Security Implications of Cyberphysical Digital Microfluidic Biochips

Sk Subidh Ali[†], Mohamed Ibrahim[‡], Ozgur Sinanoglu[†], Krishnendu Chakrabarty[‡], and Ramesh Karri[↑]
[†]New York University Abu Dhabi, [‡]Duke University, [↑]New York University New York

***Abstract*—A digital microfluidic biochip (DMFB) is an emerging technology that enables miniaturized analysis systems for point-of-care clinical diagnostics, DNA sequencing, and environmental monitoring. A DMFB reduces the rate of sample and reagent consumption, and automates the analysis of assays. In this paper, we highlight the security vulnerabilities of DMFBs by identifying two potential attacks on a DMFB that performs enzymatic glucose assay on serum. In the first attack, the attacker adjusts the concentration of the glucose sample and thereby modifies the final result. In the second attack, the calibration curve of the assay operation is maliciously modified in order to make it deviate from the nominal/golden calibration curve. We demonstrate these attacks using a digital microfluidics synthesis simulator. The results show that the attacks are stealthy as they do not result in any noticeable change in the DMFB synthesis**

I. Introduction

Digital microfluidics is a lab-on-a-chip technology that enables miniaturized analysis systems for biochemical applications such as point-of-care clinical diagnostics [1] and DNA sequencing [2]. Many techniques have been developed to address various aspects of automated design and optimization of digital microfluidic biochips (DMFBs) [3]. These includes architectural-level synthesis [4], module placement [5], and droplet routing [6]. An equally important aspect of DMFB design is the integration of sensors, a necessity for the realization of physical-aware control systems [7]. The progress of fluidic sample preparation and chemical reactions can be monitored using integrated waveguides [8], capacitive sensors [9], or CCD cameras [10]. The sensor readouts can be used to dynamically reconfigure DMFB operations in real-time, enabling fault-tolerant assay execution on a DMFB [11].

Despite the advantages offered by digital microfluidics for clinical diagnosis, immunoassays and DNA sequencing process, there has been no study on the potential security implications of DMFBs. Recent cyberattacks have revealed the vulnerabilities of automated systems [12], [13], [14], [14].

A fully automated DMFB is typically controlled by a computer, which applies a set of control sequences on the input pads of a DMFB. If an attacker gets control of the DMFB, he/she can maliciously modify the assay operation and manipulates the assay outcome. The attacker could be a person who wants to jeopardize another person's health by manipulating his/her clinical diagnostic results. An organization can be adversarial and can disrupt the products from a specific vendor. In this paper, we demonstrate attacks on a fully automated DMFB performing enzymatic glucose assay on serum and show how an attacker can control the assay operations of a DMFB and can manipulate the assay outcomes.

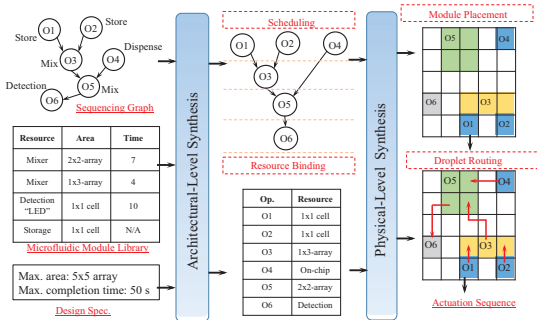

Fig. 1: A CAD flow for automated design of a DMFB.

II. Background

A typical DMFB consists of a two-dimensional electrode array, on-chip reservoirs, and sensors. A basic cell in a DMFB consists of two parallel plates. The electrode surface is coated with a thin layer of an insulator such as Paralyene C [1]. Both plates are also coated with a thin film to provide a hydrophobic platform that is necessary for smooth droplet actuation. When an electric field is applied between the parallel plates, the interfacial surface energies are modulated and an electrical double layer is created, which in turn alters the apparent contact angle of a conductive liquid droplet that is in contact with the hydrophobic surface. The change in the contact angle, in turn, influences the wetting behavior of the droplet.

Using DMFB CAD tools a high-level assay specification is converted into an actuation sequence, which is an executable program that runs the DMFB. Fig. 1 highlights the overall CAD flow for DMFBs. First the high-level assay specification is converted into a *sequencing graph* $G = (V, E)$, where a node $v \in V$ corresponds to a fluid-handling operation (e.g., dispensing, mixing, dilution, and detection) and an edge $e \in E$ between two nodes $(v1, v2)$ represents the dependency between them. The sequencing graph represents the starting point for the CAD flow besides the application specifications and the module library of the DMFB. The CAD flow generates the electrode-actuation sequences, which store the droplet control information at each time step. The status of an individual control signal at a certain time-step is "1" (actuated), "0" (not actuated), or "X" (don't-care).

III. Attacks on a DMFB

We highlight attacks based on the adversary's control over the DMFB. Let us assume that the attacker takes control of the

978-1-4673-7166-7/15/$31.00 ©2015 IEEE

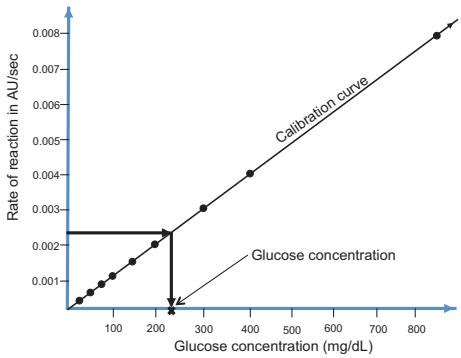

Fig. 2: Glucose calibration curve.

DMFB either by breaking into the system and gaining access to the controller or by forming a malicious nexus with one of the users of the system (the attacker himself could be a user). The attacker can tamper with the normal execution of a DMFB and alter its outcome. We also assume that the attacker:

1) knows about the assay operation in detail.
2) knows the CAD tools used. He/she could be a user or may purchase the tool and become familiar with it.
3) does not have control over the DMFB results, such as the sensor outputs. Hence, he/she cannot directly tamper with the results generated by the DMFB.

A. Attack on-vitro measurement of glucose

We use in-vitro measurement of glucose, which is a widely used clinical-diagnosis method for diabetes mellitus (hyperglycemia), as a case study. According to data from the Centers for Disease Prevention and Control (CDC), in 2011 alone, 22.9 million people in the US were diagnosed with diabetes [15]. A diabetic patient has to undergo regular glucose test for proper monitoring. Based on the blood glucose level, the amount of insulin to be injected into the patient is determined.

The bench-top sequence for this test, known as *glucose assay*, is realized on a DMFB as a colorimetric assay in which the color change is detected using an absorbance measurement system consisting of a light emitting diode and a photodiode [16]. This assay measures the glucose concentration level in a blood sample by constructing the glucose *calibration curve* (Fig. 2) via serial dilutions of the standard glucose solution. The X-axis represents the different concentrations formed by these dilutions (in mg/dL) and the Y-axis represents the rate of reaction quantified by the change in absorbance degree reported as AU/sec (absorbance unit per second). Using this curve, the concentration of the glucose sample under test is estimated by interpolation. As shown in Fig. 2, the reaction rate of the sample is a point on the Y-axis and the corresponding point on the X-axis is the sample concentration.

B. Attack Model

The attacker can manipulate the assay either by changing the concentration of the sample or by causing deviations in the calibration curve. Using these two assay manipulation techniques we demonstrate two potential attacks on a DMFB. To demonstrate the attacks, we consider the following three scenarios:

1) **Golden execution:** No attack is carried out.
2) **Attack 1:** The concentration of the glucose sample is modified via a malicious dilution operation.
3) **Attack 2:** The calibration curve is manipulated by tampering with the concentrations of the glucose solution during calibration.

1) Golden execution: The sequencing graph shown in Fig. 3 describes the golden execution for the glucose assay. The sequencing graph consists of four independent reaction chains 1, 2, 3, and 4, measuring the rate of reaction for a blank/buffer droplet (reaction chain 1), glucose solution concentrations 800, 400, 200, 100, 50, 25 mg/dL (reaction chain 2), glucose solution concentrations 300, 150, 75 mg/dL (reaction chain 4), and the glucose sample (reaction chain 3). The calibration curve is generated using the reaction chains 1, 2, and 4, while the reaction chain 3 is used to determine the glucose concentration of the sample.

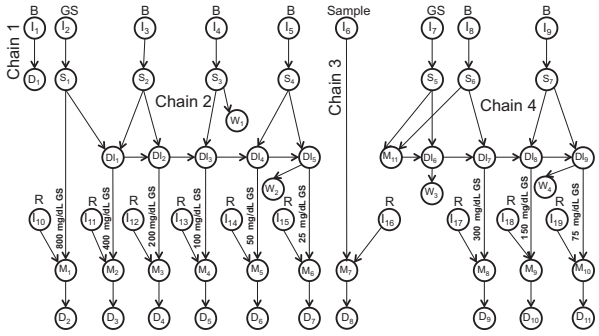

Fig. 3: Golden execution: B is the $1.4\mu L$ buffer droplet, Sample is the $0.7\mu L$ glucose sample droplet, R is the $0.7\mu L$ reagent droplet, GS is the $1.4\mu L$ 800mg/dL glucose solution droplet, and W_i is the waste droplet. D_i, Dl_i, S_i, M_i, and I_i are the detection, dilution, splitting, mixing, and dispensing operations, respectively.

2) Attack 1: The attacker changes the concentration of the glucose sample as shown in Fig. 4. The thick dotted lines show the changes in the golden sequencing graph. The waste buffer droplet generated from S_3 is mixed with the glucose sample droplet of I_6 and then diluted in Dl_{10}. Since the concentration of the glucose sample is halved, the result of the assay execution will be wrong. Using the golden calibration curve shown in Fig 6, the user will interpret the result as follows. In the golden calibration curve, the dots are the standard sample points corresponding to glucose solution concentrations (75, 150, $\cdots$, 800 mg/dL). The user will interpret the sample concentration as 110 mg/dL instead of the original concentration of 220 mg/dL. Hence, the patient may not be treated with the medication for high blood sugar, which could be life threatening.

If the patient or the medical practitioner wants to verify the result then there are two possible options: either to repeat

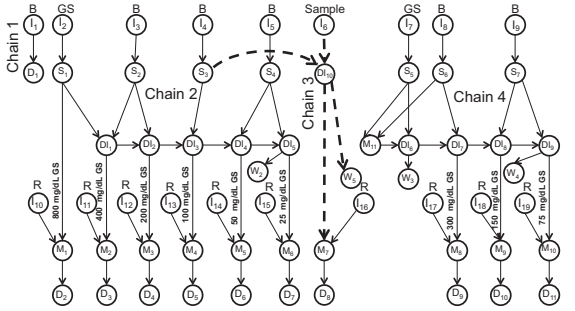

Fig. 4: In Attack 1, the waste buffer droplet generated by the splitting operation S_3 is used to dilute the sample droplet in Dl_{10}. The thick dotted lines show the changes in the golden sequencing graph.

the same test on the same DMFB, or to test it on a different DMFB by a different lab. It is highly likely that the test when repeated by a different lab will yield the correct result.

3) Attack 2: The attacker tampers with the golden calibration curve to have the resulting reported concentration of the glucose sample higher than the golden value. The attack is performed by tampering with the sequencing graphs for reaction chains 2 and 4 to generate a malicious calibration curve. The two waste buffer droplets generated from D_1 and S_3 in the golden sequencing graph are used for this purpose. The malicious sequencing graph for such an attack is shown in Fig. 5.

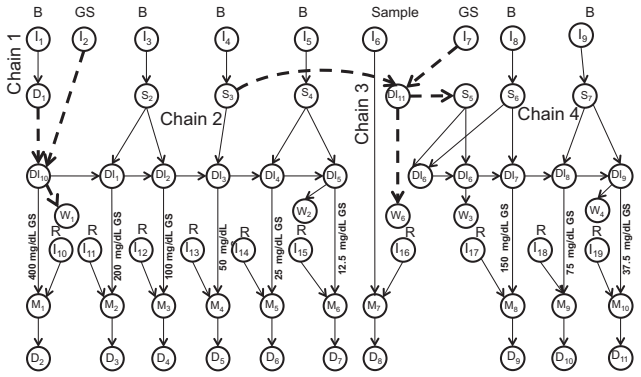

Fig. 5: In Attack 2, the discarded buffer droplets of D_1 and S_3 are mixed with the droplets of I_2 and I_7, respectively, diluting the reaction chains 2 and 4, respectively.

The thick dotted lines show the changes in the golden sequencing graph. The waste buffer droplet (after D_1) in the reaction chain 1 is merged with the glucose solution (the droplet generated from I_2) in the reaction chain 2, thus diluting the entire reaction chain 2. The glucose solution concentrations in the reaction chain 2 are reduced to (400, 200, 100, 50, 25, 12.5 mg/dL) half of their golden values. Similar effect can also be seen in the reaction chain 4, where the waste buffer droplet generated from S_3 is mixed with the glucose solution droplet generated from I_7. The dotted curve in Fig. 6 shows the malicious calibration curve generated by Attack 2.

The DMFB user is unaware that the calibration curve is

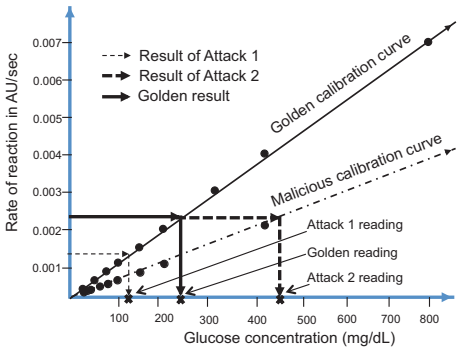

Fig. 6: Glucose calibration: The dots on the calibration curves represent the sample points. The thick lines and the thin dotted lines projected onto the X-axis represent the golden reading and the Attack 1 reading, respectively. The thick dotted lines projected onto the X-axis represent the Attack 2 reading.

malicious. The user will interpret the result using the malicious calibration curve (the dotted curve in Fig. 6). The result will show a higher concentration of glucose compared to the golden result. As the figure shows, the original concentration is 220 mg/dL when the golden calibration curve is used. Following Attack 2, the measured concentration is 440 mg/dL since the malicious calibration curve is used. Hence, the patient will be falsely alarmed and may receive a high dose of insulin, if this is the only test that he relies on.

C. Experimental Results

The golden, Attack 1, and Attack 2 sequencing graphs are executed using an open-source DMFB tool [17] on a 17×31 electrode-array DMFB with 7 input reservoirs[1]. A 100 Hz clock was considered for actuating the electrodes. The DMFB design times for the golden, Attack 1, and Attack 2 assays are 35, 39, and 62 milliseconds, respectively, while the assay execution times are 8.5, 9.26, and 10.46 seconds, respectively. Attack 1 is difficult to detect, since the difference in the DMFB synthesis time (35 ms vs 39 ms) and assay execution time (8.5 s vs 9.26 s) are negligible. This is because the attack alters the glucose sample using one additional dilution operation. Attack 2 impacts a large portion of the glucose assay, since it alters the concentrations of the glucose solution. The difference between the golden assay execution time and Attack 2 assay execution time is 1.9 seconds (8.5 s vs 10.46 s). The difference in the DMFB synthesis time is only 23ms (39 ms vs 62 ms). It is unlikely that the user can identify such a small change in the DMFB assay execution times.

IV. Discussion on Other Attack Models

So far, we have addressed two attacks on a DMFB. An attacker can also launch some denial-of-service (DoS) attacks on a DMFB. Cross-contamination is the best way for an attacker to perform a DoS attack on DMFBs. During transportation, a sample/reagent droplet leaves behind some residue along the

[1]We used list scheduler, left-edge placer, and maze droplet router for the DMFB design

route. If another droplet follows the same route or intersects it may be contaminated by the residues. Furthermore, two droplets may inadvertently mix with each other if they come too close during their transportation. A malicious CAD tool designer can implant a malicious code in the routing algorithm, which if triggered will modify the droplet routes to violate these routing and fluidic constraints.

Table I illustrates the cause-effect relationships for several attacks. A cell X, Y that is labelled as "Yes," indicates that an attack cause Y can result in effect X. For example, the sample concentration can be tampered with by modifying the sequence of dilution operations (row 1). The modification can be done either during the architectural-level or during the physical-level synthesis. During the architectural-level synthesis, the attacker can modify the timing of scheduled operations. During the physical-level synthesis, malicious modification can be done in two different ways: 1) by changing the placement of mixing/dilution operations, such that the operations are assigned to mixers with unsuitable sizes; and 2) by tampering with the droplet routing to extend a droplet route, increasing the likelihood of contamination and increasing the rate of liquid evaporation in DMFBs [9].

TABLE I: Taxonomy of attacks on DMFBs

Attack effect (X)	Attack cause (Y)			
	Architectural-level synthesis[2]	Physical-level synthesis[3]	Physical tampering	Actuation voltage
Modify sample concentration	Yes	Yes	No	No
Contaminate	No	Yes	No	No
Alter incubation or mixing time	Yes	Yes	No	No
Tamper with on-chip sensor	Yes	Yes	Yes	No
Alter DMFB life time	No	No	No	Yes

The incubation/mixing time can also be modified during the architectural-level or during the physical-level synthesis (row 3). Contamination opportunities can be created during the physical-level synthesis (row 2). On-chip sensors can be tampered with in several ways (row 4): 1) An accurate detection requires holding the droplet stationary for a fixed duration of time [16]. Changing this time impacts the accuracy of the measurement. 2) The results can be tampered with by generating an attack on the signal-conditioning and the analog-to-digital conversion sequence. Therefore, even though the sensors report a accurate result, the controller that receives this signal will interpret a wrong result. (3) The sensors themselves may be tampered with so that they report wrong results. An important factor which affects the life-time of the DMFB is the actuation voltage. An excessive actuation voltage may result in dielectric layer breakdown and may damage the DMFB.

[2]Architectural-level synthesis includes scheduling and resource binding.

[3]Physical-level synthesis includes module placement and droplet routing.

V. Conclusions

We have reported the first ever security assessment of DMFBs. We have described attacks, which if carried out, can have a catastrophic effect on the integrity of the assay outcomes. We have demonstrated the impact of such an attack on a state-of-the-art in-vitro glucose measurement assay. We have evaluated the feasibility and stealthiness of the attack. The results confirm that the attacks require small and easy to implement changes to the sequencing graph. Future research will focus on detection and protection of malicious attacks on DMFBs.

Acknowledgement

This work was supported in part by Center for Interdisciplinary Studies in Security and Privacy Abu Dhabi (CRISSP-AD).

References

[1] R. Sista, Z. Hua, P. Thwar, A. Sudarsan, V. Srinivasan, A. Eckhardt, M. Pollack, and V. Pamula, "Development of a digital microfluidic platform for point of care testing," *Lab on a Chip*, vol. 8, no. 12, pp. 2091–2104, 2008.

[2] D. J. Boles, J. L. Benton, G. J. Siew, M. H. Levy, P. K. Thwar, M. A. Sandahl, J. L. Rouse, L. C. Perkins, A. P. Sudarsan, R. Jalili *et al.*, "Droplet-based pyrosequencing using digital microfluidics," *Analytical chemistry*, vol. 83, no. 22, pp. 8439–8447, 2011.

[3] K. Chakrabarty, "Design automation and test solutions for digital microfluidic biochips," *IEEE TCAS*, vol. 57, no. 1, pp. 4–17, 2010.

[4] F. Su and K. Chakrabarty, "Architectural-level synthesis of digital microfluidics-based biochips," in *Proc. IEEE/ACM ICCAD*, 2004, pp. 223–228.

[5] F. Su and K. Chakrabarty, "Unified high-level synthesis and module placement for defect-tolerant microfluidic biochips," in *Proc. IEEE/ACM DAC*, 2005, pp. 825–830.

[6] F. Su, W. Hwang, and K. Chakrabarty, "Droplet Routing in the Synthesis of Digital Microfluidic Biochips," in *Proc. DATE*, vol. 1, 2006, pp. 1–6.

[7] Y. Luo, K. Chakrabarty, and T.-Y. Ho, "Error recovery in cyberphysical digital microfluidic biochips," *IEEE TCAD*, vol. 32, no. 1, pp. 59–72, 2013.

[8] N. M. Jokerst, L. Lin, S. Palit, M. Royal, S. Dhar, M. Brooke, and T. Tyler, "Progress in chip-scale photonic sensing." *IEEE TBCS*, vol. 3, no. 4, pp. 202–211, 2009.

[9] R. B. Fair, "Digital microfluidics: is a true lab-on-a-chip possible?" *Microfluidics and Nanofluidics*, vol. 3, no. 3, pp. 245–281, 2007.

[10] Y.-J. Shin and J.-B. Lee, "Machine vision for digital microfluidics," *Review of Scientific Instruments*, vol. 81, no. 1, p. 014302, 2010.

[11] Y. Luo, K. Chakrabarty, and T.-Y. Ho, "Real-Time Error Recovery in Cyberphysical Digital-Microfluidic Biochips Using a Compact Dictionary," *IEEE TCAD*, vol. 32, no. 12, pp. 1839–1852, Dec 2013.

[12] W. Houser, "Could What Happened to Sony Happen to Us?" *IT Professional*, vol. 17, no. 2, pp. 54–57, 2015.

[13] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE HealthCom*, 2011, pp. 150–156.

[14] R. Langner., "To kill a centrifuge: A technical analysis of what Stuxnet?s creators tried to achieve," 2010, http://www.langner.com/en/wpcontent/uploads/2013/11/To-kill-a-centrifuge.pdf.

[15] "Centers for Disease Control and Prevention: Diabetes Public Health Resource," [Online] http://www.cdc.gov/diabetes/statistics/prev/national/figpersons.htm, 2011.

[16] V. Srinivasan, V. K. Pamula, and R. B. Fair, "Droplet-based microfluidic lab-on-a-chip for glucose detection," *Analytica Chimica Acta*, vol. 507, no. 1, pp. 145–150, 2004.

[17] D. Grissom and P. Brisk, "A field-programmable pin-constrained digital microfluidic biochip," in *Proc. IEEE/ACM DAC*, 2013, pp. 1–9.