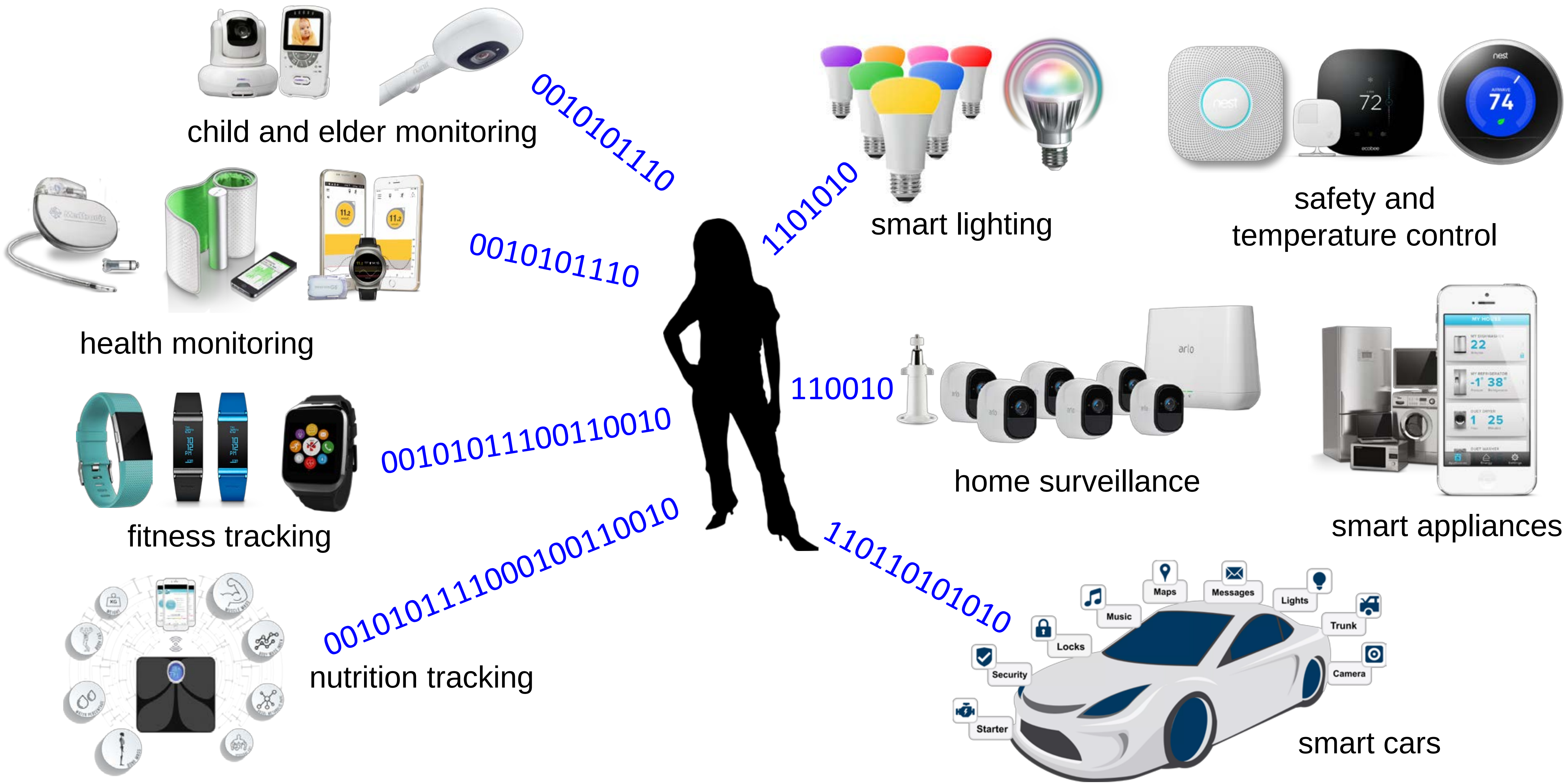
HELP: Helper-Enabled In-Band Device Pairing Resistant Against Signal Cancellation

Nirnimesh Ghose, Loukas Lazos, and Ming Li
Department of Electrical and Computer Engineering,
University of Arizona, Tucson

Presented at the :
26th USENIX Security Symposium, Vancouver

A Pervasive Network-Enabled Ecosystem

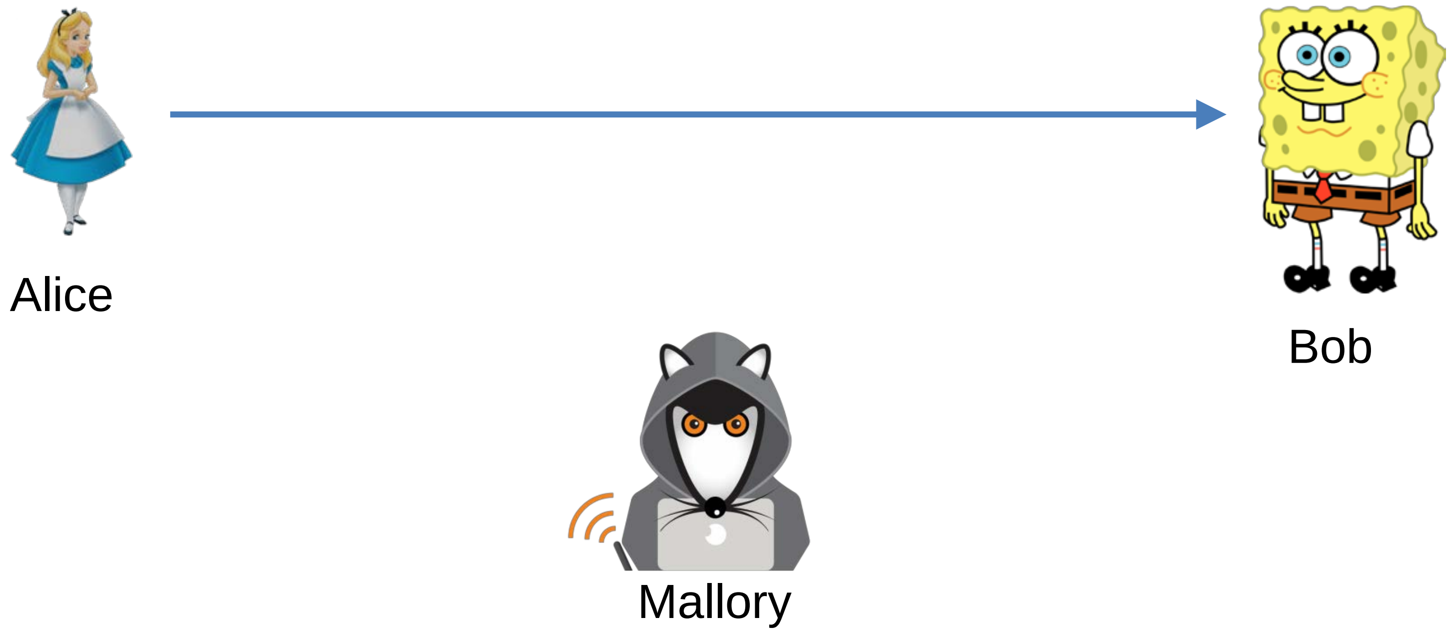


How to we secure the information flow to protect the plethora of collected sensitive data?

We need some

HELP!

Classic Trust Establishment Problem – Alice, Meet Bob



Achieve mutual authentication and key agreement in the presence of Mallory

- Authenticate the identity of Bob and Alice
- Verify the integrity of the communications
- Agree on a common secret

Problem Setup for Secure Device Pairing

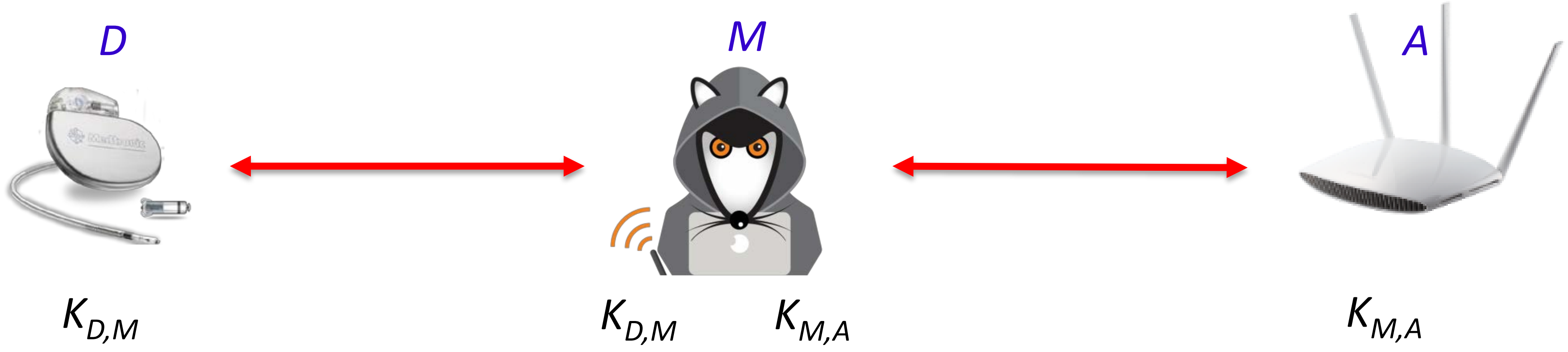
In the context of this work, securely pair new devices with a hub

By the end of the device pairing

- A has verified the authenticity of D
- *D* and *A* share a common key $K_{D,A}$

Challenge: Most new devices lack advanced interfaces such as keyboards, monitors, etc.

Threat Model

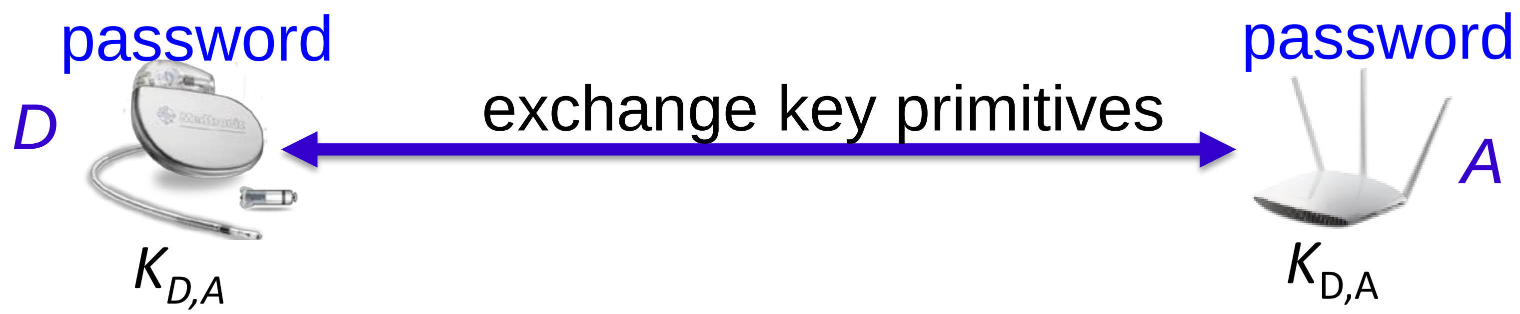


Goals: (a) pair a rogue device with the hub, (b) force *D* to join a rogue hub

Means: Perform a MitM attack over wireless

- Aware of the channel between D and A, which is predictable and relatively stable
- Aware of the D-M and M-A channels
- Can synchronize with D (by listening to preambles)
- Can perform overshadowing and/or signal cancellation attacks (worst-case adversary)

Existing Solutions for Trust Establishment



Manually enter a password to the device – requires an advanced interface

Preload password to device – manufacturers often opt for preloading the same password to multiple devices, which leads to massive vulnerabilities (Mirai botnet)

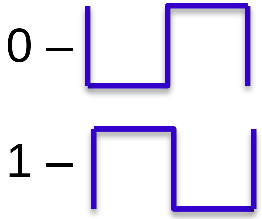
Execute a Diffie-Hellman (DH) key exchange – Vulnerable to MitM

Perform out-of-band verification using light, sound, LEDs, etc. – requires advanced interfaces

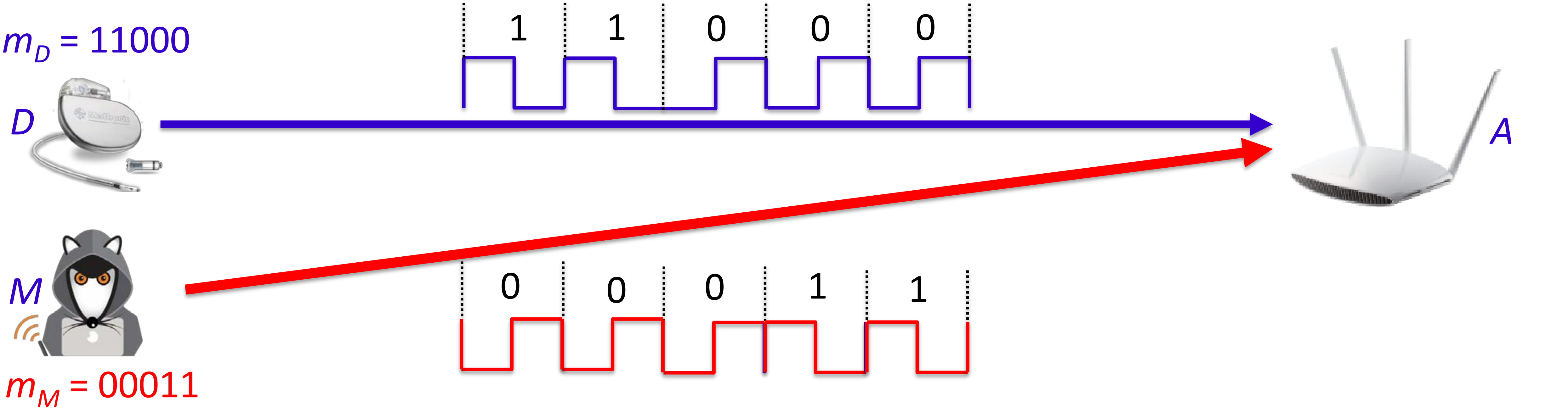
Non-cryptographic verification techniques – often require specialized hardware

In-band verification techniques – only require a common RF interface

In-Band Integrity Verification



Manchester coded ON-OFF keyed message



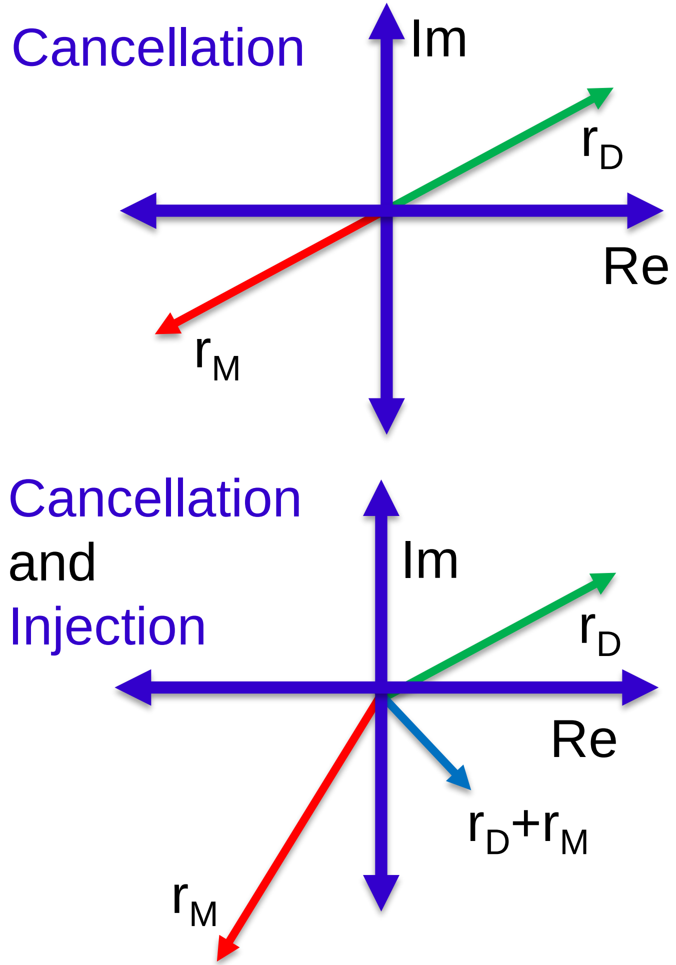
Prior works assume signal cancellation is not possible due to the rich scattering environment+ or it occurs with limited probability*

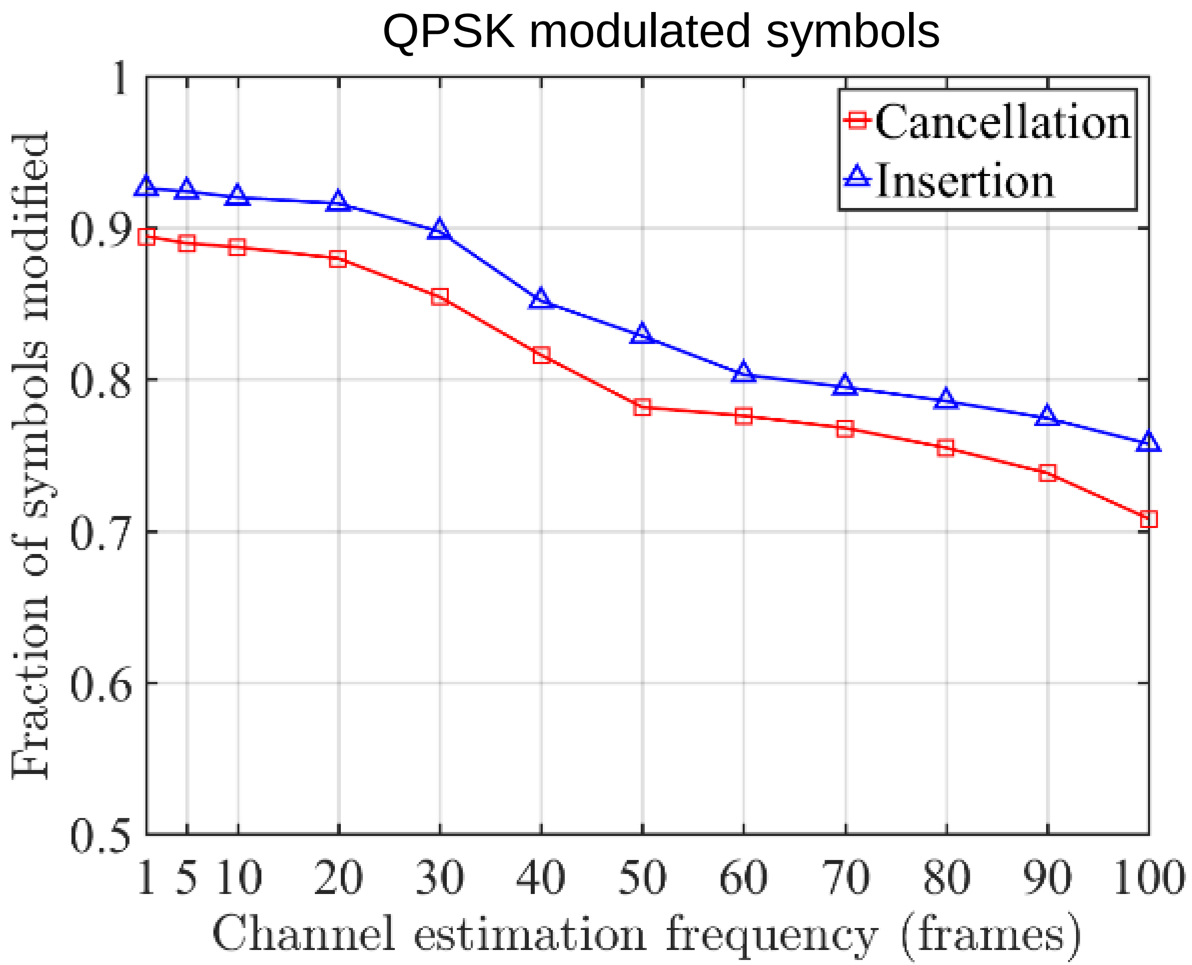
+ Čapkun, Srdjan, et al. "Integrity codes: Message integrity protection and authentication over insecure channels." *IEEE Transactions on Dependable and Secure Computing* 5.4 (2008): 208-223.
+ Gollakota, Shyamnath, et al. "Secure In-Band Wireless Pairing." In *Proc. of the USENIX security symposium*. 2011.
* Hou, Yantian, Ming Li, and Joshua D. Guttman. "Chorus: scalable in-band trust establishment for multiple constrained devices over the insecure wireless channel." In *Proc. of the sixth ACM WiSec Conference*, 2013.
* Hou, Yantian, et al. "Message Integrity Protection over Wireless Channel by Countering Signal Cancellation: Theory and Practice." In *Proc. of the 10th ACM AsiaCCS*, 2015.

Signal Manipulation Attack

The infeasibility of signal cancellation assumption does not always hold

Pöpper *et al.*[*] demonstrated an effective relay signal cancellation attack using a pair of directional antennas





* Pöpper, Christina, et al. "Investigation of Signal and Message Manipulations on the Wireless Channel." In *Proc. of the ESORICS*. Vol. 11. 2011.

Our Contributions

Constructed an in-band message integrity verification primitive, for devices that do not share any secrets

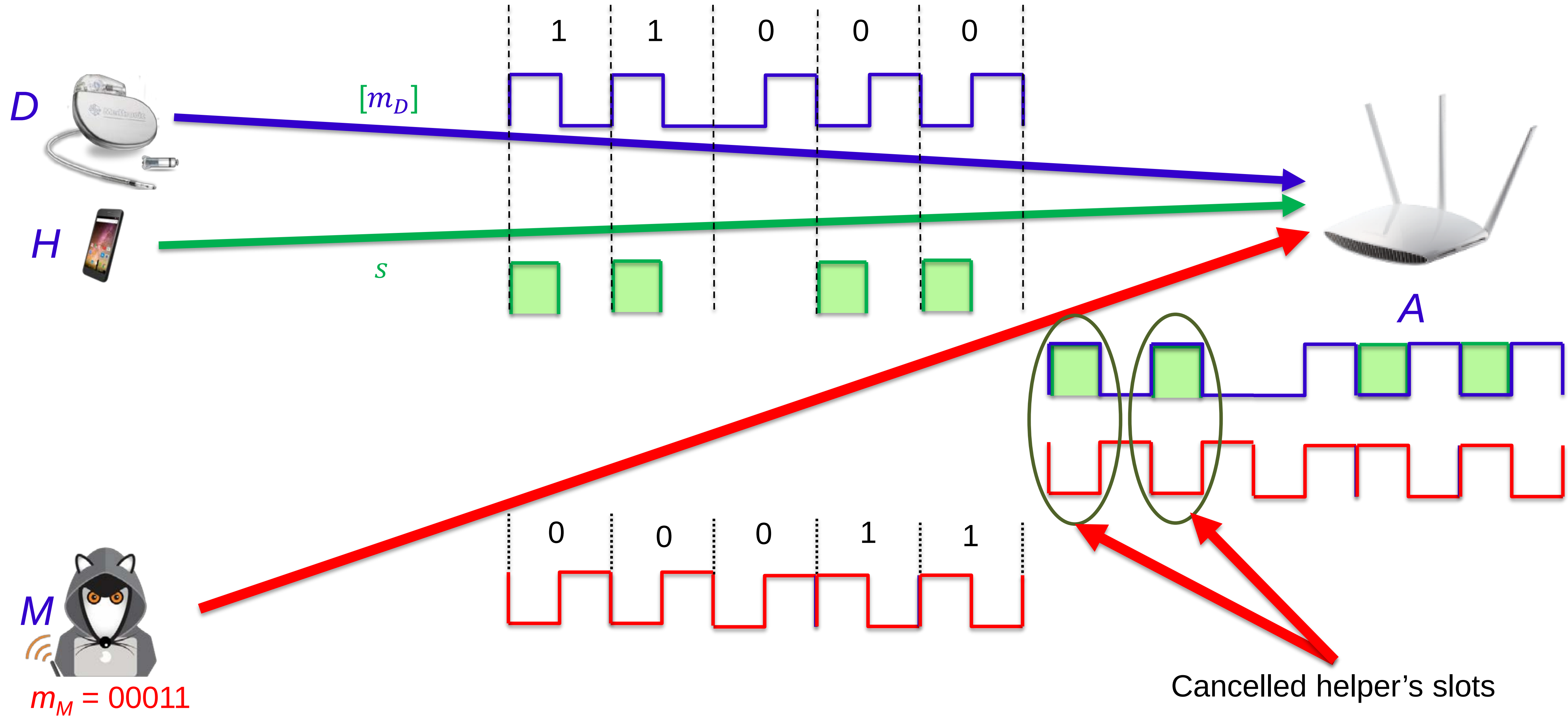
Proposed HELP, a DH-based authenticated key agreement protocol, which is the first protocol resistant to MitM attacks based on signal cancellation

Analyzed security and showed negligible success probability even if perfect signal cancellation can be achieved

Implemented HELP on the USRP testbed and validated the

- effectiveness of the primitive in detecting message injections/modifications
- the adversary’s diminishing success in pairing rogue devices

HELP – Integrity Verification Primitive



Device Pairing with HELP

$ID_{\mathrm{D}}, (G, q, g)$

$ID_{\mathrm{A}}, (G, q, g)$

Pick $X_D \in_U \mathbb{Z}_q$
$z_D \leftarrow g^{X_D} mod\ q$
$m_D \leftarrow ID_D, z_D$

Pick $X_A \in_U \mathbb{Z}_q$
$z_A \leftarrow g^{X_{BS}} mod\ q$
$m_A \leftarrow ID_{BS}, z_{BS}$

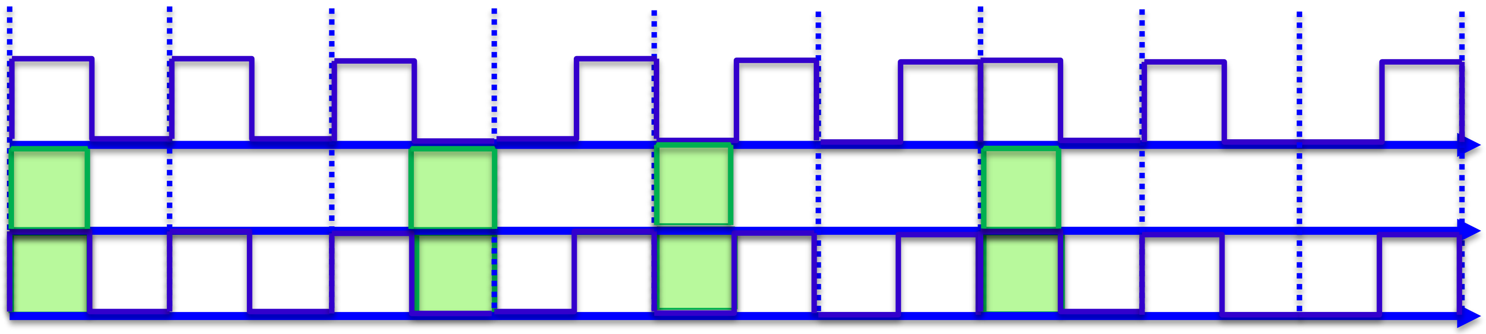
(H active) $\xrightarrow{[h(m_D), m_D] + m_H}$

(H active) $\xrightarrow{AE(s, K)}$ Verify and Extract m_D

$\xleftarrow{m_A}$

$K_{D,A} = g^{X_D X_A} mod\ q$

$K_{D,A} = g^{X_D X_A} mod\ q$



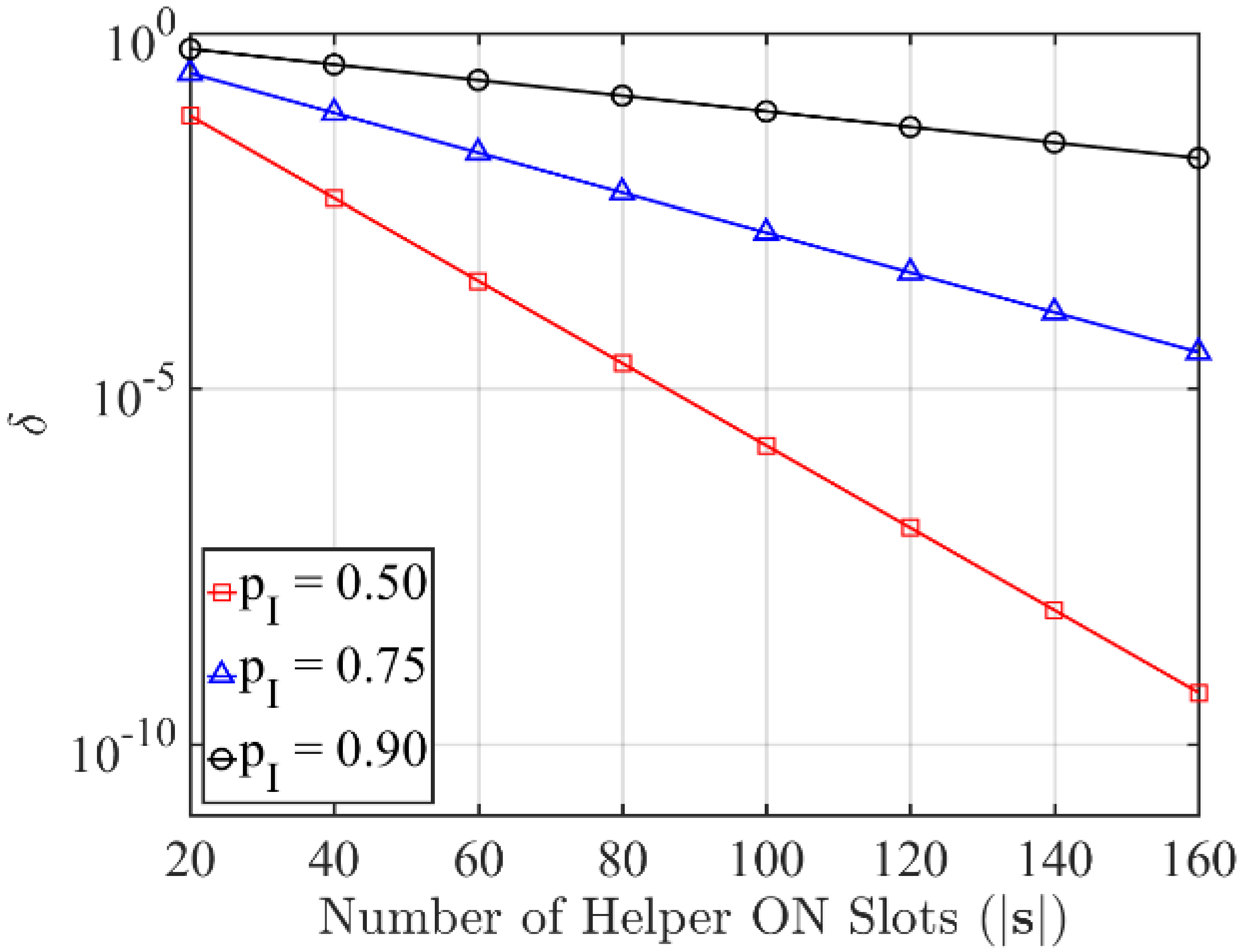
Security Analysis of the Help Primitive

probability of inferring the helper's activity during one slot

$$\delta = \left(1 - \frac{1 - p_I}{4}\right)^{|\mathbf{s}|}$$

Number of helper's ON slots

probability that the hub accepts a message forgery



Security Analysis of the Device Pairing Protocol

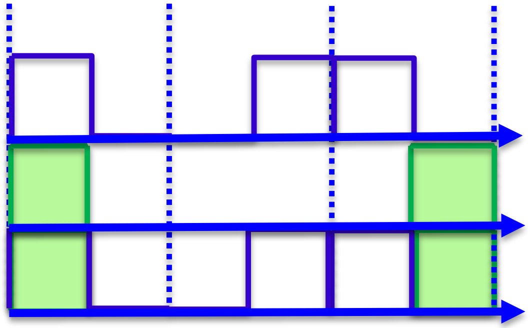
Given ID_D
(G, q, g)
Pick $X_D \in_U \mathbb{Z}_q$
$z_D \leftarrow g^{X_D} mod\ q$
$m_D \leftarrow ID_D, z_D$

Given ID_M
(G, q, g)
Pick $X_M \in_U \mathbb{Z}_q$
$z_A \leftarrow g^{X_M} mod\ q$
$m_A \leftarrow ID_M, z_M$

Given ID_A
(G, q, g)
Pick $X_A \in_U \mathbb{Z}_q$
$z_A \leftarrow g^{X_A} mod\ q$
$m_A \leftarrow ID_A, z_A$

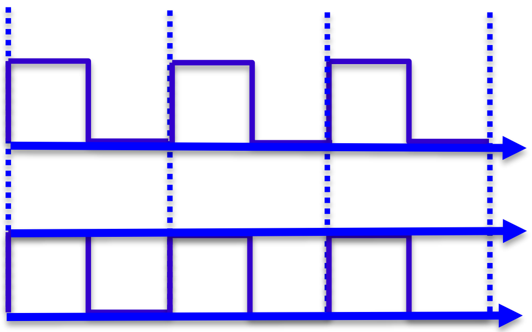
[$h(m_D)$, m_D]

(*H* active) m_H 



[$h(m_M)$, m_M]

[$h(m_D)$, m_D] + m_H



[$h(m_M)$, m_M]

(*H* active) 

AE(*s*,*K*)

AE(*s*,*K*)

Extract m_M
Fails s verification

m_M

m_A

Cancel and Inject
Fails to extract m_D
$K_{D,M} = g^{X_D X_M} mod\ q$
$K_{M,A} = g^{X_M X_A} mod\ q$

$K_{D,M} = g^{X_D X_M} mod\ q$

$K_{M,A} = g^{X_M X_A} mod\ q$

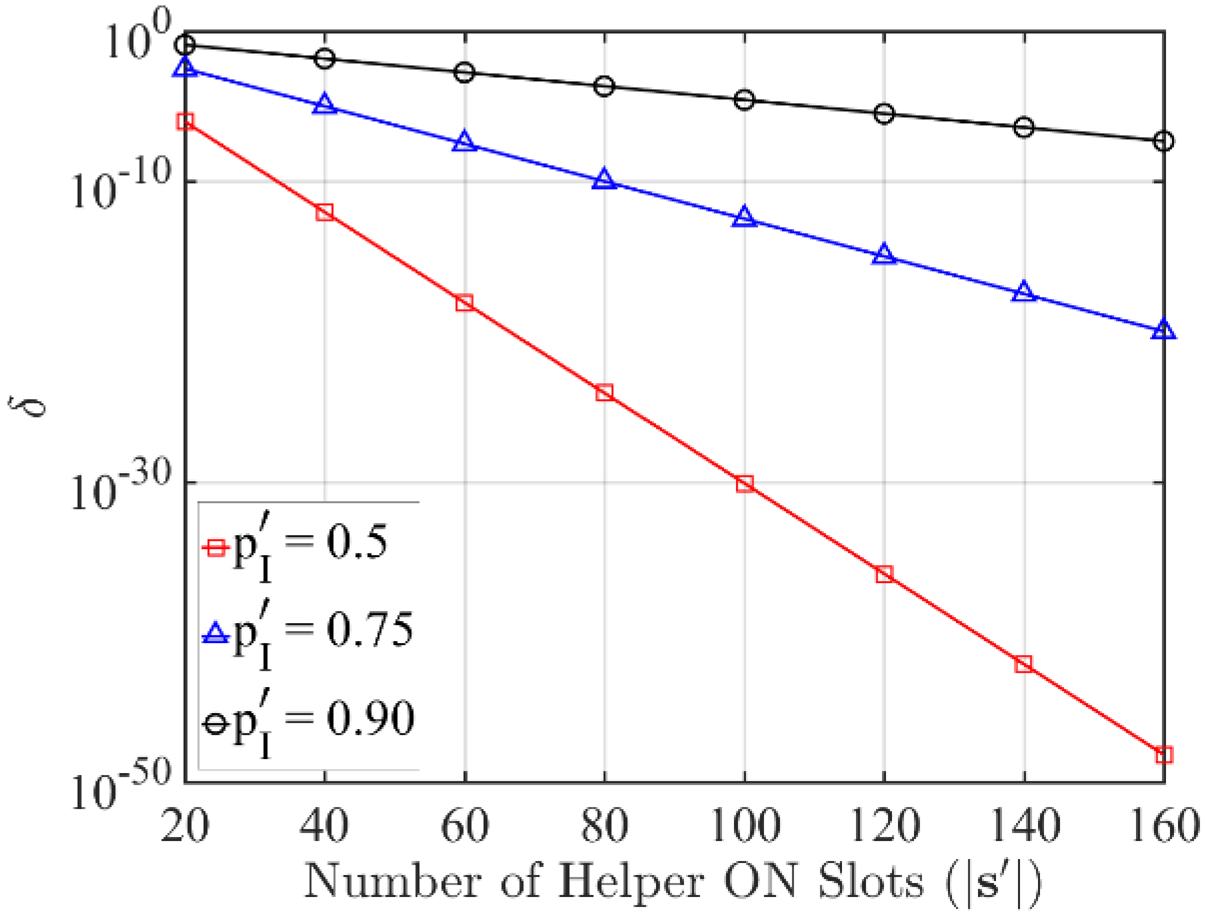
Security Analysis of the Downlink Direction

probability of inferring the helper's activity during one slot

$$\delta = (p_I')^{|\mathbf{s}'|}$$

Number of helper's ON slots

probability that the device accepts a message forgery

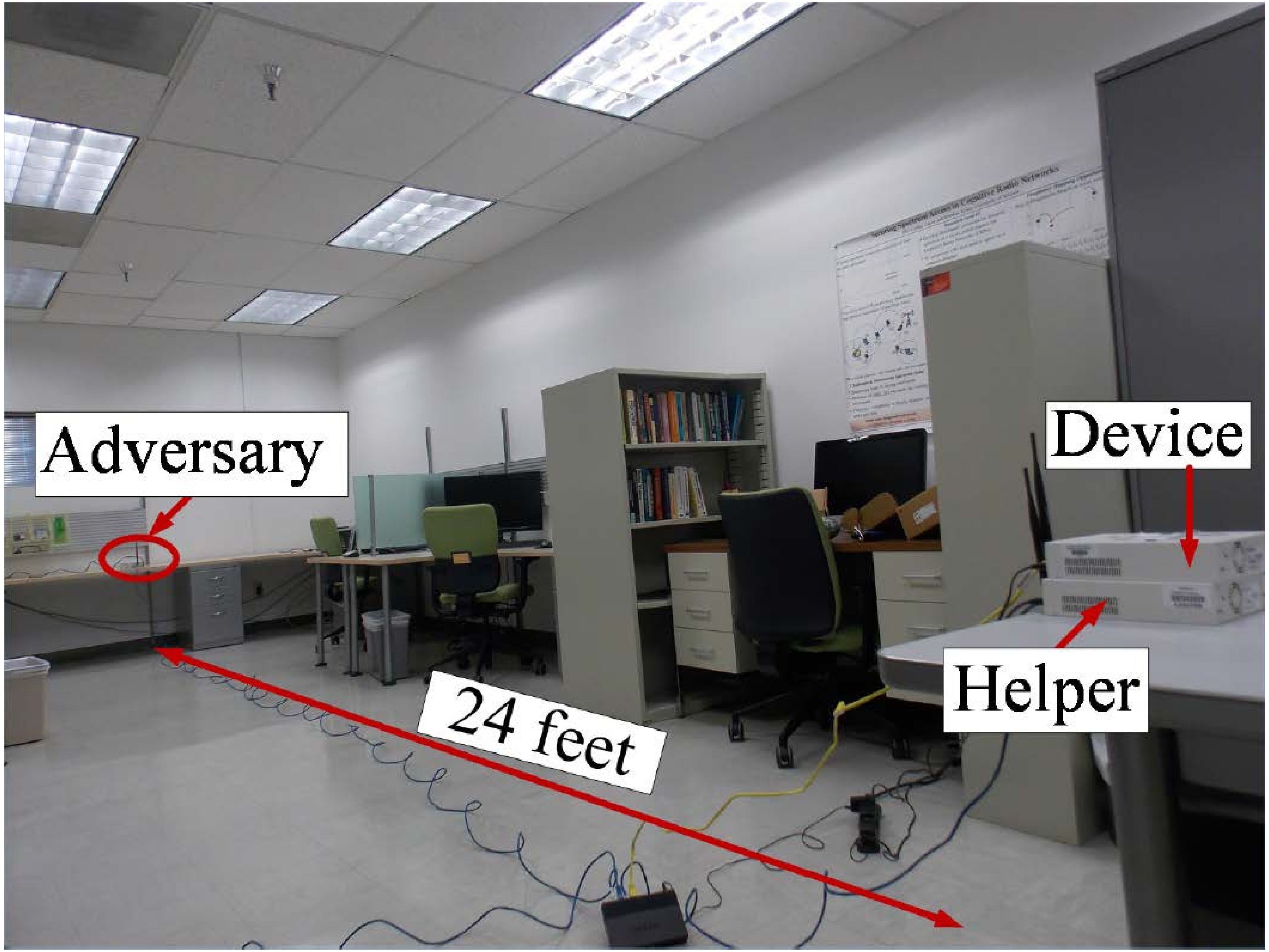


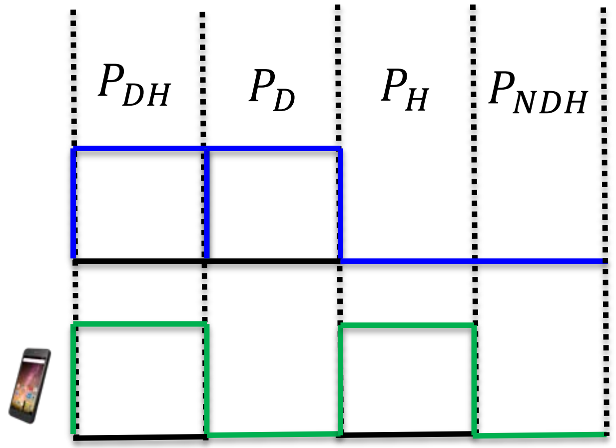
Probability of Helper Activity Inference (p_I)

Adversary's capability in timely identifying the helper's ON slot, the adversary could employ several PHY-layer characteristics:

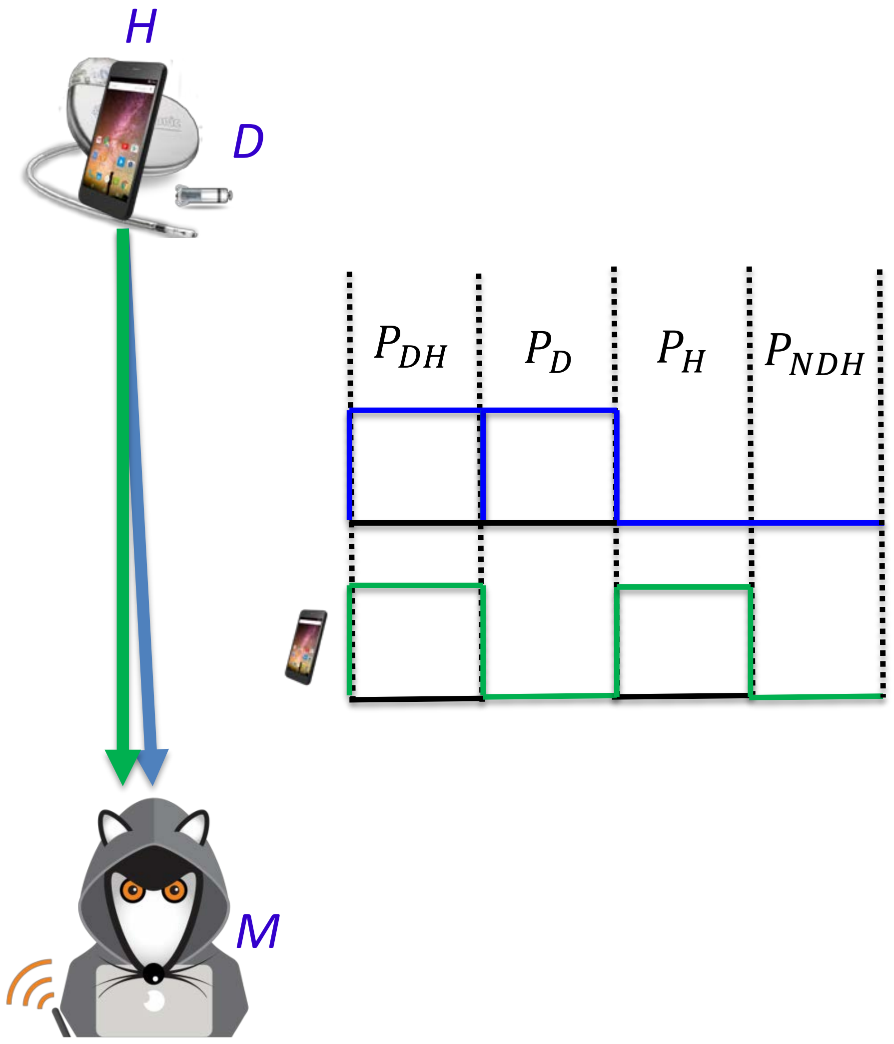
- Frequency offset
- Channel impulse response
- I/Q origin offset
- Transient radio state
- Angle of arrival for incoming signal
- Received signal strength
- Time offset

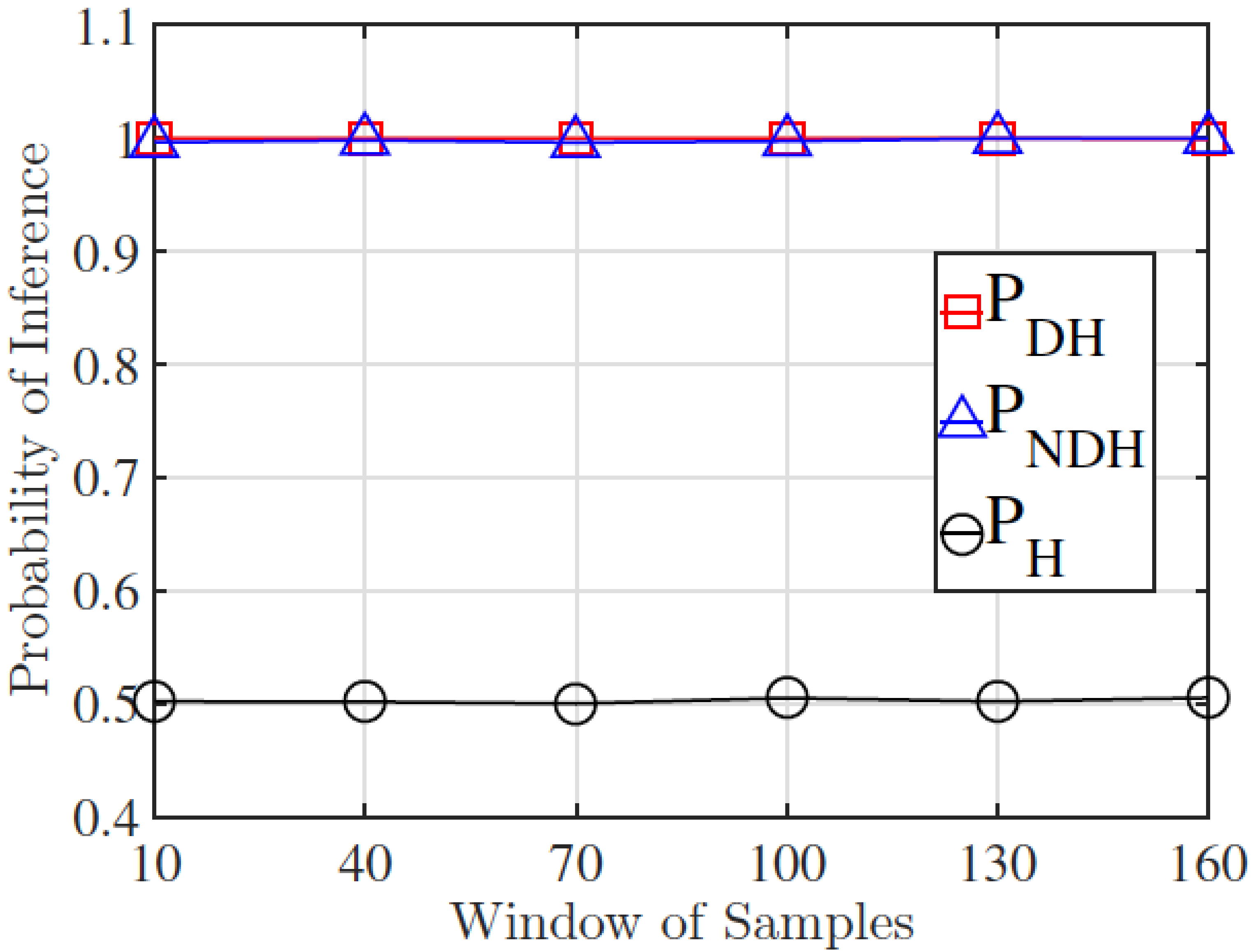
Fast Helper Detection based on RSS



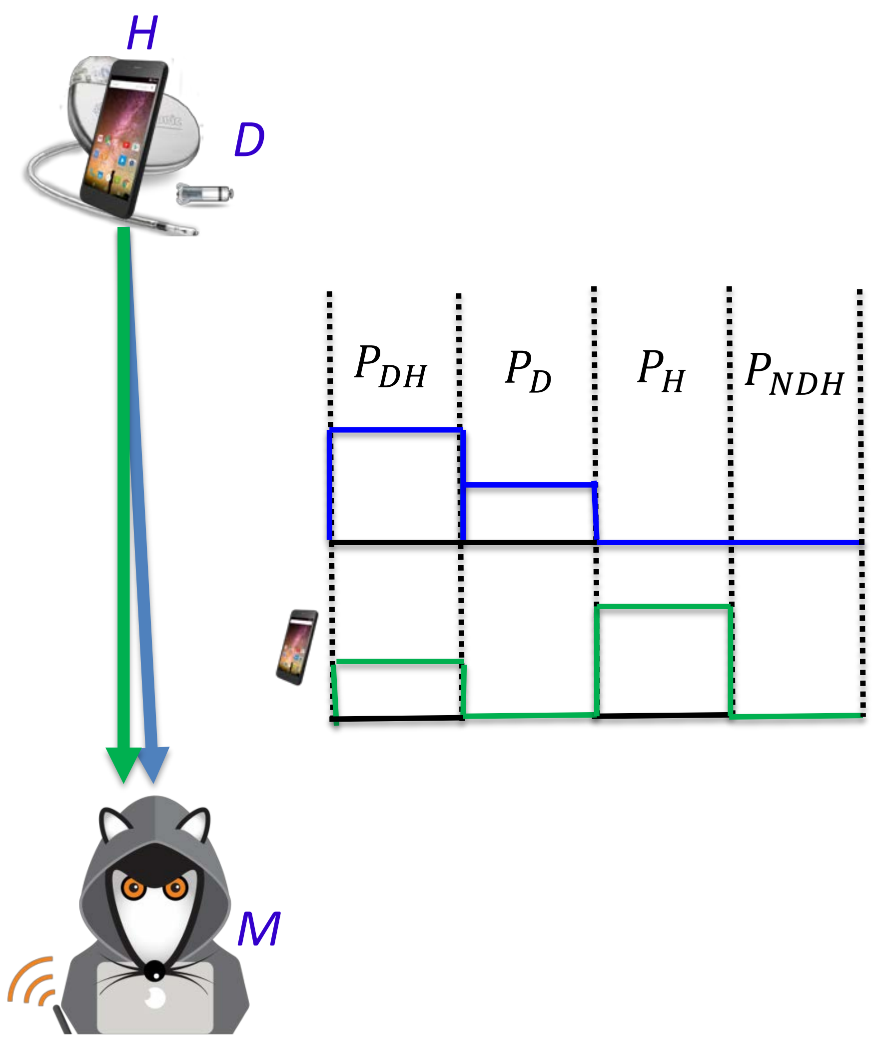


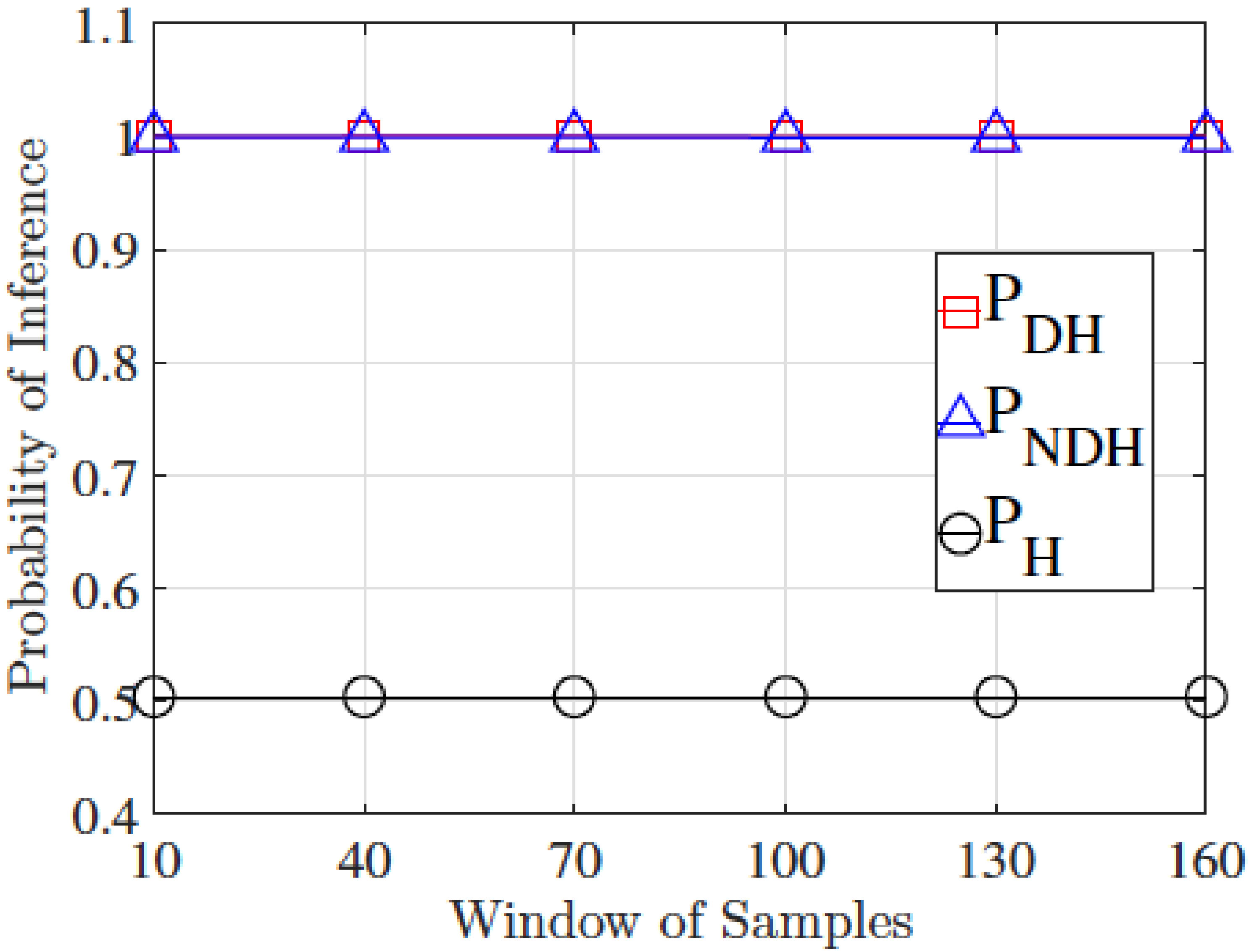
Probability of Inference with *H* and *D* transmit at Fixed Power



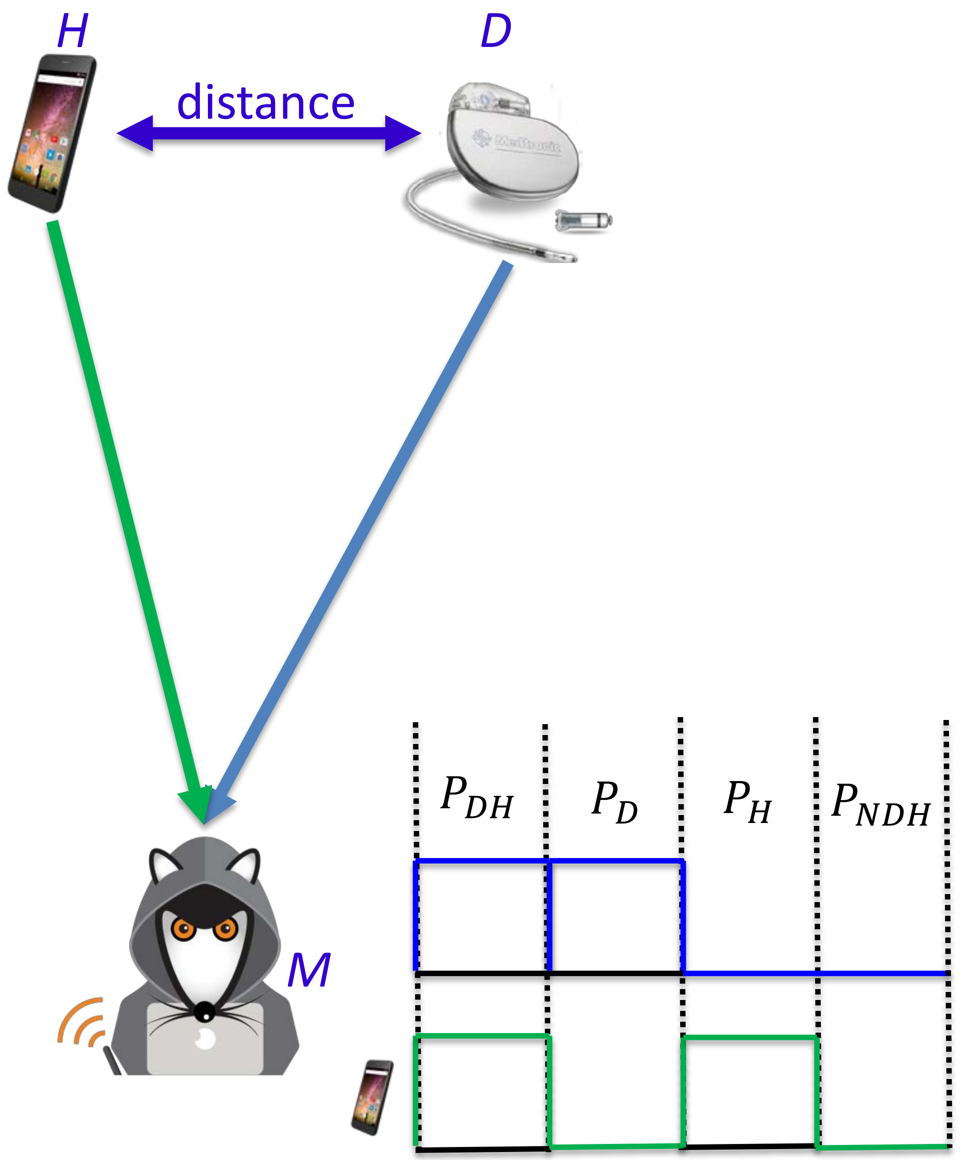


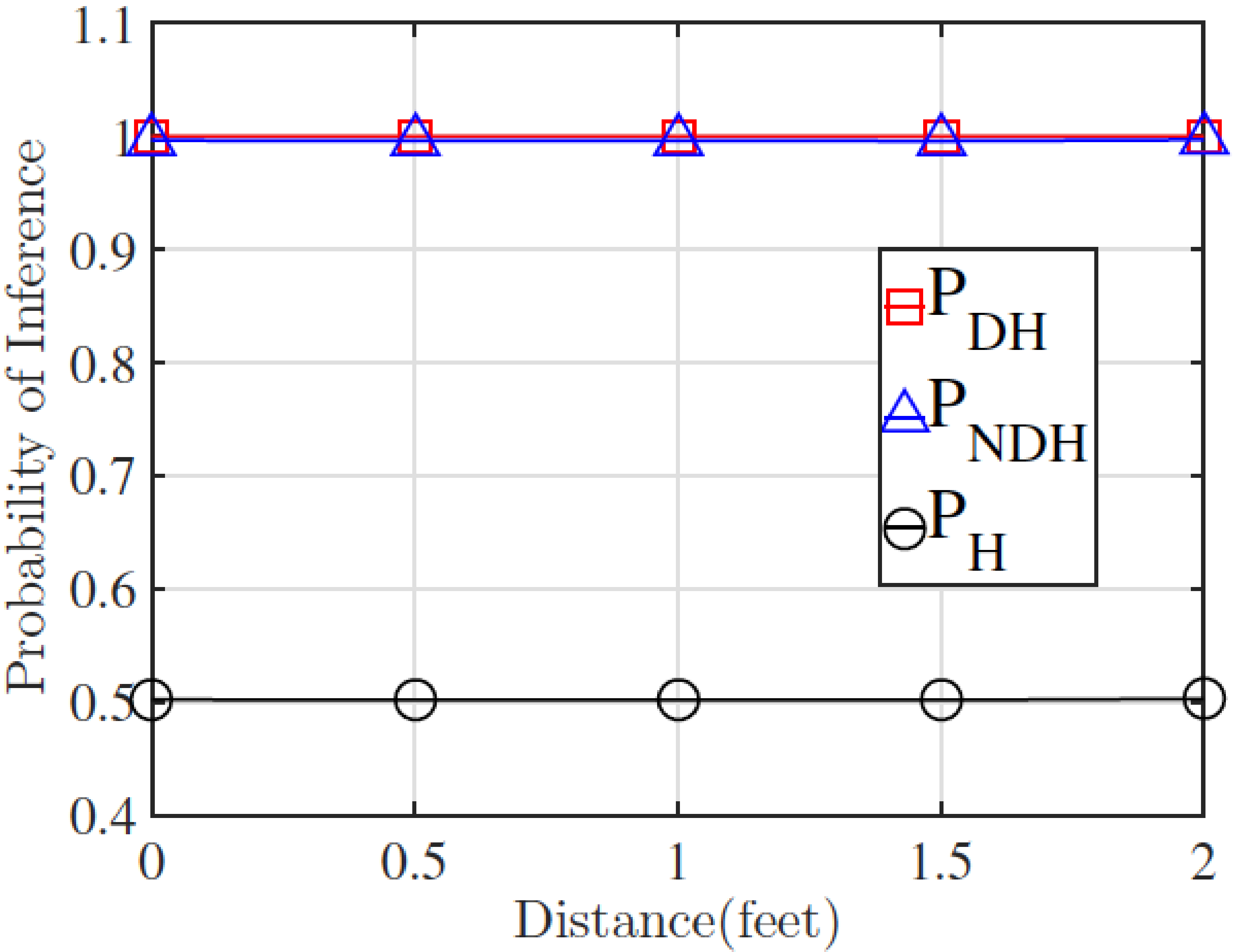
Probability of Inference with *H* and *D* transmit at Varying Power



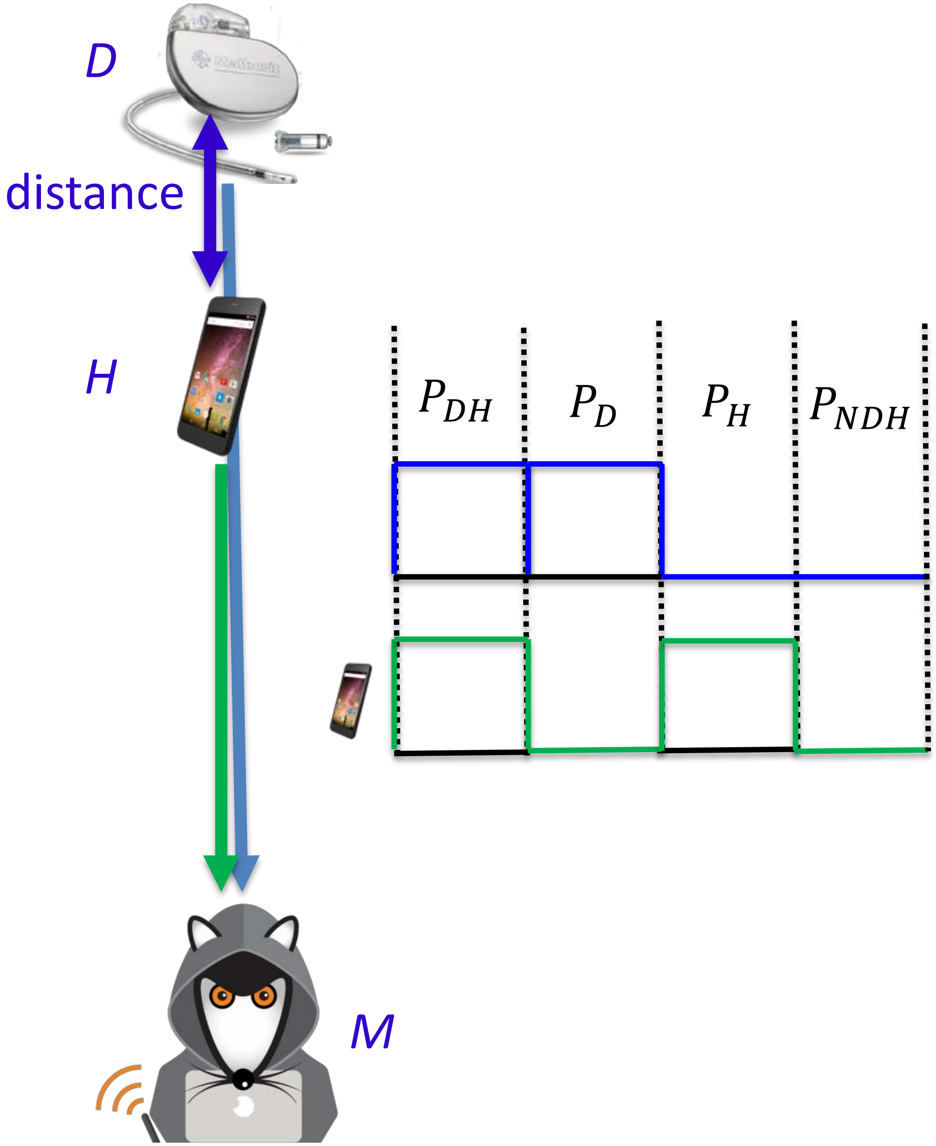


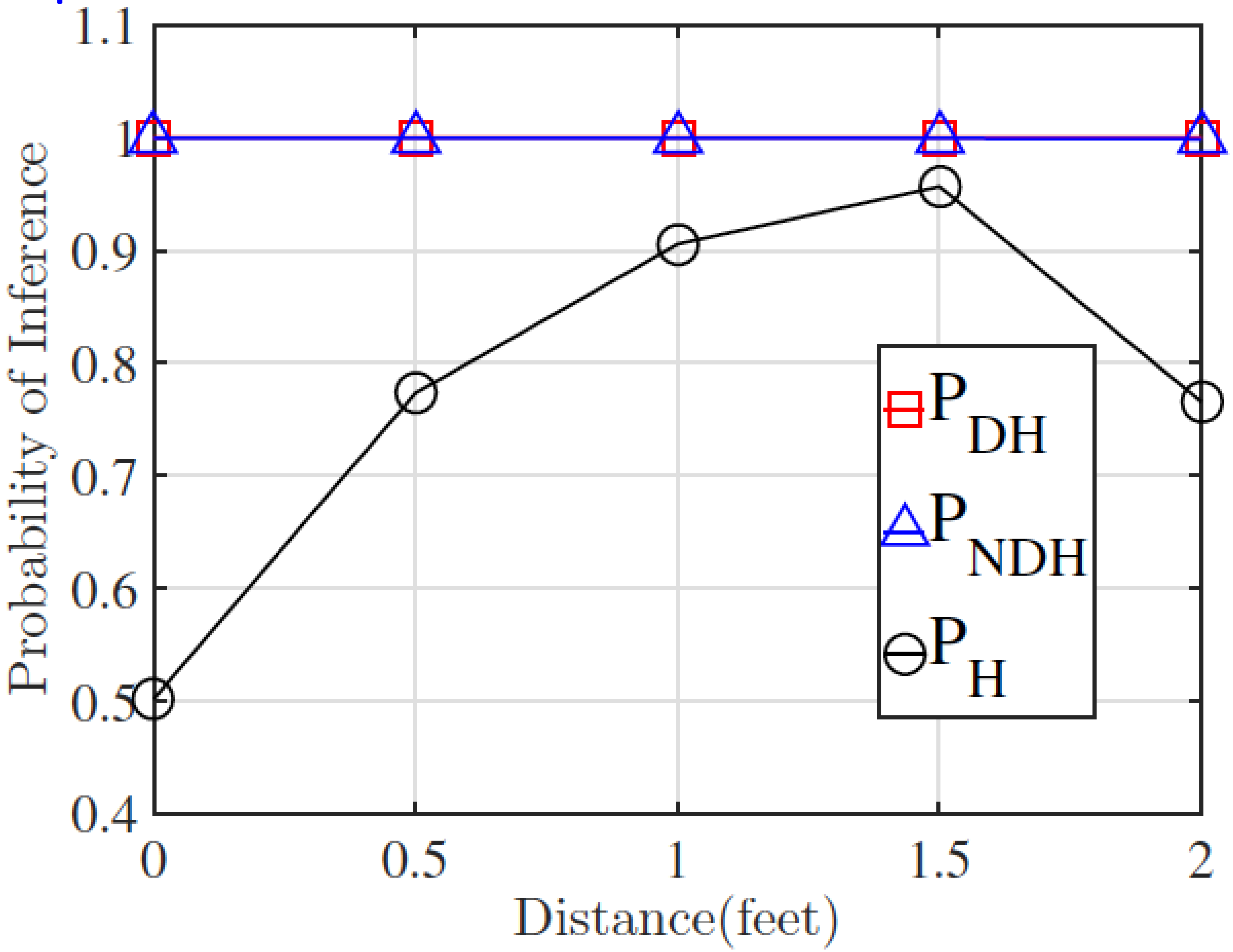
Probability of Inference when *H* and *D* remain Equidistant



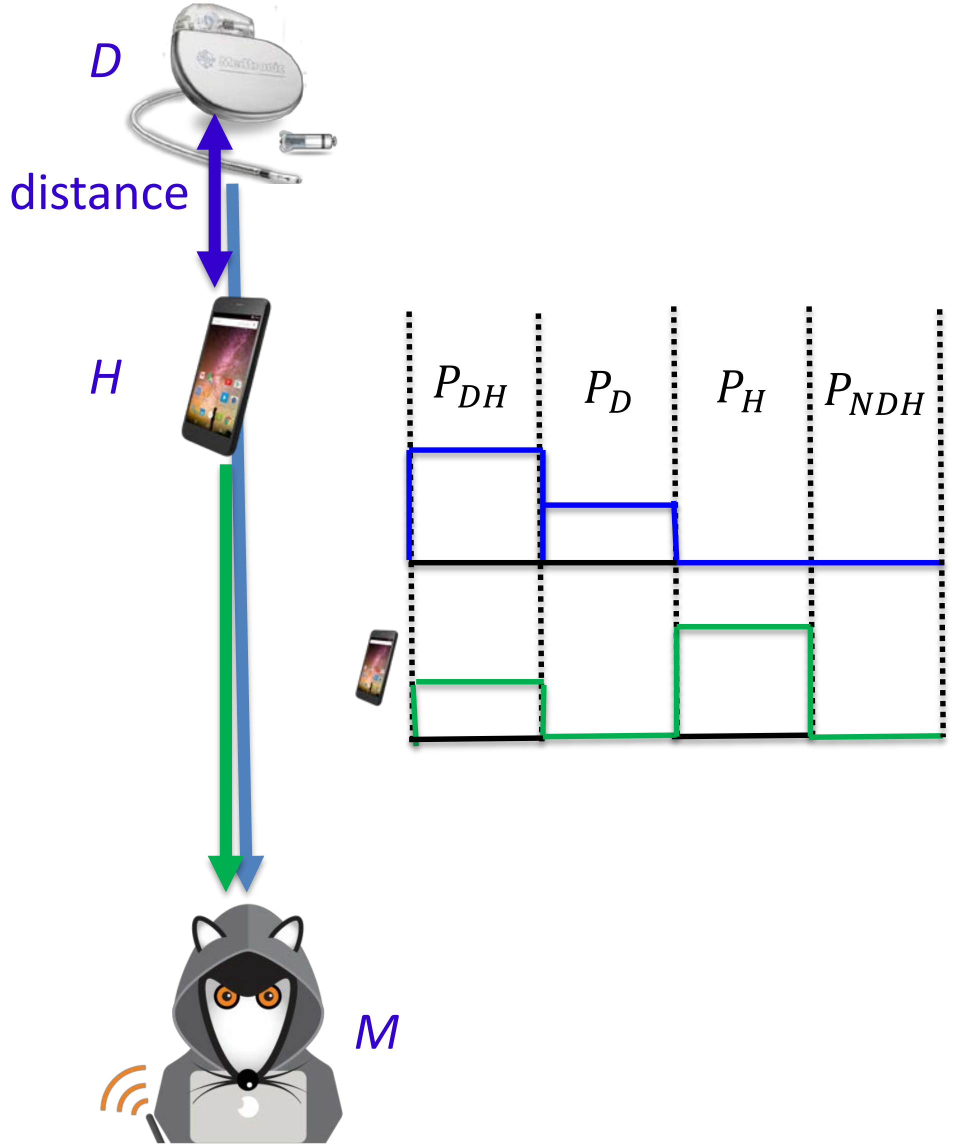


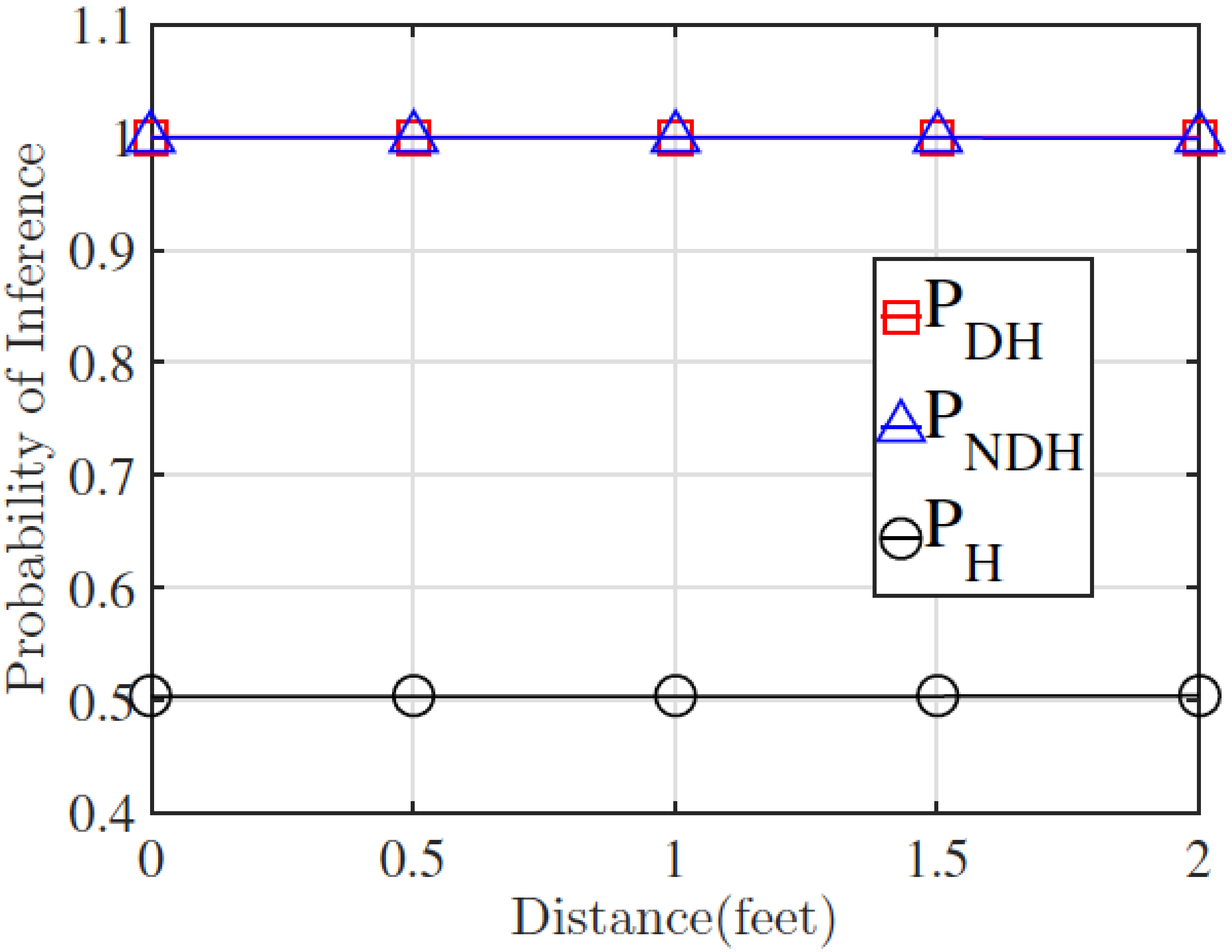
Probability of Inference when *H* is Moved Towards *M*
H,*D* powers are fixed



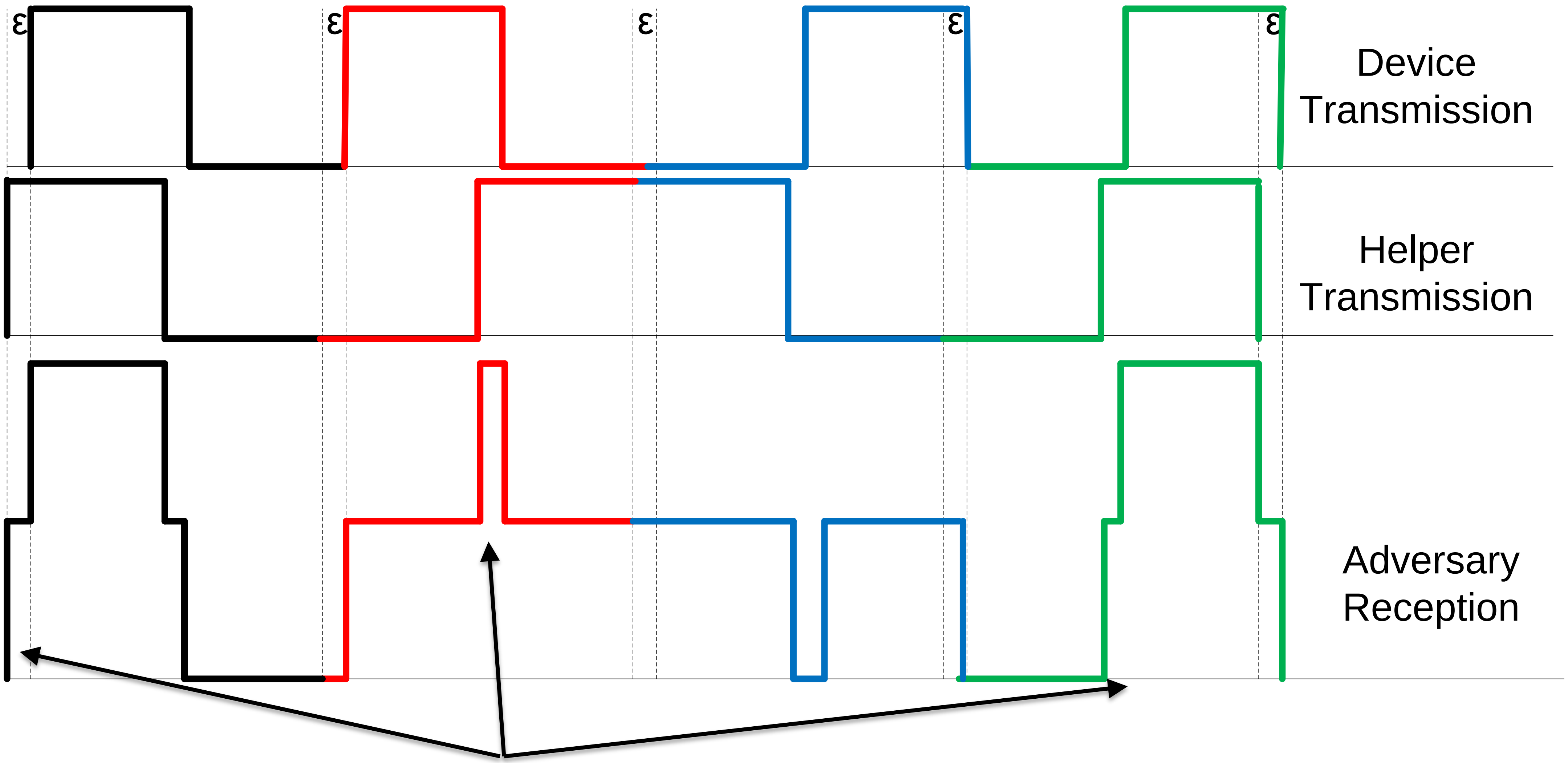


Probability of Inference when *H* is Moved Towards *M*
H,*D* powers are Randomized



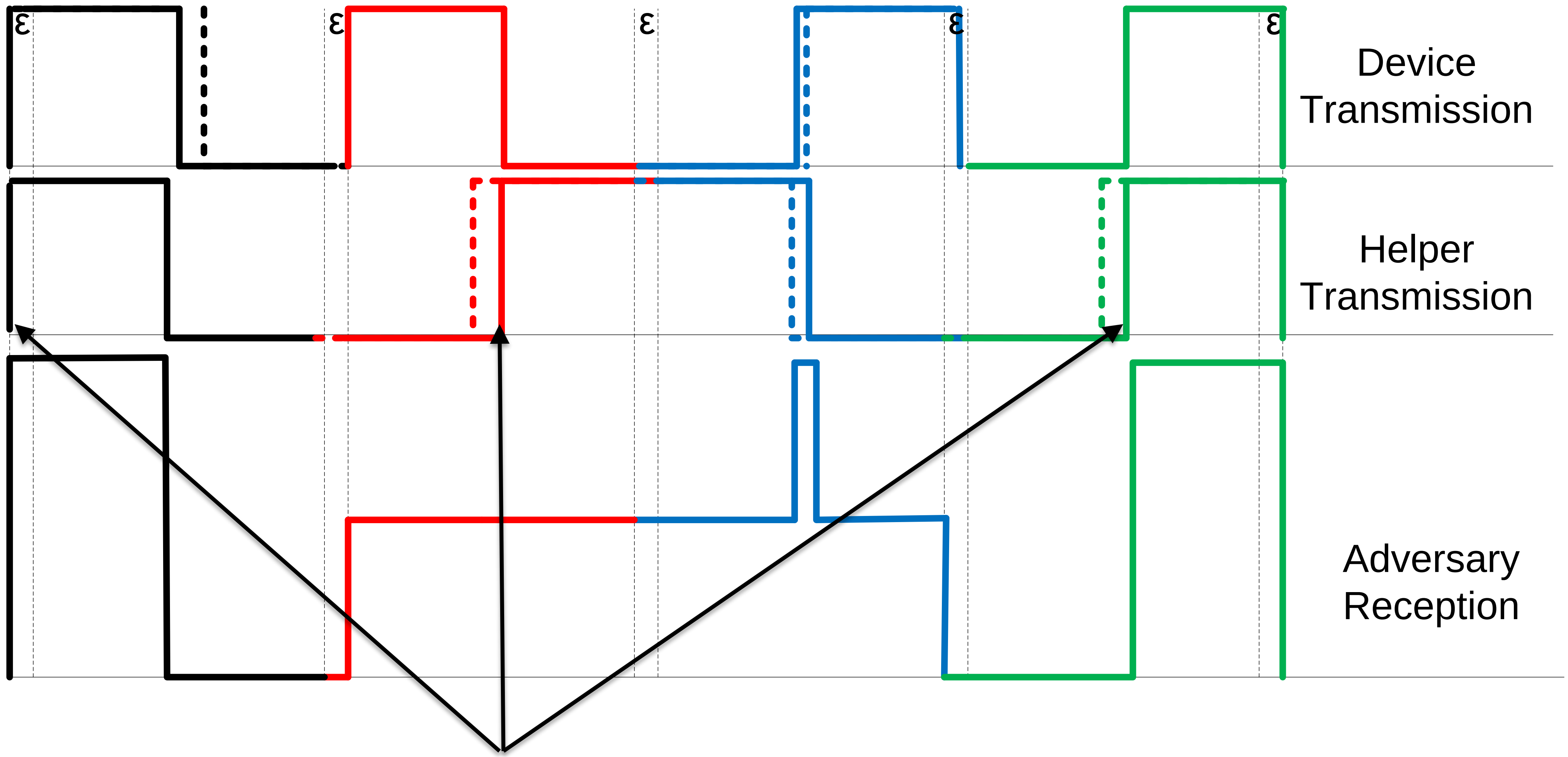


Fast Helper Detection Based on Time



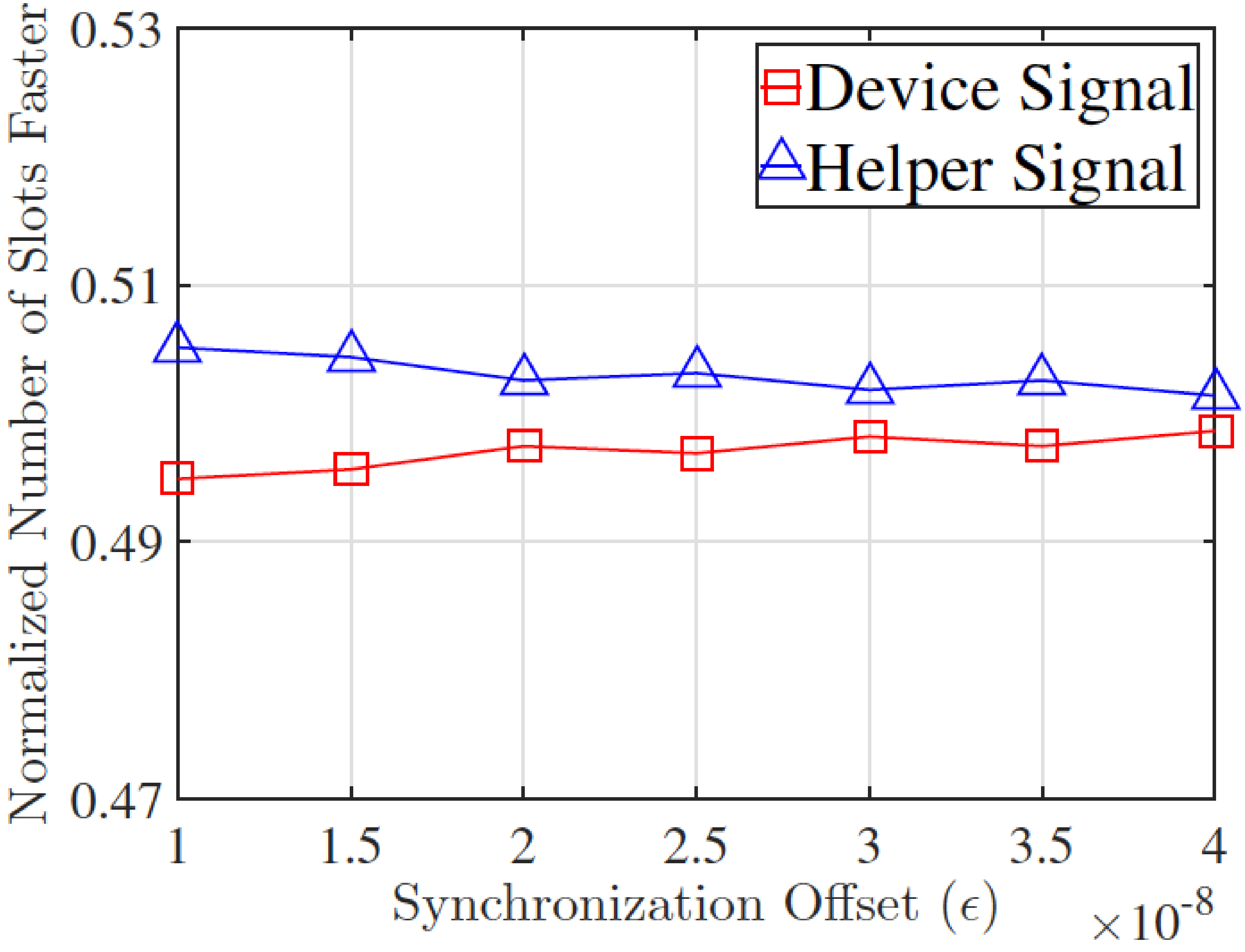
helper is always faster (or slower)

Randomize Slot Starting Times

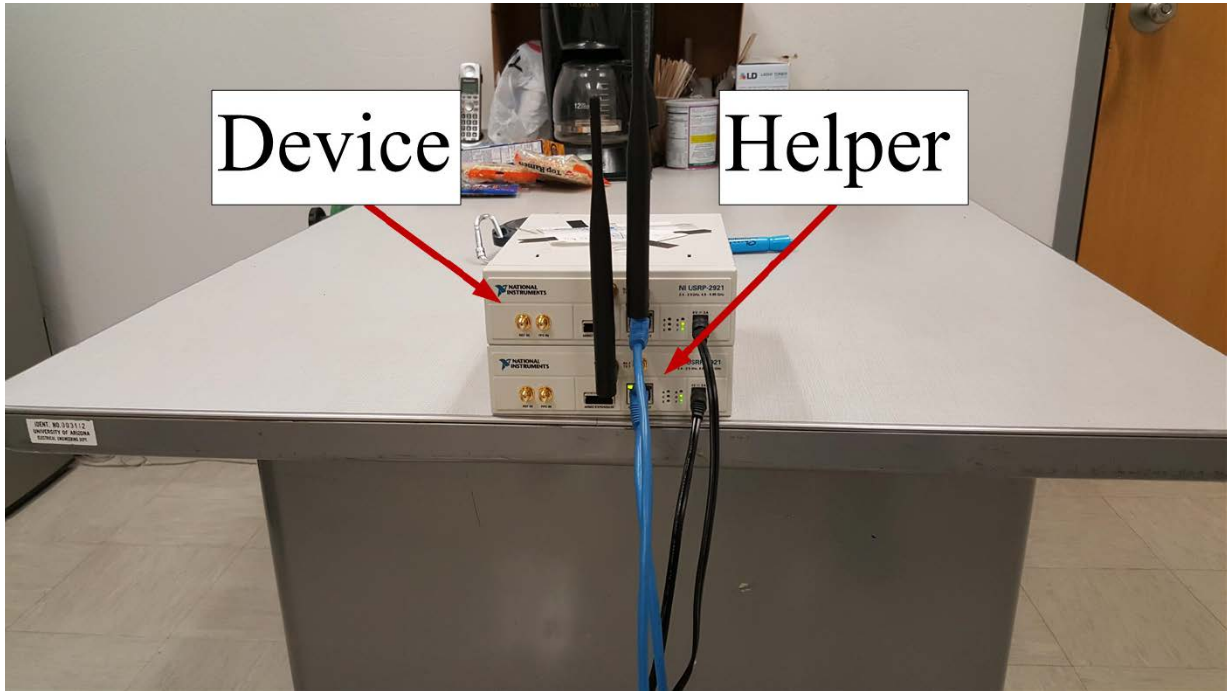


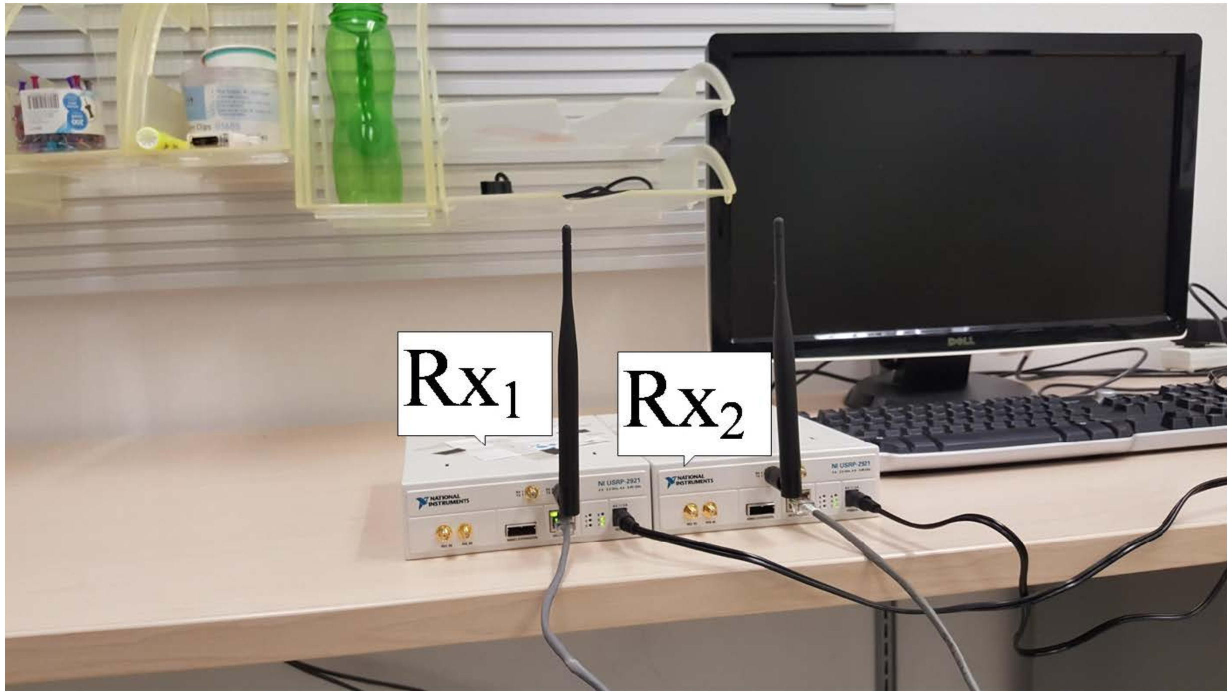
helper is sometimes faster, sometimes slower

Normalized Number of Slots that Each Device is Faster

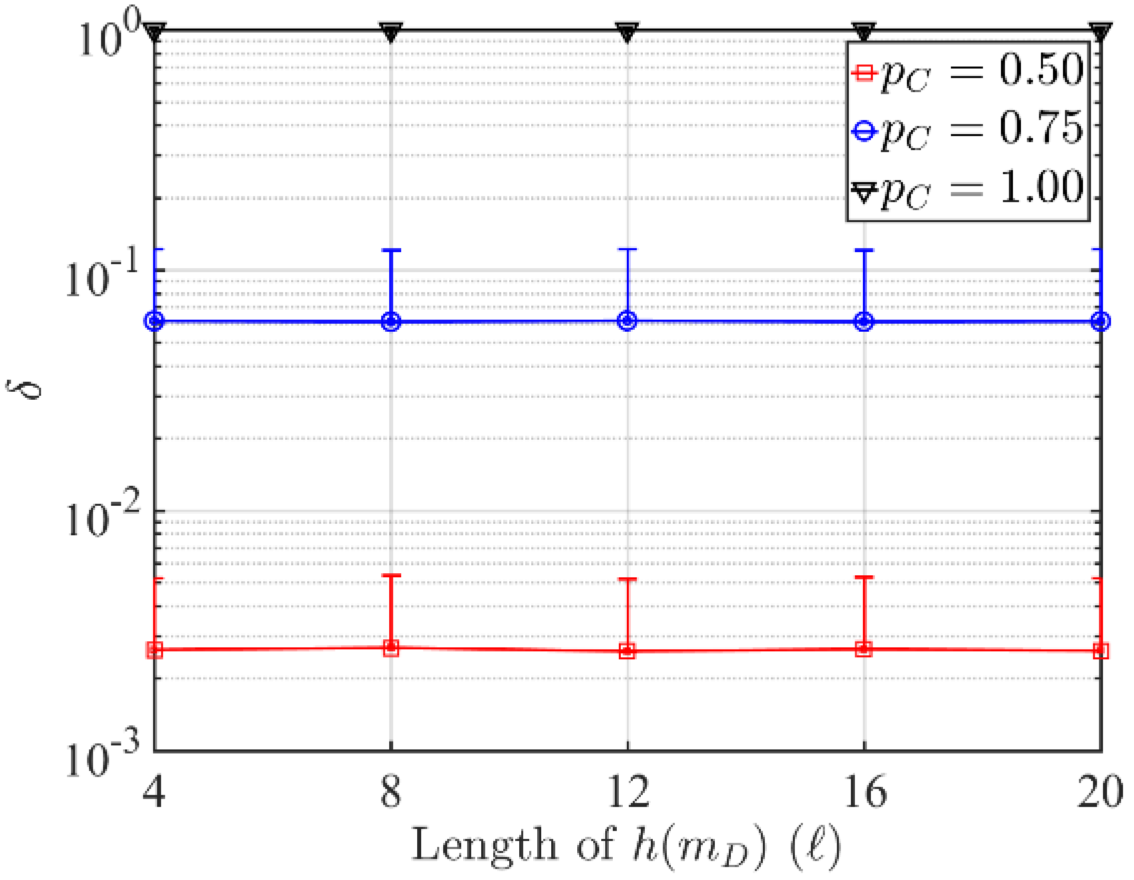


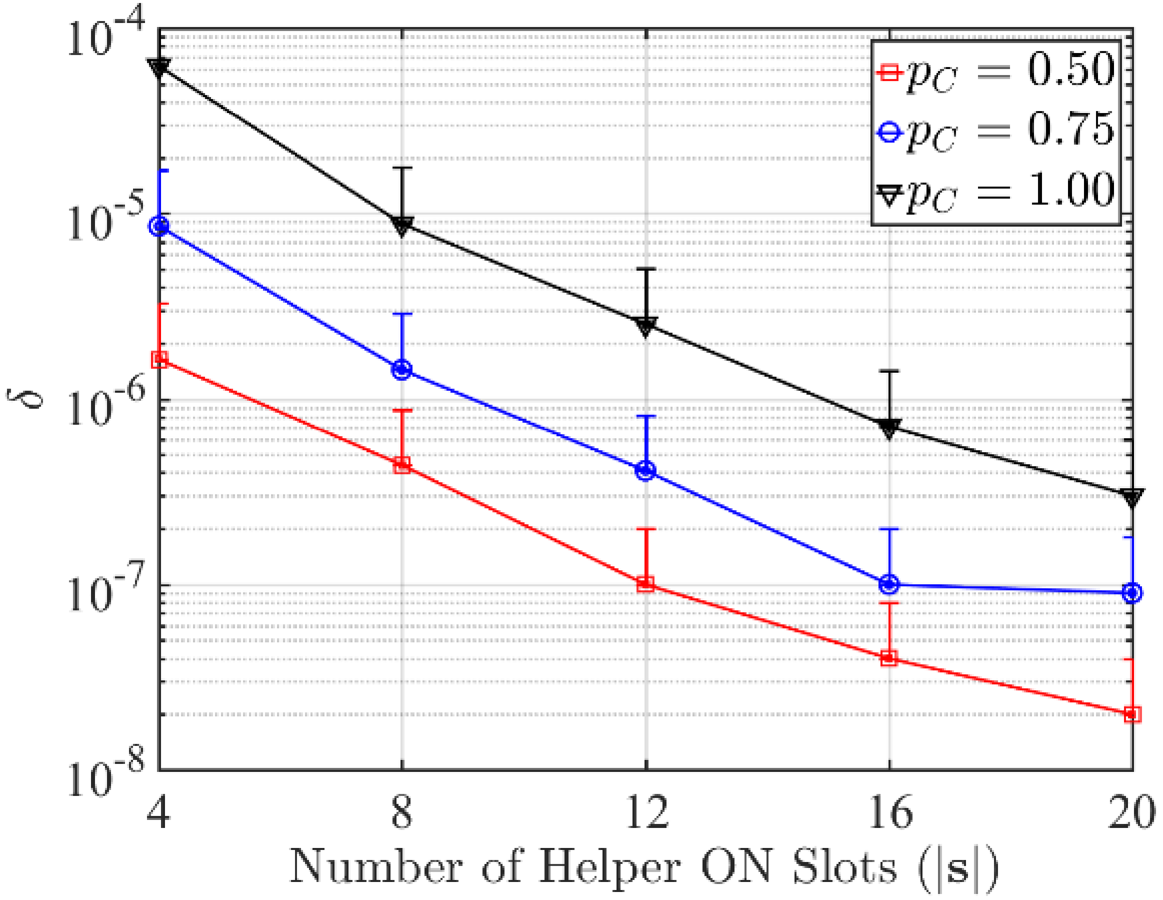
Protocol Evaluation Setup





Protocol Evaluation Results





Conclusions and Future Work

We proposed a new PHY-layer integrity protection scheme called HELP that is resistant to signal cancellation attacks

Our protocol is aimed at alleviating the device pairing problem for IoT devices that may not have the appropriate interfaces for entering or pre-loading cryptographic primitives.

We showed that the DH key agreement protocol using HELP can resist MitM attacks without requiring an authenticated channel between device and the hub.

Future Work: Investigate a MitM-resistant in-band pairing technique that does not rely on ON-OFF keying so that it is compatible with COTS devices