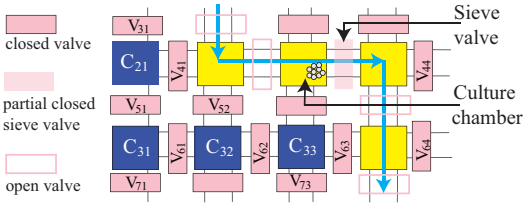

Fig. 6: Part of an FPVA loads cells in the culture chamber by trapping the cells in the chamber adjacent to the sieve valve.

1) A yeast cell suspension is introduced through a partially closed *sieve* valve. As a result, cells are trapped in the *culture chambers* (Fig. 6).
2) Nutrients are supplied to the culture chambers in two alternating steps, forming the *perfusion* cycle: (a) Allow diffusion of nutrients between the culture chamber and the adjacent perfusion channel (Fig. 7). (b) Exchange the medium in the perfusion channel while the culture chambers are closed to prevent cross-talk (Fig. 7).
3) Cell culture experiments are duplicated for experimenting with inducing and non-inducing conditions under the control of the PHO5 promoter, which is induced in the absence of inorganic phosphate. The transcription of PHO5 is regulated in response to the level of inorganic phosphate present in the growth medium [23]. The inducing and non-inducing condition is maintained by the dotted red path and the green path in Fig. 7(b) and Fig. 7(a), respectively.
4) Fluorescence detection is done in all culture chambers.

A. Transpose attack

In one half of the perfusion cycle, the medium is replenished in one section, while in the other section, chambers are perfused with nutrients. This is alternated, forming the perfusion cycle, as shown in Figs. 7(a)-(b). The period of the cycle is $1\,\text{min}$, which implies that activity in each section switches between medium-replenishing and nutrient-perfusion after every $30\,\text{sec}$. An attacker can change the rate of fluid replacement ($1\,\text{min}$), which in turn changes the perfusion cycle period ($2\,\text{min}$), which affects the cell growth in the chambers [4]. This does not change the flow time because the red and green paths have equivalent path lengths. However, the number of deviant chambers between Figs. 7(a)-(b) is 14, which could lead to detection by a CCD camera.

B. Tunneling attack

The chambers are isolated when the side valves V_{42}, V_{62} in Fig. 7(d) are opened to diffuse nutrients. An attacker can open

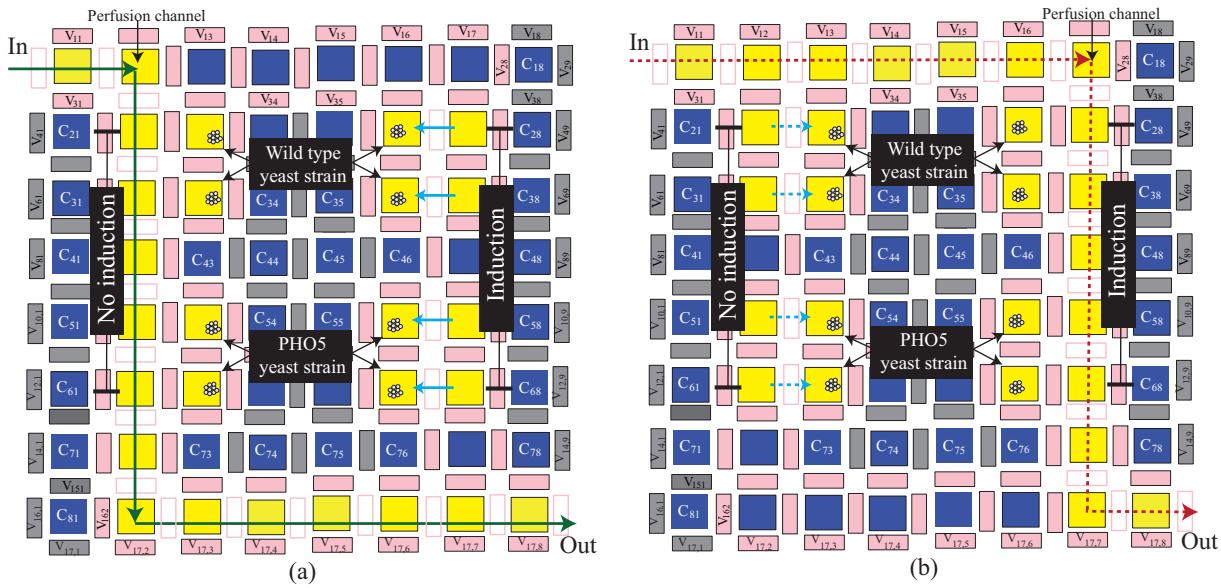

Fig. 7: An 8×8 FPVA performing 8 cell culture experiments. The growth condition in the chambers to the right (left) side is induced (not-induced) by absence (presence) of inorganic phosphate. (a) In the left, perfusion channel (solid green) is loaded without induction and in the right, perfusion of nutrients (solid blue) is allowed with induction. (b) In the left, perfusion of nutrients (dotted blue) is allowed without induction and in the right, perfusion channel (dotted red) is loaded with induction.

valves to establish a path through either chambers (C_{34} and C_{35}) or (C_{54} and C_{55}) to contaminate the growth conditions of induction and non-induction. Further, the attacker can open valves to form a path through one chamber: either C_{43} or C_{46} to introduce cross-talk between two different yeast strains. This leads to a wrong result.

C. Aging attack

In the assay implementation, there are 44 unused valves, shown in grey in Fig. 7(a). Further, there are valves that are temporarily unused in various stages of assay implementation. For example, valves V_{34}, V_{35} are used in one half of perfusion cycle (Fig. 7(a)) and are dormant in the other half (Fig. 7(b)). These can be switched on and off without getting detected by the CCD camera. Opening or closing of a valve takes 100 ms. Therefore, in 9 hours of culturing, a valve (one of the 44 dormant valves) can be actuated a maximum of 4500 times. This can severely hamper the lifetime of the biochip.

V. Security Metrics

We next define metrics to capture the stealthiness of an attack and susceptibility of implementation to attacks.

A. Evading Pressure Sensor

An attack on FPVA can increase the flow time of a fluid as monitored at the output port. For example, the transpose attack in Fig. 5(b) increases the source-to-sink path length of each fluid by one chamber compared to the original path length. A difference in flow time can be detected by the pressure sensor at the output. To avoid this the difference between real-time flow time and golden flow time, denoted by ΔF, should be zero. In the transpose attack described in the case study of cell culture, this condition is met ($\Delta F = 0$) because there is no change in flow time.

B. Evading CCD Camera

Let there be 'T' chambers in an FPVA biochip. Assume that 'k' random chambers are monitored by the CCD camera in a given cycle since random monitoring offers better security in a resource-constrained system [9]. The probability that a random chamber is being monitored is given by 'coverage ratio' $\frac{k}{T}$. The probability that a random chamber is overlooked i.e., the probability of evasion P_e is given by the equation.

$$P_e = \left(1 - \frac{k}{T}\right) \tag{1}$$

The attacker's objective is to escape detection by the CCD camera - which checks whether the chambers are filled or not. So, the attacker wants to minimize the number of chambers whose status is different from the golden state. An ideal attack is one where there is no change in the sensor readings of the state of any chamber, as shown in Examples 3 and 4. We define an attack metric called "delta N" (ΔN). Let Boolean variables S_i and S_i^g be the real-time and golden state of i^{th} chamber, where '0' denotes an empty chamber. and '1' denotes a filled chamber. Then,

$$\Delta N = \sum_i |S_i - S_i^g| \tag{2}$$

If there are ΔN deviant chambers in a cycle, the probability

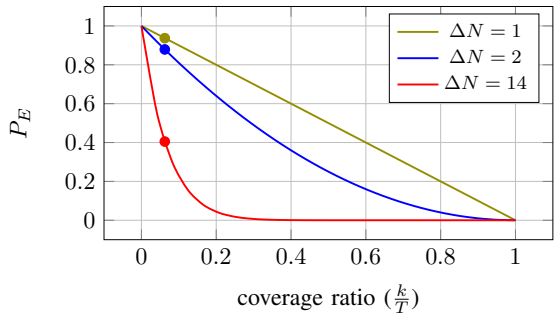

Fig. 8: Probability of evasion (P_E) decreases with increase in the deviant chambers (ΔN) for a given camera coverage ($\frac{k}{T}$).

that all of them go undetected is given as follows.

$$P_E = \left(1 - \frac{k}{T}\right)^{\Delta N} \tag{3}$$

Contamination of the growth condition (induction/non-induction) in the cell culture case study leads to two deviant chambers i.e., $\Delta N = 2$. The yeast strain cross contamination attack leads to one deviant chamber i.e., $\Delta N = 1$ and transpose attack leads to $\Delta N = 14$. Using this information. we plot the probability of evasion for a varying coverage ($\frac{k}{T}$), as shown in Fig 8. Let the cycle time be 100 milliseconds, same as the time required to open/close a valve. A CCD camera requires 238 microseconds to monitor one chamber [9]. Therefore, it can observe four chambers in this cycle time of 100 milliseconds. This implies that $k = 4$. From Equation 3, $P(E) = 0.937$, 0.879, and 0.405 for $\Delta N = 1$, 2, and 14 respectively, as shown in Fig. 8.

C. Results

We performed a similar analysis on an immunoassay implementation on the 8×8 FPVA [7]. The results of the analysis are shown in Table I. The high probability of evasion ($P(E) \sim 1$) confirms the stealthy nature of the attacks. Due to the proximity of different fluid channel routes, the flow time deviation (ΔF) in the tunneling attacks is zero. The aging attack cannot be detected because it operates on the dormant parts of the FPVA.

TABLE I: Attack metrics for real-life assays.

Benchmark	**Attack**	ΔF	ΔN	P_E for $k = 4$
Cell culture	Transpose	0	1	0.405
	Tunneling	0	1	0.937
	Aging	0	0	1
Immunoassay	Transpose	2	1	0.937
	Tunneling	0	0	1
	Aging	0	0	1

VI. Conclusion

An FPVA biochip facilitates one to create arbitrary channels on the biochip dynamically. We show that one can abuse this capability to launch stealthy attacks such as transposing, tunneling, and deliberate aging. We highlight the practicality of the attacks by implementing them on real-life bioassays and measure the stealth and susceptibility security metrics. The results show that the bioassay implementation on FPVAs is prone to attacks that elude detection. This highlights the need for security aware bioassay synthesis and biochip system designs. We anticipate that our work will motivate further exploration of FPVA security.

Acknowledgment

This research is supported in part by the Army Research Office under grant number W911NF-17-1-0320, NSF Award numbers CNS-1833622 and CNS-1833624, NYU Center for Cyber Security (CCS), and CCS-AD.

References

[1] A. H. C. Ng *et al.*, "Immunoassays in microfluidic systems," *Anal. Bioanal.Chem.*, vol. 397, no. 3, pp. 991–1007, Jun 2010.
[2] M. Ibrahim *et al.*, "Synthesis of cyberphysical digital-microfluidic biochips for real-time quantitative analysis," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 36, no. 5, pp. 733–746, 2017.
[3] (2018) Rapid test helps with administering the "correct" drug. [Online]. Available: https://www.technologynetworks.com/diagnostics/news/rapid-test-helps-with-administering-the-correct-drug-298565
[4] F. Meuwly *et al.*, "Optimization of the medium perfusion rate in a packed-bed bioreactor charged with cho cells," *Cytotechnology*, vol. 46, no. 1, pp. 37–47, Sep 2004.
[5] R. B. Fair, "Digital microfluidics: is a true lab-on-a-chip possible?" *Microfluid Nanofluid*, vol. 3, no. 3, pp. 245–281, 2007.
[6] N. Vergauwe *et al.*, "A versatile electrowetting-based digital microfluidic platform for quantitative homogeneous and heterogeneous bio-assays," *J. Micromech. Microeng.*, vol. 21, no. 5, p. 054026, 2011.
[7] L. M. Fidalgo *et al.*, "A software-programmable microfluidic device for automated biology," *Lab Chip*, vol. 11, pp. 1612–1619, 2011.
[8] T.-M. Tseng *et al.*, "Reliability-aware synthesis for flow-based microfluidic biochips by dynamic-device mapping," in *Design Autom. Conf.*, 2015, pp. 1–6.
[9] J. Tang *et al.*, "Secure randomized checkpointing for digital microfluidic biochips," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 6, pp. 1119–11 132, 2018.
[10] ——, "Security implications of cyberphysical flow-based microfluidic biochips," in *IEEE Asian Test Symp.*, 2017, pp. 115–120.
[11] A. Grimmer *et al.*, "Close-to-optimal placement and routing for continuous-flow microfluidic biochips," in *Asia and South Pacific Design Automation Conference*, 2017, pp. 530–535.
[12] Z. Li *et al.*, "Efficient and adaptive error recovery in a micro-electrode-dot-array digital microfluidic biochip," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 99, 2017.
[13] C. Liu *et al.*, "Testing microfluidic fully programmable valve arrays (FPVAs)," in *Design, Auto. Test in Europe*, 2017, pp. 91–96.
[14] S. S. Ali *et al.*, "Microfluidic encryption of on-chip biochemical assays," in *IEEE Biomed. Circuits Syst. Conf.*, 2016, pp. 152–155.
[15] C.-W. Hsieh *et al.*, "Piracy prevention of digital microfluidic biochips," in *Asia and South Pacific Des. Autom. Conf.*, 2017, pp. 512–517.
[16] S. Bhattacharjee *et al.*, "Locking of biochemical assays for digital microfluidic biochips," in *IEEE European Test Symp.*, 2018, pp. 1–6.
[17] J. Tang *et al.*, "Tamper-resistant pin-constrained digital microfluidic biochips," in *Proc. Design Auto. Conf.*, 2018, pp. 67:1–67:6.
[18] S. Mohammed *et al.*, "Security assessment of micro-electrode-dot-array biochips," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, 2018 (to appear).
[19] ——, "Shadow attacks on MEDA biochips," in *Intl. Conf. Comput. Aided Design*, 2018 (to appear).
[20] R. Langner, "Stuxnet: dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, 2011.
[21] S. S. Ali *et al.*, "Security implications of cyberphysical digital microfluidic biochips," in *Proc. IEEE Intl. Conf. Computer Design*, 2015, pp. 483–486.
[22] J. Mercer, "Reliability of solenoid valves," *Institution of Mechanical Engg. conf. proceedings*, 1969.
[23] H. Rudolph *et al.*, "The yeast PHO5 promoter: phosphate-control elements and sequences mediating mRNA start-site selection," *Proc. Natl. Acad. Sci. USA*, vol. 84, no. 5, pp. 1340–1344, 1987.