

Authors' copy downloaded from: <https://sprite.utsa.edu/>

Copyright may be reserved by the publisher.



# Analyzing Defense Strategies Against Mobile Information Leakages: A Game-Theoretic Approach

Kavita Kumari<sup>1</sup>[0000–0002–0491–4577],  
Murtuza Jadliwala<sup>1</sup>[0000–0001–9316–1943],  
Anindya Maiti<sup>2</sup>[0000–0001–6461–2805],  
and Mohammad Hossein Manshaei<sup>3</sup>[0000–0003–3765–7500]

<sup>1</sup>Department of Computer Science,  
University of Texas at San Antonio, San Antonio, TX 78249, USA

<sup>2</sup>Institute for Cyber Security,  
University of Texas at San Antonio, San Antonio, TX 78249, USA

<sup>3</sup>Department of Electrical and Computer Engineering,  
Isfahan University of Technology, Isfahan, 84156-83111, Iran  
kavita.kumari@utsa.edu, murtuza.jadliwala@utsa.edu,  
a.maiti@ieee.org, manshaei@cc.iut.ac.ir

**Abstract.** Abuse of zero-permission sensors (e.g., accelerometers and gyroscopes) on-board mobile and wearable devices to infer users’ personal context and information is a well-known privacy threat, and has received significant attention in the literature. At the same time, efforts towards relevant protection mechanisms have been ad-hoc and have main focus on threat-specific approaches that are not very practical, thus garnering limited adoption within popular mobile operating systems. It is clear that privacy threats that take advantage of unrestricted access to these sensors can be prevented if they are effectively regulated. However, the importance of these sensors to all applications operating on the mobile platform, including the dynamic sensor usage and requirements of these applications, makes designing effective access control/regulation mechanisms difficult. Moreover, this problem is different from classical intrusion detection as these sensors have no system- or user-defined policies that define their authorized or correct usage. Thus, to design effective defense mechanisms against such privacy threats, a clean slate approach that formalizes the problem of sensor access (to zero-permission sensors) on mobile devices is first needed. The paper accomplishes this by employing game theory, specifically, signaling games, to formally model the strategic interactions between mobile applications attempting to access zero-permission sensors and an on-board defense mechanism attempting to regulate this access. Within the confines of such a formal game model, the paper then outlines conditions under which equilibria can be achieved between these entities on a mobile device (i.e., applications and defense mechanism) with conflicting goals. The game model is further analyzed using numerical simulations, and also extended in the form of a repeated signaling game.

## 1 Introduction

Modern mobile and wearable devices, equipped with state-of-the-art sensing and communication capabilities, enable a variety of novel context-based applications such as social networking, activity tracking, wellness monitoring and home automation. The presence of a diverse set of on-board sensors, however, also provide an additional attack surface to applications intending to infer personal user information in an unauthorized fashion. In order to thwart such privacy threats, most modern mobile operating systems (including, Android and iOS) have introduced stringent access controls on front-end or user-accessible sensors, such as microphone, camera and GPS. As a result, the focus of adversarial applications has now shifted to employing on-board sensors that are not guarded by strong user or system-defined access control policies. Examples of such back-end or user-inaccessible sensors include accelerometer, gyroscope, power meter and ambient light sensor, and we refer to these as *zero-permission sensors*. As all installed applications have access to them by default, and that they cannot be actively disengaged by users on an application-specific basis, these zero-permission sensors pose a significant privacy threat to mobile device users, as it has been extensively studied in the security literature [5, 24, 1, 21, 14, 19, 8, 17, 6, 15, 16, 18, 10, 26, 12, 25, 11, 23, 13].

At the same time, development of efficient and effective protection mechanisms against such privacy threats is still an open problem [2]. One of the main reasons why zero-permission sensors have limited or no access control policies associated with them is because they are required by a majority of applications (accessed by means of a common set of libraries or APIs) primarily for efficient and user-friendly operation on the device’s small and constrained form factor and display. For instance, gyroscope data is used by applications to re-position front-ends (or GUIs) depending device orientation, while an ambient light sensor is used to update on-screen brightness. Thus, a straightforward approach of completely blocking access or reducing the frequency at which applications can sample data from these sensors is not feasible, as it will significantly impact their usability. Alternatively, having a static access control policy for each application is also not practical as it will become increasingly complex for users to manage these policies. Moreover, such an approach will not protect against applications that gain legitimate access to these sensors (based on such static policies). Given that all applications (with malicious intentions or not) can request access to these sensors without violating any system security policy, an important challenge for a defense mechanism is to differentiate between authentic sensor access requests and requests that could be potentially misused.

In order to begin addressing this long-standing open problem, we take a clean-slate approach by first formally (albeit, realistically) modeling the strategic interactions between (honest or potentially malicious) mobile applications and an on-board defense mechanism that cannot differentiate between their (sensor access) requests. We employ *game-theory* as a vehicle for modeling and analyzing these interactions. Specifically, we model the following scenario. A defense mechanism on a mobile operating system receives requests to access zero-permission

sensors from two different *types* of applications: *honest* and *malicious*. Each of these applications could send either a *normal* or a *suspicious* request for access to on-board zero-permission sensors. A request could be classified as suspicious or normal (non-suspicious) based on the context, frequency or amount of requested sensor data. Although honest applications would typically make normal requests, they could also make suspicious requests depending on application- or context-specific operations and requirements to improve overall application performance and usability. The goal of malicious applications, on the other hand, is to successfully infer private user data from these requests. Normal requests would give them some (probably, not enough) data to carry out these privacy threats, however, suspicious requests could give them additional critical data either to amplify or increase the success probability of their attacks. The defense mechanism, on receiving the request, has one of the following two potential responses: (i) *accept* the request and release the requested sensor data, or (ii) *block* the request preventing any data being released to the requesting application. It should be noted that the defense mechanism does not know the type of the application (i.e., honest or malicious) sending a particular request (i.e., suspicious or non-suspicious), as all mobile applications can currently request zero-permission sensor data without raising a flag or violating any policy. In other words, the defense mechanism has *imperfect information* on the type of application sending the request. The requesting application, on the other hand, has perfect information about its type and potential strategies of the defense mechanism. Given this scenario, the following are the main technical contributions of this paper:

1. We first formally model the strategic interactions between mobile applications and a defense mechanism (outlined above) using a *two-player, imperfect-information* game, called the *signaling game* [3]. We refer to it as the *Sensor Access Signaling Game*.
2. Next, we solve the Sensor Access Signaling Game by deriving both the pure- and mixed-strategy *Perfect Bayesian Nash Equilibria (PBNE)* strategy profiles possible in the game.
3. Finally, by means of numerical simulations, we examine how the obtained game solutions or equilibria evolve with respect to different system (or game) parameters in both the *single-stage* and *repeated* (more practical) scenarios.

Our game-theoretic model, and the related preliminary results, is the first clean-slate attempt to formally model the problem of protecting zero-permission sensors on mobile platforms against privacy threats from strategic applications and adversaries (with unrestricted access to it). Our hope is that this model will act as a good starting point for designing efficient, effective and incentive-compatible strategies for protecting against such threats.

## 2 Sensor Access Signaling Game

**System Model.** Our system (Figure 1a) comprises of two key entities residing on a user’s (mobile) device. The first is *applications (APP)* that utilize, and

thus, need access to, data from zero-permission sensors. We consider two *types* of applications: *Honest (HA)* and *Malicious (MA)*. Honest applications provide some useful service to the end-user with the help of zero-permission sensor data, while malicious applications would like to infer personal/private information about the user in the guise of offering some useful service. Both honest and malicious applications can request sensor data in a manner which may look normal/non-suspicious or suspicious (details next), regardless of their intentions or use-cases. The second entity is a sensor access regulator, which we refer to as the *Defense Mechanism (DM)*. All sensor access requests (by all applications) must pass through and processed by the *DM*. The *ideal* functionality that the *DM* would like to achieve is to block sensor requests coming from *MA*s, while allowing requests from *HA*s. As noted earlier, the *DM* itself does not know the type (i.e., honest or malicious) of application requesting sensor access - otherwise the job of the *DM* is trivial. This is also a practical assumption as currently all applications can access these sensors without violating any system/user-defined policy (to clarify, there is currently no way to set access control policies for zero-permission sensors on most mobile platforms). As the *DM* has no way of certainly knowing an application's true intentions (and thus, its type), it must rely on the received request (suspicious or non-suspicious, as described next) and its belief about the requesting application's type to determine whether it poses a threat to user privacy or not.

**Suspicious and Non-Suspicious Requests.** Zero-permission sensor access requests by the applications (to the *DM*) can be classified as either *suspicious (S)* or *non-suspicious (NS)*. Such a classification (generally, system-defined) can be accomplished using contextual information available to both the applications and the defense mechanism, such as, frequency, time, sampling rate, and relevance (according to the advertised type of service offered by the application) of these requests. Although there are several efforts in the literature in the direction of determining sensor over-privileges in mobile platforms [4, 7], we abstract away this detail to keep our model general. We, however, assume that malicious applications are able to masquerade themselves perfectly as honest applications (in terms of the issued sensor requests), which is easy to accomplish when the target of these applications is zero-permission sensors.

**Other System Parameters.** The strategic interactions between the (honest or malicious) *APP* and *DM* can be characterized using several system parameters which we summarize in Table 1. In addition to identifying these parameters, we also establish the relationship between these parameters by considering realistic network and system constraints as discussed next. For example, if the cost of an application processing a successful *S* request (i.e.,  $c^S$ ) or *NS* request (i.e.,  $c^{NS}$ ) is expressed in terms of the CPU utilization (of the application), then it is clear that  $c^S \geq c^{NS}$  because suspicious requests would usually solicit fine-grained (high sampling rate) sensor data compared to non-suspicious requests, thus requiring more processing time. By a similar rationale,  $\psi^S \geq \psi^{NS}$ , where  $\psi^S$  and  $\psi^{NS}$  are the costs to a *DM* (or the system) for processing a *S* or *NS* request, respectively. Now, the cost to the *HA* in terms of loss in usability when

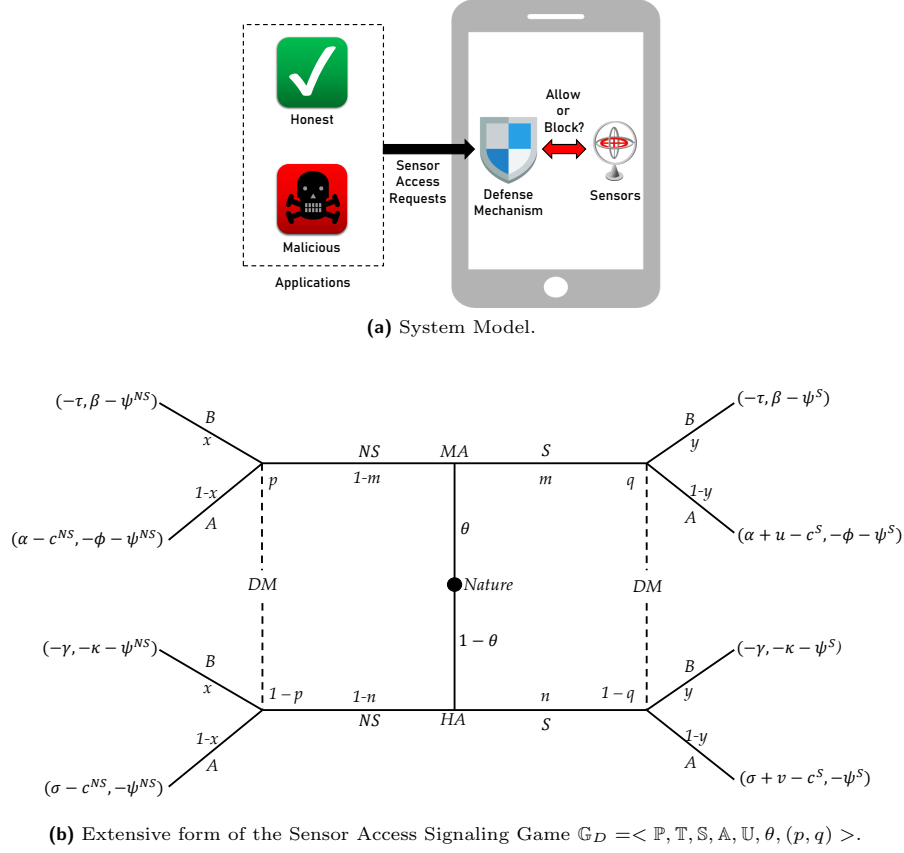


Fig. 1: Overview of the system and game models.

its request is blocked by  $DM$  (i.e.,  $\gamma$ ) and benefit for the  $HA$  in terms of gain in usability when its request is allowed by the  $DM$  (i.e.,  $\sigma$ ) are inversely proportional ( $\gamma \propto 1/\sigma$ ). Similarly, benefit to the  $MA$  when its request is allowed by  $DM$  ( $\alpha$ ) can be expressed in terms of monetary gains. An acute example would be if  $MA$  is able to successfully infer user's banking credentials using sensor data [10, 25, 12, 23], and uses it for theft. A more clement example of monetary gain could be through selling contextual data (inferred from sensor data) to advertising companies, without user's consent. Accordingly,  $MA$  is set back with a proportional cost ( $\tau$ ) if its request is rejected by  $DM$ , i.e.,  $\alpha \propto \tau$ . On the other hand,  $DM$ 's cost of allowing a  $MA$ 's request ( $\phi$ ) versus benefit to the  $DM$  for blocking  $MA$ 's request ( $\beta$ ) are also inversely proportional ( $\phi \propto 1/\beta$ ).  $DM$ 's cost of allowing a  $MA$ 's request is essentially borne by the user, but since the  $DM$  is working in the best interest of the user, we combine their costs and benefits. Consequently, in case  $DM$  blocks an  $HA$ 's request, it incurs a cost ( $\kappa$ ) representing loss of utility/usability for the user. Lastly, we also capture the *difference in benefits* for  $MA$  and  $HA$ , in case they send out a  $S$  versus  $NS$  request, as  $u$

Table 1: System entities and parameters.

Symbol	Definition
$DM$	Defense Mechanism
$HA$	Honest Application
$MA$	Malicious Application
$\theta$	Probability that Nature selects $MA$
$\mathcal{S}$	Suspicious sensor request
$\mathcal{NS}$	Non-suspicious sensor request
$q$	Belief probability of the $DM$ that the requester is of type $MA$ on receiving a $\mathcal{S}$ request
$p$	Belief probability of the $DM$ that the requester is of type $MA$ on receiving a $\mathcal{NS}$ request
$B$	$DM$ response to block a sender request
$A$	$DM$ response to allow a sender request
$c^{\mathcal{S}}$	Cost of an application processing a successful $\mathcal{S}$ request
$c^{\mathcal{NS}}$	Cost of an application processing a successful $\mathcal{NS}$ request
$\gamma$	Cost to the $HA$ when its request is blocked by $DM$
$\psi^{\mathcal{S}}$	Cost of a $DM$ processing a $\mathcal{S}$ request
$\psi^{\mathcal{NS}}$	Cost of a $DM$ processing a $\mathcal{NS}$ request
$\phi$	Cost to the $DM$ when $MA$ 's request is allowed
$\tau$	Cost to the $MA$ when its request is blocked by the $DM$
$\kappa$	Cost to the $DM$ when $HA$ 's request is blocked
$\alpha$	Benefit to the $MA$ when its request is allowed by the $DM$
$\beta$	Benefit to the $DM$ for blocking $MA$ 's request
$\sigma$	Benefit to the $HA$ when its request is allowed by the $DM$
$u$	Benefit difference to $MA$ for sending $\mathcal{S}$ instead of $\mathcal{NS}$
$v$	Benefit difference to $HA$ for sending $\mathcal{S}$ instead of $\mathcal{NS}$
$m$	probability with which $MA$ plays the $\mathcal{S}$ strategy
$n$	probability with which $HA$ plays the $\mathcal{S}$ strategy
$x$	probability with which $DM$ plays the $B$ strategy on receiving a $\mathcal{NS}$ request
$y$	probability with which $DM$ plays the $B$ strategy on receiving a $\mathcal{S}$ request

and  $v$ , respectively. In essence,  $u$  denotes the gain in benefit due to  $MA$ 's better inference accuracy caused by sensor data obtained from  $\mathcal{S}$ , and  $v$  denotes the improvement of  $HA$ 's utility/usability due to sensor data obtained from  $\mathcal{S}$ . We also assume that these different (discrete) costs and benefits are appropriately scaled and normalized such that their absolute values lie in the same range of real values. Next, we outline the signaling game formulation to capture the strategic interaction between the mobile applications (requesting zero-permission sensor access) and the defense mechanism (attempting to regulating these requests).

**Game Model.** A classical signaling game [3] is a sequential two-player incomplete information game in which *Nature* starts the game by choosing the *type* of the first player or *player 1*. Player 1 is the more informed out of the two players since it knows the choice of *Nature* and can send *signals* to the less informed player, i.e., *player 2*. Player 2 is uncertain about the type of player 1, and must decide its strategic response solely based on the signal received from player 1. In other words, player 2 must decide its best response to player 1's signal without any knowledge about the type of player 1. Both players receive some utility (payoff) depending on the signal, type of player 1 and the response by player 2 (to player 1's signal). Both the players are assumed to be rational and are interested in solely maximizing their individual payoffs.

Given the above generic description of the signaling game, let us briefly describe how our zero-permission sensor access scenario naturally lends itself as a single-stage signaling game. We refer to this game as the *Sensor Access Signaling Game* and is formally represented as  $\mathbb{G}_D = \langle \mathbb{P}, \mathbb{T}, \mathbb{S}, \mathbb{A}, \mathbb{U}, \theta, (p, q) \rangle$ , where  $\mathbb{P}$  is the set of players,  $\mathbb{T}$  is the set of player 1 types,  $\mathbb{S}$  is the set of player 1 signals,  $\mathbb{A}$  is the set of player 2 actions,  $\mathbb{U}$  is the *payoff/utility function*,  $\theta$  is the *Nature's probability distribution function*, and  $(p, q)$  are player 2's *belief functions* about player 1's type. Each sensor access request by an application can be modeled as a single stage of the above signaling game. In each such stage,  $\mathbb{P}$  contains two players, i.e., *APP* which is player 1 and the *DM* which is player 2. As there are two types of applications (or player 1), i.e., honest (*HA*) and malicious (*MA*),  $\mathbb{T} \equiv \{HA, MA\}$ . As applications can send two types of signals (or requests), i.e., suspicious (*S*) and non-suspicious (*NS*),  $\mathbb{S} \equiv \{S, NS\}$ . As the *DM* (or player 2) takes two types of actions depending on the received signal from player 1, i.e., Allow (*A*) or Block (*B*),  $\mathbb{A} \equiv \{A, B\}$ . The utility function  $\mathbb{U} : \mathbb{T} \times \mathbb{S} \times \mathbb{A} \rightarrow (\mathbb{R}, \mathbb{R})$  assigns a real-valued payoff to each player (at the end of the stage) based on the benefit received and the cost borne by each player, and is outlined in the extensive form of the game depicted in Figure 1b. The first utility in the pair is the *APP*'s utility denoted as  $U_{APP}$ , while the second utility in the pair is the *DM*'s utility denoted as  $U_{DM}$ .

Lastly, let  $\Gamma_{APP} = \{\mu_{APP} | \forall t_i \in \mathbb{T}, \sum_{\lambda \in \mathbb{S}} \mu_{APP}(\lambda | t_i) = 1; \forall t_i \in \mathbb{T}\}$  and  $\Gamma_{DM} = \{\mu_{DM} | \forall \lambda \in \mathbb{S}, \sum_{a \in \mathbb{A}} \mu_{DM}(a | \lambda) = 1; \forall \lambda \in \mathbb{S}\}$  be the strategy spaces for *APP* and *DM*, respectively. A strategy  $\mu_{APP}$  for the *APP* and  $\mu_{DM}$  for the *DM* can be either *pure* or *mixed*, as identified by parameters  $m, n, y$  and  $x$  in Figure 1b. For pure strategies  $m, n, y, x \in \{0, 1\}$ , while for mixed strategies  $0 < m, n, y, x < 1$ . Moreover, let us represent each of the *DM*'s belief functions by conditional (posterior) probability distributions as  $q = Pr(MA | S)$  and  $p = Pr(MA | NS)$ , which also imply that  $1 - q = Pr(HA | S)$  and  $1 - p = Pr(HA | NS)$ .

Now, let's characterize the set of equilibrium strategies in  $\mathbb{G}_D$ , i.e., a set of strategy pairs that are mutual best responses to each other and no player has any incentive to move away from their strategy in that pair. In order to determine mutual best responses, we need to evaluate the actions (or strategies) of each player at each *information set* of the game. *APP*'s information set comprises of a single decision point (i.e., to select a signal  $\lambda \in \{S, NS\}$ ) after Nature makes its selection of the type (*HA* or *MA*) and reveals it to *APP*. *DM*'s information set, on the other hand, comprises of two decision points because of its incomplete information about the type of *APP* chosen by Nature. Thus, *DM*'s strategy is to select an action  $a \in \{A, B\}$  depending on its belief  $Pr(t_i | \lambda)$  about the type  $t_i \in \mathbb{T}$  of *APP* in that information set. Moreover, for each  $\lambda \in \{S, NS\}$ ,  $\sum_{t_i} Pr(t_i | \lambda) = 1$ .

Our goal is to determine the existence of *Perfect Bayesian Nash Equilibria* (or *PBNE*) in  $\mathbb{G}_D$ , where strategies are combined with beliefs to determine the mutual best responses of each player at the end of each stage. A PBNE of the Sensor Access Signaling Game  $\mathbb{G}_D$  is a strategy profile  $\mu^* = (\mu_{APP}^*, \mu_{DM}^*)$  and posterior probabilities (or beliefs of the *DM*)  $Pr(t_i | \lambda)$  such that:

$$\mu_{APP}^* \in \operatorname{argmax}_{\mu_{APP} \in \Gamma_{APP}} U_{APP}(\mu_{APP}, \mu_{DM}^*, t_i); \forall t_i \in \mathbb{T}$$



where,  $U_{APP}(\cdot)$  is the utility or payoff of  $APP$  for a particular pure or mixed strategy  $\mu_{APP}$  against  $DM$ 's best response to it, when the type  $t_i$  selected by Nature, and,  $\forall \lambda \in \mathbb{S} = \{\mathcal{S}, \mathcal{NS}\}$  such that:

$$\mu_{DM}^* \in \operatorname{argmax}_{\mu_{DM} \in \Gamma_{DM}} \sum_{t_i \in \mathbb{T}} Pr(t_i|\lambda) U_{DM}(\lambda, \mu_{DM}, t_i)$$

where,  $U_{DM}(\cdot)$  is the payoff of  $DM$  for a particular pure or mixed strategy  $\mu_{DM}$  against the signal ( $\lambda$ ) received from the  $APP$ , when the type  $t_i$  selected by Nature. Moreover, the  $DM$ 's belief  $Pr(t_i|\lambda)$  about the  $APP$ 's type given a received signal  $\lambda$  should satisfy Bayes' theorem, i.e.,

$$Pr(t_i|\lambda) = \frac{Pr(\lambda|t_i)Pr(t_i)}{Pr(\lambda)} = \frac{\mu_{APP}(\lambda|t_i)Pr(t_i)}{Pr(\lambda)}$$

Four categories of PBNE can exist for a signaling game such as  $\mathbb{G}_D$ :

- **Separating PBNE:** This category comprises of strategy profiles where player 1 or  $APP$  of different types dominantly send different or contrasting types of signals  $\lambda \in \{\mathcal{S}, \mathcal{NS}\}$ . This allows  $DM$  to infer  $APP$ 's type with certainty. For instance, in a separating strategy profile  $\{(\mathcal{S}, \mathcal{NS}), \mu_{DM}^*\}$ ,  $APP$  of  $MA$  type always selects  $\mathcal{S}$  (i.e.,  $m = 1$ ) while  $HA$  always selects the  $\mathcal{NS}$  (i.e.,  $n = 0$ ).
- **Pooling PBNE:** This category comprises of strategy profiles where player 1 or  $APP$  of different types dominantly send the same type of signal  $\lambda$ . Here  $DM$  cannot infer  $APP$ 's type with certainty, but needs to update its belief (about  $APP$ 's type) based on the observed  $\lambda$ . For instance, in a pooling strategy profile  $\{(\mathcal{S}, \mathcal{S}), \mu_{DM}^*\}$ , both  $MA$  and  $HA$  types always select  $\mathcal{S}$  (i.e.,  $m, n = 1$ ).
- **Hybrid PBNE:** This category comprises of strategy profiles where one player 1 or  $APP$  type dominantly sends one type of signal, but the other type randomizes its sent signal. For instance, in a hybrid strategy profile  $\{(\mathcal{S}, (\mathcal{S}, \mathcal{NS})), \mu_{DM}^*\}$ ,  $MA$  always selects  $\mathcal{S}$  (i.e.,  $m = 1$ ), whereas  $HA$  randomizes between  $\mathcal{S}$  and  $\mathcal{NS}$  (i.e.,  $0 < n < 1$ ).
- **Mixed PBNE:** Finally, this equilibrium comprises of strategy profiles where all player 1 or  $APP$  types send signals  $\lambda$  only in a probabilistic fashion (i.e.,  $0 < m, n < 1$ ).

### 3 Game Analysis

In this section, we find the PBNE for the sensor access signaling game  $\mathbb{G}_D$ . We begin by evaluating the existence of pure strategy equilibria (i.e., separating, pooling and hybrid), including conditions and regimes for achieving these equilibria. Following that we determine the mixed strategy equilibria for  $\mathbb{G}_D$ .

**Theorem 1.** *There does not exist a separating equilibrium in the game  $\mathbb{G}_D$ .*

*Proof.* There can be two possible separating strategy profiles for  $APP$ :  $(\mathcal{S}, \mathcal{NS})$  and  $(\mathcal{NS}, \mathcal{S})$ . First, let us analyze the existence of an equilibrium on  $(\mathcal{S}, \mathcal{NS})$ , which means  $MA$  (malicious type) always selects  $\mathcal{S}$  (i.e.,  $m = 1$ ) while  $HA$

(honest type) always selects  $\mathcal{NS}$  (i.e.,  $n = 0$ ).  $DM$ 's beliefs can be calculated using Bayes' theorem as follows:

$$\begin{aligned} Pr(MA|\mathcal{S}) = q &= \frac{Pr(\mathcal{S}|MA) \times Pr(MA)}{Pr(\mathcal{S})} = \frac{Pr(\mathcal{S}|MA) \times Pr(MA)}{Pr(\mathcal{S}|MA) \times Pr(MA) + Pr(\mathcal{S}|HA) \times Pr(HA)} \\ &= \frac{m \times \theta}{m \times \theta + n \times (1 - \theta)} = \frac{1 \times \theta}{1 \times \theta + 0 \times (1 - \theta)} = 1 \end{aligned}$$

Therefore,  $Pr(HA|\mathcal{S}) = 1 - q = 0$ . Similarly, we can show that  $p = 0$ , and  $1 - p = 1$ . With these beliefs, the best response of  $DM$  can be calculated as follows. The  $DM$ 's expected utility/payoff ( $EU_{DM}$ ) from playing  $B$  or  $A$  if  $MA$  or  $HA$  selects  $\mathcal{S}$  are:

$$EU_{DM}(B, \mathcal{S}) = 1 \times (\beta - \psi^{\mathcal{S}}) + 0 \times (-\kappa - \psi^{\mathcal{S}}) = \beta - \psi^{\mathcal{S}}$$

$$EU_{DM}(A, \mathcal{S}) = 1 \times (-\phi - \psi^{\mathcal{S}}) + 0 \times (-\psi^{\mathcal{S}}) = -\phi - \psi^{\mathcal{S}}$$

As  $EU_{DM}(B, \mathcal{S}) > EU_{DM}(A, \mathcal{S})$ , the  $DM$ 's best response in this case is to play Block, i.e.,  $BR_{DM}(\mathcal{S}) = B$ . Similarly, the  $DM$ 's expected utility/payoff from playing  $B$  or  $A$  if  $MA$  or  $HA$  selects  $\mathcal{NS}$  are:

$$EU_{DM}(B, \mathcal{NS}) = 0 \times (\beta - \psi^{\mathcal{NS}}) + 1 \times (-\kappa - \psi^{\mathcal{NS}}) = -\kappa - \psi^{\mathcal{NS}}$$

$$EU_{DM}(A, \mathcal{NS}) = 0 \times (-\phi - \psi^{\mathcal{NS}}) + 1 \times (-\psi^{\mathcal{NS}}) = -\psi^{\mathcal{NS}}$$

In this case, as  $EU_{DM}(B, \mathcal{NS}) < EU_{DM}(A, \mathcal{NS})$ , the  $DM$ 's best response is to play Allow, i.e.,  $BR_{DM}(\mathcal{NS}) = A$ . In summary, if  $MA$  or  $HA$  plays  $\mathcal{S}$  then  $DM$ 's best response is  $B$ , and if  $MA$  or  $HA$  plays  $\mathcal{NS}$  then  $DM$ 's best response is  $A$ .

*Check for Equilibrium:*  $HA$  and  $MA$  will follow the strategy along the equilibrium path as long as the payoff along that path is higher than the payoff it will get if it deviates. There can be two scenarios: first if the  $MA$  deviates and plays  $\mathcal{NS}$  and second if the  $HA$  deviates and plays  $\mathcal{S}$ . Let us first analyze the case where  $MA$  deviates and plays  $\mathcal{NS}$ . The  $DM$ 's beliefs do not change, and so, if it sees  $MA$  or  $HA$  playing  $\mathcal{NS}$ , it will still always respond with its best response, i.e.,  $A$ .  $MA$  will receive a payoff of  $-\tau$  if it plays  $\mathcal{S}$  and will receive a payoff of  $\alpha - c^{\mathcal{NS}}$  if it plays  $\mathcal{NS}$ . Thus,  $MA$  has an incentive to deviate from the equilibrium path. Although it can be shown that  $HA$  does not have an incentive to deviate, equilibrium does not exist in this case because at least one  $APP$  (player 1) type has an incentive to deviate.

Next, let us analyze the existence of a separating equilibrium on  $(\mathcal{NS}, \mathcal{S})$ , which means  $MA$  always selects  $\mathcal{NS}$  (i.e.,  $m = 0$ ) and  $HA$  always selects  $\mathcal{S}$  (i.e.,  $n = 1$ ). As before, the belief functions for the  $DM$  can be calculated as:

$$Pr(MA|\mathcal{NS}) = p = \frac{Pr(\mathcal{NS}|MA) \times Pr(MA)}{Pr(\mathcal{NS})} = \frac{1 \times \theta}{1 \times \theta + 0 \times (1 - \theta)} = 1$$

Therefore,  $Pr(HA|\mathcal{NS}) = 1 - p = 0$ . Similarly, we can also show that  $q = 0$  and  $1 - q = 1$ . Thus, the  $DM$ 's expected utility/payoff from playing  $B$  or  $A$  if  $MA$  or  $HA$  selects  $\mathcal{S}$  are:

$$EU_{DM}(B, \mathcal{S}) = 0 \times (\beta - \psi^{\mathcal{S}}) + 1 \times (-\kappa - \psi^{\mathcal{S}}) = -\kappa - \psi^{\mathcal{S}}$$

$$EU_{DM}(A, \mathcal{S}) = 0 \times (-\phi - \psi^{\mathcal{S}}) + 1 \times (-\psi^{\mathcal{S}}) = -\psi^{\mathcal{S}}$$

In this case, as  $EU_{DM}(B, \mathcal{S}) < EU_{DM}(A, \mathcal{S})$ , the  $DM$ 's best response is to play Allow, i.e.,  $BR_{DM}(\mathcal{S}) = A$ . And,  $DM$ 's expected utility from playing  $B$  or  $A$  if  $MA$  or  $HA$  selects  $\mathcal{NS}$  are:

$$EU_{DM}(B, \mathcal{NS}) = 1 \times (\beta - \psi^{\mathcal{NS}}) + 0 \times (-\kappa - \psi^{\mathcal{NS}}) = \beta - \psi^{\mathcal{NS}}$$

$$EU_{DM}(A, \mathcal{NS}) = 1 \times (-\phi - \psi^{\mathcal{NS}}) + 0 \times (-\psi^{\mathcal{NS}}) = -\phi - \psi^{\mathcal{NS}}$$

As  $EU_{DM}(B, \mathcal{NS}) > EU_{DM}(A, \mathcal{NS})$ , in this case the  $DM$ 's best response is to Block, i.e.,  $BR_{DM}(\mathcal{NS}) = B$ . In summary, if  $MA$  or  $HA$  plays  $\mathcal{S}$ , then  $DM$ 's best response is  $A$  and if  $MA$  or  $HA$  plays  $\mathcal{NS}$ , then  $DM$ 's best response is  $B$ .

*Check for Equilibrium:* If  $MA$  deviates and plays  $\mathcal{S}$ ,  $DM$  will respond with it's best response  $A$ . As a result,  $MA$  will receive a payoff of  $-\tau$  if it plays  $\mathcal{NS}$  and will receive a payoff of  $\alpha + u - c^{\mathcal{S}}$  if it plays  $\mathcal{S}$ . Thus,  $MA$  has an incentive to deviate from the equilibrium path. Again, although it can be shown that  $HA$  does not have an incentive to deviate, equilibrium does not exist in this case either because at least one  $APP$  (player 1) type has incentive to deviate.

Thus, neither of the separating strategy profiles  $\{(\mathcal{S}, \mathcal{NS}), (B, A), p, q\}$  and  $\{(\mathcal{NS}, \mathcal{S}), (A, B), p, q\}$  is a  $PBNE$ .

**Theorem 2.** *There exists pooling equilibria on  $APP$  strategies of  $(\mathcal{S}, \mathcal{S})$  and  $(\mathcal{NS}, \mathcal{NS})$  in the game  $\mathbb{G}_D$ .*

*Proof.* An  $APP$  strategy profile  $(\mathcal{S}, \mathcal{S})$  means both  $MA$  and  $HA$  types always select  $\mathcal{S}$  (i.e.,  $m, n = 1$ ).  $DM$ 's beliefs in this strategy profile can be calculated as:

$$Pr(MA|\mathcal{S}) = q = \frac{Pr(\mathcal{S}|MA) \times Pr(MA)}{Pr(\mathcal{S})} = \frac{1 \times \theta}{1 \times \theta + 1 \times (1 - \theta)} = \theta$$

Therefore,  $Pr(HA|\mathcal{S}) = 1 - q = 1 - \theta$ . Accordingly, expected payoff for  $DM$  from playing  $B$  or  $A$  if either  $MA$  or  $HA$  selects  $\mathcal{S}$  are:

$$\begin{aligned} EU_{DM}(B, \mathcal{S}) &= \theta \times (\beta - \psi^{\mathcal{S}}) + (1 - \theta) \times (-\kappa - \psi^{\mathcal{S}}) \\ &= \theta(\beta + \kappa) - \kappa - \psi^{\mathcal{S}} \\ EU_{DM}(A, \mathcal{S}) &= \theta \times (-\phi - \psi^{\mathcal{S}}) + (1 - \theta) \times (-\psi^{\mathcal{S}}) \\ &= -\phi \times \theta - \psi^{\mathcal{S}} \end{aligned}$$

Now,  $DM$ 's best response to the  $APP$ 's pooling strategy of  $(\mathcal{S}, \mathcal{S})$  would be to select  $B$  (over  $A$ ) if and only if the following condition holds:

$$\theta(\beta + \kappa) - \kappa - \psi^{\mathcal{S}} \geq -\phi \times \theta - \psi^{\mathcal{S}} \equiv \theta \geq \frac{\kappa}{\beta + \kappa + \phi}$$

To analyze the existence of an equilibrium at the  $APP$ 's strategy of  $(\mathcal{S}, \mathcal{S})$ , given the  $DM$ 's best response, we must check if  $APP$  of either type ( $MA$  or  $HA$ ) has an incentive to deviate and play  $\mathcal{NS}$ . Here, if  $HA$  or  $MA$  deviate and play  $\mathcal{NS}$  and  $DM$  chooses  $A$ ,  $HA$  gains a payoff of  $\sigma - c^{\mathcal{NS}}$  compared to  $-\gamma$  if it plays  $\mathcal{S}$ , while  $MA$  gains a payoff of  $\alpha - c^{\mathcal{NS}}$  compared to  $-\tau$  if it plays  $\mathcal{S}$ . Thus, in this case both  $HA$  and  $MA$  have an incentive to deviate and play  $\mathcal{NS}$  and there is no equilibrium. Here, if  $HA$  or  $MA$  deviate and play  $\mathcal{NS}$  and  $DM$

chooses  $B$ ,  $HA$  will receive a payoff of  $-\gamma$ , same as if it plays  $\mathcal{S}$ , while  $MA$  will receive a payoff of  $-\tau$ , same as if it plays  $\mathcal{S}$ . Thus, in this case, both  $HA$  and  $MA$  do not have any incentive to switch to  $\mathcal{NS}$  and an equilibrium exists. In summary, an equilibrium on the  $APP$ 's pooling strategy of  $(\mathcal{S}, \mathcal{S})$  exists when  $\theta \geq \frac{\kappa}{\beta + \kappa + \phi}$ .

Inversely, the  $DM$ 's best response to  $APP$ 's pooling strategy of  $(\mathcal{S}, \mathcal{S})$  would be to select  $A$  (over  $B$ ) if and only if the following holds:

$$\theta(\beta + \kappa) - \kappa - \psi^{\mathcal{S}} \leq -\phi \times \theta - \psi^{\mathcal{S}} \equiv \theta \leq \frac{\kappa}{\beta + \kappa + \phi}$$

Here, if  $HA$  or  $MA$  deviate and play  $\mathcal{NS}$  and  $DM$  chooses  $A$ ,  $HA$  will receive a payoff of  $\sigma - c^{\mathcal{NS}}$  if it plays  $\mathcal{NS}$  and will receive a payoff of  $\sigma + v - c^{\mathcal{S}}$  if it plays  $\mathcal{S}$ . On the other hand,  $MA$  will receive a payoff of  $\alpha - c^{\mathcal{NS}}$  if it plays  $\mathcal{NS}$  and will receive a payoff of  $\alpha + u - c^{\mathcal{S}}$  if it plays  $\mathcal{S}$ . Thus, in this case, there will be a pooling equilibrium if and only if:

$$\begin{aligned} \sigma + v - c^{\mathcal{S}} &\geq \sigma - c^{\mathcal{NS}} \equiv v \geq c^{\mathcal{S}} - c^{\mathcal{NS}}, \text{ and} \\ \alpha + u - c^{\mathcal{S}} &\geq \alpha - c^{\mathcal{NS}} \equiv u \geq c^{\mathcal{S}} - c^{\mathcal{NS}} \end{aligned}$$

Here, if  $HA$  or  $MA$  deviate and play  $\mathcal{NS}$  and  $DM$  chooses  $B$ ,  $HA$  will receive a payoff  $-\gamma$  compared to  $\sigma + v - c^{\mathcal{S}}$  if it plays  $\mathcal{S}$ , while  $MA$  will receive a payoff of  $-\tau$  compared to  $\alpha + u - c^{\mathcal{S}}$  if it plays  $\mathcal{S}$ . Thus, in this particular case,  $HA$  and  $MA$  do not have any incentive to deviate as well. In summary, an equilibrium on  $APP$ 's pooling strategy of  $(\mathcal{S}, \mathcal{S})$  also exists when  $\theta \leq \frac{\kappa}{\beta + \kappa + \phi}$ .

As the proof of a pooling equilibrium on the  $APP$  strategy of  $(\mathcal{NS}, \mathcal{NS})$  follows an analogous methodology, it is omitted to conserve space. In summary, equilibrium on the  $APP$ 's pooling strategy of  $(\mathcal{NS}, \mathcal{NS})$  exists when  $\theta \geq \frac{\kappa}{\beta + \kappa + \phi}$ , or when  $\theta \leq \frac{\kappa}{\beta + \kappa + \phi}$ . For complete proofs, please refer to [9].

**Theorem 3.** *There exists hybrid equilibria on the  $APP$  strategy profiles  $(\mathcal{S}, (\mathcal{S}, \mathcal{NS}))$ ,  $(\mathcal{NS}, (\mathcal{S}, \mathcal{NS}))$ ,  $((\mathcal{S}, \mathcal{NS}), \mathcal{S})$  and  $((\mathcal{S}, \mathcal{NS}), \mathcal{NS})$ , in the game  $\mathbb{G}_D$ .*

*Proof.* An  $APP$  strategy profile  $(\mathcal{S}, (\mathcal{S}, \mathcal{NS}))$  means that  $MA$  always selects  $\mathcal{S}$  (i.e.,  $m = 1$ ), whereas  $HA$  selects  $\mathcal{S}$  with some probability  $n$  and  $\mathcal{NS}$  with probability  $1 - n$  where  $(0 < n < 1)$ .  $DM$ 's beliefs in this strategy profile can thus be calculated as:

$$\begin{aligned} Pr(MA|\mathcal{S}) = q &= \frac{Pr(\mathcal{S}|MA) \times Pr(MA)}{Pr(\mathcal{S})} = \frac{1 \times \theta}{1 \times \theta + n \times (1 - \theta)} = \frac{\theta}{\theta(1 - n) + n} \\ Pr(MA|\mathcal{NS}) = p &= \frac{Pr(\mathcal{NS}|MA) \times Pr(MA)}{Pr(\mathcal{NS})} = \frac{0 \times \theta}{0 \times \theta + (1 - n) \times (1 - \theta)} = 0 \end{aligned}$$

Now, let's compute the  $DM$ 's best response for each of the strategies  $\mathcal{S}$  and  $\mathcal{NS}$  of  $APP$ . In order to determine that, we need to first compute the expected utilities/payoffs obtained by  $DM$  for playing  $B$  or  $A$  if  $APP$  ( $MA$  or  $HA$ ) selects  $\mathcal{NS}$  or  $\mathcal{S}$ , which is given by:

$$\begin{aligned} EU_{DM}(B, \mathcal{NS}) &= p \times (\beta - \psi^{\mathcal{NS}}) + (1 - p) \times (-\kappa - \psi^{\mathcal{NS}}) = -\kappa - \psi^{\mathcal{NS}} \\ EU_{DM}(A, \mathcal{NS}) &= p \times (-\phi - \psi^{\mathcal{NS}}) + (1 - p) \times (-\psi^{\mathcal{NS}}) = -\psi^{\mathcal{NS}} \end{aligned}$$

$$EU_{DM}(B, \mathcal{S}) = q \times (\beta - \psi^{\mathcal{S}}) + (1 - q) \times (-\kappa - \psi^{\mathcal{S}})$$

$$EU_{DM}(A, \mathcal{S}) = q \times (-\phi - \psi^{\mathcal{S}}) + (1 - q) \times (-\psi^{\mathcal{S}})$$

It is clear from these expected utilities obtained by the *DM* in this strategy profile that it will always plays *A* (i.e., *A* always dominates *B*) when the *APP* plays  $\mathcal{NS}$ . On the contrary, there are two possibilities in terms of the *DM*'s best response to an application's strategy of  $\mathcal{S}$ . The first possibility is for the *DM* to always Block or *B*, i.e., *B* would dominate *A*. This, however, holds only if the following is true:

$$q(\beta - \psi^{\mathcal{S}}) + (1 - q)(-\kappa - \psi^{\mathcal{S}}) \geq q(-\phi - \psi^{\mathcal{S}}) + (1 - q)(-\psi^{\mathcal{S}}) \equiv q \geq \frac{(1 - q)\kappa}{\beta + \phi}$$

Now, as *DM* always plays *A* for  $\mathcal{NS}$ , *HA* has more incentive to play  $\mathcal{NS}$  because it will gain  $\sigma - c^{\mathcal{NS}}$  compared to  $-\gamma$  if it plays  $\mathcal{S}$ . Also, *MA* has more incentive to play  $\mathcal{NS}$  since it will gain  $\alpha - c^{\mathcal{NS}}$  compared to  $-\tau$  if it plays  $\mathcal{S}$ . In other words, *APP* is not indifferent between playing  $\mathcal{S}$  and  $\mathcal{NS}$  when  $q \geq \frac{(1 - q)\kappa}{\beta + \phi}$ , and strongly prefers playing  $\mathcal{NS}$ . Thus, there is no hybrid equilibria at  $(\mathcal{S}, (\mathcal{S}, \mathcal{NS}))$  when  $q \geq \frac{(1 - q)\kappa}{\beta + \phi}$ .

The second possibility, in terms of the *DM*'s best response to an *APP*'s strategy of  $\mathcal{S}$ , is for the *DM* to Accept or *A* (i.e., *A* dominates *B*) which is true if  $q \leq \frac{(1 - q)\kappa}{\beta + \phi}$ . This combined with the fact that the *DM* always plays *A* for  $\mathcal{NS}$ , it is clear that when  $q \leq \frac{(1 - q)\kappa}{\beta + \phi}$ , *DM* invariantly plays *A* for both the  $\mathcal{S}$  and  $\mathcal{NS}$  strategies of the *APP*. In this case, if *MA* deviates and plays  $\mathcal{NS}$  it will gain  $\alpha - c^{\mathcal{NS}}$  compared to  $\alpha + u - c^{\mathcal{S}}$  if it plays  $\mathcal{S}$ . Similarly, *HA* will gain  $\sigma - c^{\mathcal{NS}}$  instead of  $\sigma + v - c^{\mathcal{S}}$  if it plays  $\mathcal{S}$ . Therefore, in order to make *APP* indifferent between playing  $\mathcal{S}$  and  $\mathcal{NS}$  so that a hybrid equilibrium can be achieved at  $(\mathcal{S}, (\mathcal{S}, \mathcal{NS}))$ , the following conditions must be satisfied:

$$\alpha - c^{\mathcal{NS}} \simeq \alpha + u - c^{\mathcal{S}} \equiv c^{\mathcal{S}} - c^{\mathcal{NS}} \simeq u$$

$$\sigma - c^{\mathcal{NS}} \simeq \sigma + v - c^{\mathcal{S}} \equiv c^{\mathcal{S}} - c^{\mathcal{NS}} \simeq v$$

In summary, a hybrid equilibrium is possible at  $(\mathcal{S}, (\mathcal{S}, \mathcal{NS}))$  if and only if the above conditions hold.

In order to conserve space, we omitted the proofs for hybrid equilibria on the *APP* strategies  $(\mathcal{NS}, (\mathcal{S}, \mathcal{NS}))$ ,  $((\mathcal{S}, \mathcal{NS}), \mathcal{S})$  and  $((\mathcal{S}, \mathcal{NS}), \mathcal{NS})$ . The proofs for all these three strategies follow an analogous methodology, all of which result in a hybrid equilibrium under certain conditions. Table 2 summarizes these equilibrium conditions for all the hybrid equilibria in the game  $\mathbb{G}_D$ .

**Theorem 4.** *There exists a mixed strategy PBNE in the game  $\mathbb{G}_D$ .*

*Proof.* First, let's determine the conditions for each *APP* type to randomize (or be indifferent) between its choices. Let's assume *DM* plays the mixed strategy  $(yB, (1 - y)A)$  for  $\mathcal{S}$  (i.e., suspicious requests) and  $(xB, (1 - x)A)$  for  $\mathcal{NS}$  (i.e., non-suspicious requests). Then for the *APP* type *MA*, the expected utilities/payoffs of playing  $\mathcal{S}$  and  $\mathcal{NS}$  are:

$$EU_{MA}(\mathcal{S}) = y \times -\tau + (1 - y) \times (\alpha + u - c^{\mathcal{S}})$$

Table 2: List of PBNEs.

Conditions	Range of $\theta$	PBNE Profiles
--	$\theta \geq \frac{\kappa}{\beta + \kappa + \phi}$	$\mathcal{PBNE} = \{(S, S), (B, B), p, q\}$
$v \geq c^S - c^{\mathcal{NS}}, u \geq c^S - c^{\mathcal{NS}}$	$\theta \leq \frac{\kappa}{\beta + \kappa + \phi}$	$\mathcal{PBNE} = \{(S, S), (A, A), p, q\}$
--	$\theta \leq \frac{\kappa}{\beta + \kappa + \phi}$	$\mathcal{PBNE} = \{(S, S), (A, B), p, q\}$
--	$\theta \geq \frac{\kappa}{\beta + \kappa + \phi}$	$\mathcal{PBNE} = \{(\mathcal{NS}, \mathcal{NS}), (B, B), p, q\}$
$v \leq c^S - c^{\mathcal{NS}}, u \leq c^S - c^{\mathcal{NS}}$	$\theta \leq \frac{\kappa}{\beta + \kappa + \phi}$	$\mathcal{PBNE} = \{(\mathcal{NS}, \mathcal{NS}), (A, A), p, q\}$
--	$\theta \leq \frac{\kappa}{\beta + \kappa + \phi}$	$\mathcal{PBNE} = \{(\mathcal{NS}, \mathcal{NS}), (B, A), p, q\}$
$c^S - c^{\mathcal{NS}} \simeq u, c^S - c^{\mathcal{NS}} \simeq v$	$q \leq \frac{(1-q)\kappa}{\beta + \phi}$	$\mathcal{PBNE} = \{(S, (S, \mathcal{NS})), (A, A), p, q\}$
$c^S - c^{\mathcal{NS}} \simeq u, c^S - c^{\mathcal{NS}} \simeq v$	$p \leq \frac{(1-p)\kappa}{\beta + \phi}$	$\mathcal{PBNE} = \{(\mathcal{NS}, (S, \mathcal{NS})), (A, A), p, q\}$
--	$q \geq \frac{(1-q)\kappa}{\beta + \phi}$	$\mathcal{PBNE} = \{((S, \mathcal{NS}), S), (B, B), p, q\}$
--	$p \geq \frac{(1-p)\kappa}{\beta + \phi}$	$\mathcal{PBNE} = \{((S, \mathcal{NS}), \mathcal{NS}), (B, B), p, q\}$

$$EU_{MA}(\mathcal{NS}) = x \times -\tau + (1-x) \times (\alpha - c^{\mathcal{NS}})$$

$MA$  is indifferent between playing  $\mathcal{S}$  and  $\mathcal{NS}$  if  $EU_{MA}(\mathcal{S}) = EU_{MA}(\mathcal{NS})$ , which gives:

$$y(\tau + \alpha + u - c^S) - x(\tau + \alpha - c^{\mathcal{NS}}) = u - c^S + c^{\mathcal{NS}} \quad (1)$$

Similarly, for the  $APP$  type  $HA$ , the expected utilities/payoffs of playing  $\mathcal{S}$  and  $\mathcal{NS}$  are:

$$EU_{HA}(\mathcal{S}) = y \times -\gamma + (1-y) \times (\sigma + v - c^S)$$

$$EU_{HA}(\mathcal{NS}) = x \times -\gamma + (1-x) \times (\sigma - c^{\mathcal{NS}})$$

$HA$  is indifferent between playing  $\mathcal{S}$  and  $\mathcal{NS}$  if  $EU_{HA}(\mathcal{S}) = EU_{HA}(\mathcal{NS})$ , which gives:

$$y(\gamma + \sigma + v - c^S) - x(\gamma + \sigma - c^{\mathcal{NS}}) = v - c^S + c^{\mathcal{NS}} \quad (2)$$

Solving Equations 1 and 2 for  $x$  and  $y$ , we get  $DM$ 's mixed strategy for which each  $APP$  type is indifferent between playing  $\mathcal{S}$  and  $\mathcal{NS}$ . Let this  $x = x^*$  and  $y = y^*$ .

Now let's determine the conditions for  $DM$  to randomize (or be indifferent) between its choices. First, if  $DM$  observes  $APP$  ( $MA$  or  $HA$ ) played  $\mathcal{S}$ , its expected payoffs from playing  $B$  and  $A$  are:

$$EU_{DM}(\mathcal{B}) = q \times (\beta - \psi^S) + (1-q) \times (-\kappa - \psi^S)$$

$$EU_{DM}(\mathcal{A}) = q \times (-\phi - \psi^S) + (1-q) \times -\psi^S$$

Now,  $DM$  is indifferent between playing  $B$  and  $A$  on seeing  $\mathcal{S}$  if,  $EU_{DM}(\mathcal{B}) = EU_{DM}(\mathcal{A})$ , which gives:

$$q = \frac{\kappa}{\kappa + \beta + \phi} = q^*$$

Similarly,  $DM$ 's expected utilities/payoffs from playing  $B$  and  $A$ , when it sees  $\mathcal{NS}$  are:

$$EU_{DM}(\mathcal{B}) = p \times (\beta - \psi^{NS}) + (1 - p) \times (-\kappa - \psi^{NS})$$

$$EU_{DM}(\mathcal{A}) = p \times (-\phi - \psi^{NS}) + (1 - p) \times -\psi^{NS}$$

$DM$  is indifferent between playing  $B$  and  $A$  on seeing  $\mathcal{NS}$  if  $EU_{DM}(\mathcal{B}) = EU_{DM}(\mathcal{A})$ , which gives:

$$p = \frac{\kappa}{\kappa + \beta + \phi} = p^*$$

Now, we determine  $APP$  ( $MA$  or  $HA$ ) randomization (mixed strategy) that is consistent with  $DM$ 's beliefs. For that, we use Bayes rule to calculate the  $DM$ 's beliefs  $q$  and  $p$  as:

$$q = q^* = \frac{m \times \theta}{m \times \theta + n \times (1 - \theta)} \quad (3)$$

$$p = p^* = \frac{(1 - m) \times \theta}{(1 - m) \times \theta + (1 - n) \times (1 - \theta)} \quad (4)$$

We can solve Equations 3 and 4 for  $m$  and  $n$ , to obtain  $MA$ 's and  $HA$ 's mixed strategy for which they are indifferent in playing  $\mathcal{S}$  and  $\mathcal{NS}$  consistent with the  $DM$ 's beliefs. It is easy to show that there exists a system of (cost/benefit) parameters for which such a solution exists. Let these solutions be represented as  $m^*$  and  $n^*$ . Then, the mixed strategy PBNE  $\mu^*$  will occur at:

$\mu_{APP}^*$ :  $MA$  plays  $(m^* \mathcal{S} + (1 - m^*) \mathcal{NS})$  and  $HA$  plays  $(n^* \mathcal{S} + (1 - n^*) \mathcal{NS})$

$\mu_{DM}^*$ :  $DM$  plays  $y^* B + (1 - y^*) A$  to  $\mathcal{S}$  and  $x^* B + (1 - x^*) A$  to  $\mathcal{NS}$

$DM$ 's beliefs:  $q = Pr(MA|\mathcal{S}) = q^*$  and  $p = Pr(MA|\mathcal{NS}) = p^*$

Example of a mixed equilibrium: Substituting  $\theta = \frac{1}{2}$ ,  $q = \frac{1}{4}$  and  $p = \frac{3}{4}$  in Equations 3 and 4, and solving for  $m$  and  $n$ , results in  $m = \frac{1}{4}$  and  $n = \frac{3}{4}$ .

## 4 Numerical Analysis

We perform numerical simulations to analyze how the various PBNEs in our Sensor Access Signaling Game  $\mathbb{G}_D$  evolves with respect to the various game and system parameters. Specifically, we evaluate the  $MA$ 's payoff,  $HA$ 's payoff and  $DM$ 's expected utility ( $EU_{DM}$ ) in a representative separating strategy profile  $(\mathcal{S}, \mathcal{NS})$ , a pooling strategy profile  $(\mathcal{S}, \mathcal{S})$ , a hybrid strategy profile  $((\mathcal{S}, \mathcal{NS}), \mathcal{S})$  and a mixed strategy profile, by varying the value of  $\theta$  (Nature's selection probability). The results are outlined in Figure 2, and the set of system parameters chosen for the numerical simulations are summarized in Figure 2f. The parametric values chosen for our numerical analysis were primarily to showcase the trends observable in different strategy profiles. They may or may not be reflective of their values in real-life, but we did our best to establish the inequalities between parameters as completely as possible.

**Separating strategy  $(\mathcal{S}, \mathcal{NS})$ .** As proved earlier, there is no equilibrium in any of the separating strategy profiles, and the same can also be observed in Figure

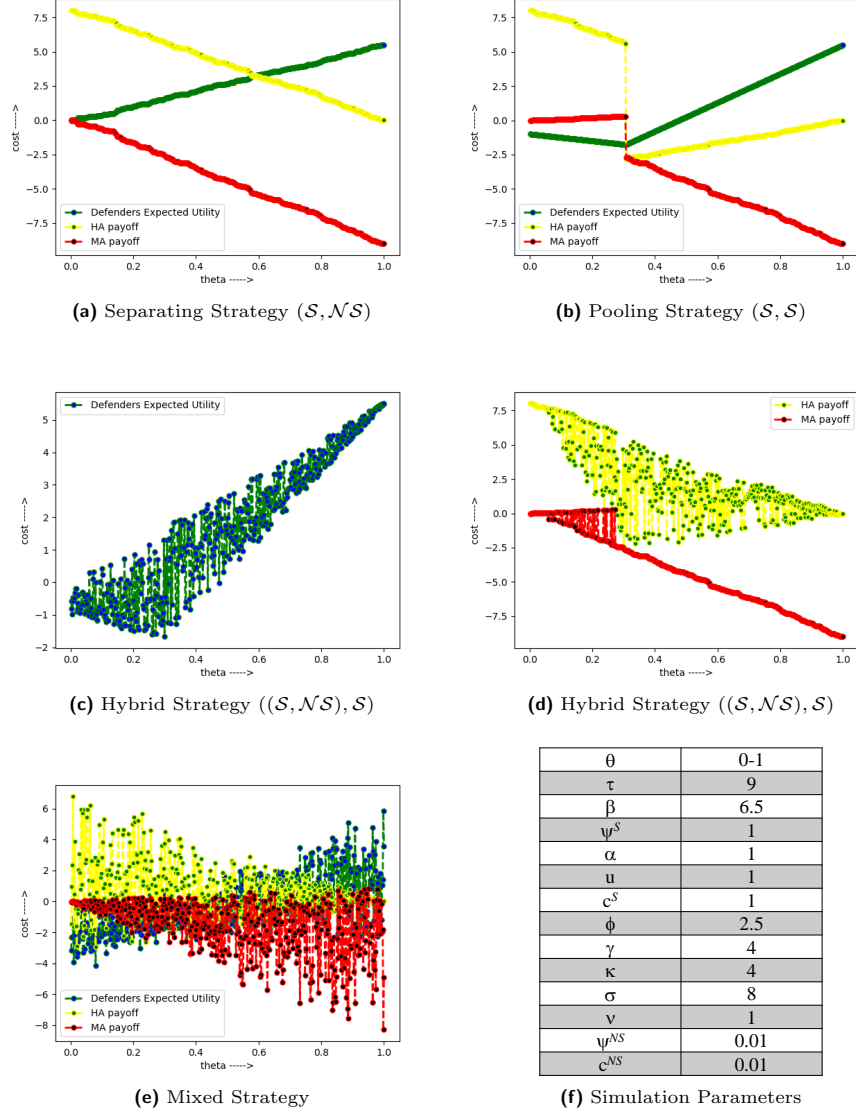


Fig. 2: (a-e) Effect of  $\theta$  on different strategy profiles. Each point is a average of 500 iterations. (f) Default simulation parameters.



2a. We observe that  $EU_{DM}$  is linearly increasing, which implies that  $DM$  is blocking suspicious requests from  $MA$ , as the only way  $DM$  can increase its utility is by playing  $B$ . Both  $MA$ 's and  $HA$ 's payoffs are linearly decreasing because  $DM$  is playing  $B$  more than  $A$ .

**Pooling strategy  $(S, S)$ .** In Figure 2b we observe that the  $HA$ 's payoff and  $DM$ 's expected utility initially decrease while  $MA$ 's payoff increases, for increasing values of  $\theta$ . However, beyond a certain value of  $\theta$  the trend reverses, i.e.,  $HA$ 's payoff and  $DM$ 's expected utility increase linearly while  $MA$ 's payoff decreases.

**Hybrid strategy  $((S, \mathcal{NS}), S)$ .** In this strategy profile (Figure 2c),  $EU_{DM}$  is affected by random signals coming from  $MA$ . However, we can also observe that as  $\theta$  increases  $EU_{DM}$  gradually increases.  $EU_{DM}$  also stabilized for higher values of  $\theta$ . On the other hand,  $HA$ 's and  $MA$ 's payoffs are decreasing as expected when increasing  $\theta$  (Figure 2d).

**Mixed strategy.** In Figure 2e we observe the effect of a mixed strategy in each player's payoff/utility. The payoffs and utilities are highly unstable as  $m$ ,  $n$ ,  $x$  and  $y$  are all drawn from a random distribution for the mixed strategy.

In summary, our numerical evaluations validate our game-theoretic results.

## 5 Repeated Game

So far, we have outlined PBNE results and related numerical analysis for the Sensor Access Signaling Game  $\mathbb{G}_D$  in the single stage (or single-shot) scenario. In practice, however, the game  $\mathbb{G}_D$  will be *repeated* several times (possibly, as long as the system is running). Thus, it is important to analyze how the game  $\mathbb{G}_D$  will evolve in a repeated scenario.

### 5.1 Background

Before proceeding ahead, let us provide some technical background on repeated games. There are two broad categories of repeated games:

**(i) Finite Repeated Games:** Here, a stage game is repeated for a *finite* number of times. Repeated games could support strategy profiles (also known as *reward* and *punishment* strategies) that support deviation from stage game Nash Equilibria through cooperation. Players could cooperate and play a reward strategy (also referred to as a *Subgame Perfect Equilibrium* (SPE)) that is not a Nash Equilibrium strategy, if the expected utility of every player is strictly greater than the expected utility from the Nash Equilibrium strategy [20]. Due to the lower expected utility, the Nash Equilibrium strategy becomes the *punishment* strategy, which would be applied if any of the players deviate from the SPE. However, if a finite repeated game consists of stage games that each have a unique Nash Equilibrium, then the repeated game also has a unique SPE of playing the stage game Nash Equilibrium in each stage. This can be explained by *unravelling* from the last stage, where players must play the unique Nash Equilibrium. In the second-to-last stage, as players cannot condition the future (i.e., the last stage) outcomes, again they must play the unique Nash

Equilibrium for optimal expected utility. This backward induction continues until the first stage of the game, implying that players must always play the Nash Equilibrium strategy to ensure overall optimal expected utility. This (players not cooperating on a reward strategy) is a limitation of finite repeated games with a unique Nash Equilibrium, that can be solved if the game is repeated infinitely.

**(ii) Infinite Repeated Games:** In a repeated game with an infinite (or unknown) number of stages, players can condition their present actions upon the unknown future. Without a known end stage, players will be more inclined to cooperate on a mutually beneficial reward strategy, rather than a static Nash Equilibrium as seen in a finite repeated game. The payoff/utility for a player  $i$  in an infinite repeated game can be computed by discounting the expected utilities in future stages using a *discount factor*  $\delta$  ( $0 \leq \delta \leq 1$ ) as:

$$u_i = u_i^1 + \delta u_i^2 + \delta^2 u_i^3 + \dots + \delta^{t-1} u_i^{t-1} + \dots = \sum_{t=1}^{\infty} \delta^{t-1} u_i^t$$

And, the average (normalized) expected utility for player  $i$  is  $(1-\delta) \sum_{t=1}^{\infty} \delta^{t-1} u_i^t$ . In an infinitely repeated game, players can effectively employ a *reward-and-punishment* strategy, but to do so each player must maintain a *history* of the past actions taken by all players. Let  $H_t$  denote the set of all possible histories ( $h_t$ ) of length  $t$  and let  $H = \cup_{t=1}^{\infty} H_t$  be the set of all possible histories. A pure strategy ( $\omega_i$ ) for player  $i$  is a mapping  $\omega_i : H \rightarrow \Omega_i$  that maps histories ( $H$ ) into player actions ( $\Omega_i$ ) of the stage game. In an infinitely repeated game  $\mathbb{G}(t, \delta)$  of  $n$  players, a strategy profile  $\omega = (\omega_1, \dots, \omega_n)$  is a Subgame Perfect Equilibrium (SPE) if and only if there is no player  $i$  and no single history  $h_{t-1}$  for which player  $i$  would gain by deviating from  $\omega_i(h_{t-1})$ . Next, let us analyze the Sensor Access Signaling Game  $\mathbb{G}_D$  for the infinite repeated scenario.

## 5.2 Repeated $\mathbb{G}_D$ with History: A Case Study

Let us analyze one of the possible scenarios of an infinitely repeated game  $\mathbb{G}_D(t)$ , where we assume  $\{(\mathcal{S}, \mathcal{NS}), \mathcal{NS}, (B, A), q, p\}$  as the *reward* strategy and  $\{(\mathcal{S}, \mathcal{NS}), \mathcal{NS}, (B, B), q, p\}$  as the *punishment* strategy. In this scenario,  $HA$  may start sending  $\mathcal{S}$  at a later point in the game in order to increase its payoff from  $\sigma - c^{\mathcal{NS}}$  to  $\sigma + v - c^{\mathcal{S}}$ . However, as each player maintains a history of action sets for every player, as soon as  $HA$  deviates from the SPE,  $DM$  will enforce the *punishment* strategy profile, thus blocking all the incoming requests whether it is  $\mathcal{S}$  or  $\mathcal{NS}$ .  $MA$  is randomizing between  $\mathcal{S}$  and  $\mathcal{NS}$  according to the feasible reward strategy profile, so it does not matter to  $DM$  if  $MA$  deviates or not. It is not logical to assume that  $DM$  will deviate as it is  $DM$ 's responsibility to keep check on the deviations of  $APP$ . Moreover, each stage in the game  $\mathbb{G}_D(t)$  is a sequential game, where  $DM$  reacts to  $APP$ 's signal in every stage of the game.

After each stage of the game, the set of actions of player  $APP$  and the corresponding responses of player  $DM$  will be known to all players. Players may change their strategy after a certain period or stage, based on the history information until that stage. Figure 3a shows the effect of history on the repeated games. We observe that  $HA$ 's utility fluctuates whenever it deviates from the

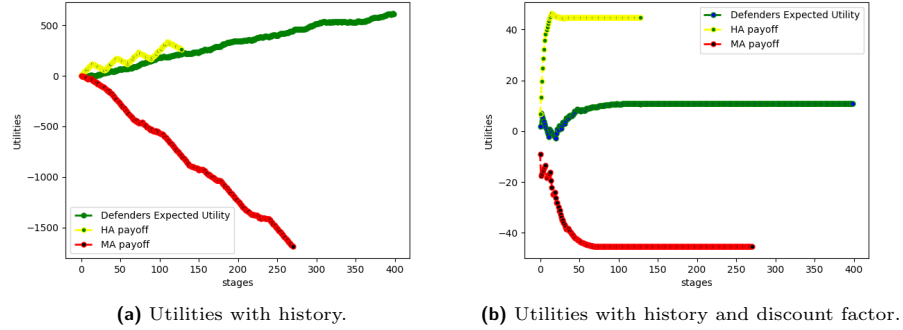


Fig. 3: Cumulative utilities for  $DM$ ,  $MA$ , and  $HA$  in repeated games.

cooperative reward strategy. With a strategy reset interval of 100 stages, we observe that  $HA$ 's utility follows a up-down pattern in every interval, reflective of a start with reward strategy, then  $HA$ 's deviation from reward strategy, and followed by  $DM$ 's switch to the punishment strategy. Overall,  $MA$ 's cumulative payoff is lower than  $HA$ 's cumulative payoff, which is desired in our system as we want the  $DM$  to thwart  $MA$  while allowing  $HA$  to function normally.

We also study the effect of *discount factor*  $\delta$  (on the game  $\mathbb{G}_D(t, \delta)$ ), which determines players' patience. If the value of  $\delta$  is high, then there is a high chance that game is going to progress to the next stage, prompting player to cooperate on the reward strategy for longer. In Figure 3b, we initially observe  $HA$ 's utility increasing and  $MA$ 's utility decreasing as per the reward strategy. However, as the game progresses, the cumulative utilities converge because (i) the utilities are heavily discounted, and (ii) players switch to the Nash Equilibrium strategy as a result of the discounted utility.

## 6 Related Work

Several recent works demonstrated the feasibility of side-channel inference attacks using mobile [5, 24, 1, 21, 14, 19, 8, 17, 6, 15, 16, 18] and wearable [10, 26, 12, 25, 11, 23, 13] device sensors. Some of these works also propose defense mechanism against the specific type of attack that was demonstrated. For example, Miluzzo et al. [17] proposed to drastically reduce the maximum allowed sensor sampling rate, in order to prevent keystroke inference attacks on mobile keypads using mobile device motion sensors. However, reducing the sensor sampling rate for all applications may cause certain applications to malfunction, leading to poor user experience. To minimize unnecessary regulation of sensors at all times, Maiti et al. [12] proposed an activity recognition-based defense framework. In their framework, the defense mechanism continuously monitors user's current activity (using smartwatch motion sensors data), and regulates third

party applications’ access to motion sensor only when typing activity is detected (in order to prevent keystroke inference). However, while such ad-hoc defense approaches are effective in preventing a specific type of attack, they may not be effective against other types of side-channel attacks. In this work, we generalize the problem of side-channel attacks using mobile and wearable sensors, by modeling all different types of attacks as a Bayesian signaling game between a mobile application and a defense mechanism [22].

## 7 Conclusion

In this paper, we modeled the problem of zero-permission sensor access control for mobile applications using game theory. By means of a formal and practical signaling game model, we proved conditions under which equilibria can be achieved between entities with conflicting goals in this setting, i.e., honest and malicious applications who are requesting sensor access to maximize their utility and attack goals, respectively, and the defense mechanism who wants to protect against attacks without compromising system utility. By means of numerical simulations, we further studied how the different theoretically derived equilibria will evolve in terms of the payoffs received by the application and the defense mechanism. Our results in this paper have helped shed light on how a defense mechanism can act in a strategically optimal manner to protect the mobile system against malicious applications that take advantage of zero-permission sensors to leak private user information and are impossible to detect otherwise.

## Acknowledgment

Research reported in this publication was supported by the Division of Computer and Network Systems (CNS) of the National Science Foundation (NSF) under award number 1828071 (originally 1523960).

## References

1. Cai, L., Chen, H.: Touchlogger: Inferring keystrokes on touch screen from smartphone motion. In: HotSec (2011)
2. Cai, L., Machiraju, S., Chen, H.: Defending against sensor-sniffing attacks on mobile phones. In: ACM MobiHeld. pp. 31–36 (2009)
3. Cho, I.K., Kreps, D.M.: Signaling games and stable equilibria. *The Quarterly Journal of Economics* **102**(2), 179–221 (1987)
4. Felt, A.P., Chin, E., Hanna, S., Song, D., Wagner, D.: Android permissions demystified. In: ACM CCS. pp. 627–638 (2011)
5. Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D.: A survey of mobile malware in the wild. In: ACM SPSM (2011)
6. Gao, X., Firner, B., Sugrim, S., Kaiser-Pendergrast, V., Yang, Y., Lindqvist, J.: Elastic pathing: Your speed is enough to track you. In: ACM UbiComp (2014)

7. Hammad, M., Bagheri, H., Malek, S.: Determination and enforcement of least-privilege architecture in android. In: IEEE ICSA. pp. 59–68 (2017)
8. Han, J., Owusu, E., Nguyen, L., Perrig, A., Zhang, J.: Accomplice: Location inference using accelerometers on smartphones. In: ACM COMSNETS (2012)
9. Kumari, K., Jadliwala, M., Maiti, A.: Analyzing Defense Strategies Against Mobile Information Leakages: A Game-Theoretic Approach (Full Report). <https://sprite.utsa.edu/art/defender> (2019), online; accessed 2019-04-30
10. Liu, X., Zhou, Z., Diao, W., Li, Z., Zhang, K.: When good becomes evil: Keystroke inference with smartwatch. In: ACM CCS. pp. 1273–1285 (2015)
11. Maiti, A., Jadliwala, M., He, J., Bilogrevic, I.: Side-channel inference attacks on mobile keypads using smartwatches. *IEEE Transactions on Mobile Computing* **17**(9), 2180–2194 (2018)
12. Maiti, A., Armbruster, O., Jadliwala, M., He, J.: Smartwatch-based keystroke inference attacks and context-aware protection mechanisms. In: ACM AsiaCCS (2016)
13. Maiti, A., Heard, R., Sabra, M., Jadliwala, M.: Towards inferring mechanical lock combinations using wrist-wearables as a side-channel. In: ACM WiSec. pp. 111–122 (2018)
14. Marquardt, P., Verma, A., Carter, H., Traynor, P.: (sp)iphone: Decoding vibrations from nearby keyboards using mobile phone accelerometers. In: ACM CCS (2011)
15. Michalevsky, Y., Boneh, D., Nakibly, G.: Gyrophone: Recognizing speech from gyroscope signals. In: USENIX Security (2014)
16. Michalevsky, Y., Nakibly, G., Veerapandian, G.A., Boneh, D., Nakibly, G.: Powerspy: Location tracking using mobile device power analysis. In: USENIX Security (2015)
17. Miluzzo, E., Varshavsky, A., Balakrishnan, S., Choudhury, R.R.: Tappprints: Your finger taps have fingerprints. In: ACM MobiSys (2012)
18. Narain, S., Vo-Huu, T.D., Block, K., Noubir, G.: Inferring user routes and locations using zero-permission mobile sensors. In: IEEE S&P (2016)
19. Nguyen, L., Cheng, H., Wu, P., Buthpitiya, S., Zhang, Y.: Pnlum: System for prediction of next location for users with mobility. In: Nokia Mobile Data Challenge Workshop (2012)
20. Osborne, M.J., Rubinstein, A.: A course in game theory. MIT press (1994)
21. Owusu, E., Han, J., Das, S., Perrig, A., Zhang, J.: Accessory: Password inference using accelerometers on smartphones. In: ACM HotMobile (2012)
22. Rahman, M.A., Manshaei, M.H., Al-Shaer, E.: A game-theoretic approach for deceiving remote operating system fingerprinting. In: 2013 IEEE Conference on Communications and Network Security (CNS). pp. 73–81. IEEE (2013)
23. Sabra, M., Maiti, A., Jadliwala, M.: Keystroke inference using ambient light sensor on wrist-wearables: A feasibility study. In: ACM WearSys (2018)
24. Schlegel, R., Zhang, K., Zhou, X., Intwala, M., Kapadia, A., Wang, X.: Sound-comber: A stealthy and context-aware sound trojan for smartphones. In: NDSS (2011)
25. Wang, C., Guo, X., Wang, Y., Chen, Y., Liu, B.: Friend or foe?: Your wearable devices reveal your personal pin. In: ACM AsiaCCS (2016)
26. Wang, H., Lai, T.T.T., Roy Choudhury, R.: Mole: Motion leaks through smart-watch sensors. In: ACM MobiCom (2015)