IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 10, 2017, accepted April 27, 2017, date of publication May 2, 2017, date of current version June 7, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2700330

Physical Layer Authentication in Nano Networks at Terahertz Frequencies for Biomedical Applications

MUHAMMAD MAHBOOB UR RAHMAN[1], (Member, IEEE), QAMMER H. ABBASI[1,2,3,4], (Senior Member, IEEE), NISHTHA CHOPRA[4], (Student Member, IEEE), KHALID QARAQE[3], (Senior Member, IEEE), AND AKRAM ALOMAINY[4], (Senior Member, IEEE)

[1]Electrical Engineering Department, Information Technology University, Lahore 54000, Pakistan
[2]School of Engineering, University of Glasgow, G128qq Glasgow, U.K.
[3]Department of Electrical and Computer Engineering, Texas A&M University at Qatar, Doha 23784, Qatar
[4]School of Electronic Engineering and Computer Science, Queen Mary University of London, E14ns London, U.K.

Corresponding author: Muhammad Mahboob Ur Rahman (mahboob.rahman@itu.edu.pk)

This work was supported by NPRP under Grant 7-125-2-061 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

ABSTRACT This paper presents a study on physical layer authentication problem for *in vivo* nano networks at terahertz (THz) frequencies. A system model based on envisioned nano network for *in vivo* body-centric nano communication is considered and *distance-dependent pathloss* based authentication is performed. Experimental data collected from THz time-domain spectroscopy setup shows that pathloss can indeed be used as a device fingerprint. Furthermore, simulation results clearly show that given a maximum tolerable false alarm rate, detection rate up to any desired level can be achieved within the feasible region of the proposed method. It is anticipated that this paper will pave a new paradigm for secured, authenticated nano network for future applications, e.g., drug delivery and Internet of nano-things-based intelligent office.

INDEX TERMS Physical layer security, authentication, terahertz band, intrusion detection, body sensor networks.

I. INTRODUCTION

With the advent of novel nano-materials (e.g., graphene-based carbon nano tubes etc.) with remarkable properties, interest in development of nano devices, their inter-connectivity to realize the internet of nano things [1]–[4], and its applicability in biomedical applications [5] is increasing rapidly. When compared with the traditional methods, e.g., endoscopy [6], the wireless-capable nano-scale devices are less obtrusive and non-invasive in nature which makes them an ideal candidate for the in-vivo biomedical applications [5], [7]. Terahertz (THz) band (0.1–10 THz) is considered as the most promising band for operation of nano devices [5], because of its non-ionization and robustness to the fading characteristics.

As of today, there are very limited studies in open literature which discuss nano-scale communication in THz band and its applicability in the biomedical domain [1], [5], [8]–[15]. Specifically, the literature so far comprises of the studies which investigate the antenna design [9], propagation models [10], transceiver design [11], [16], networking issues [12], [17], and data rates [18]. Though there have been studies which discuss physical layer authentication in macro-macro interface (see, e.g., [19] and references therein) and micro-micro interface (see, e.g., [20] and references therein); to the best of authors' knowledge, no studies have been performed so far to discuss the security and authentication issues related to nano-scale communication at THz frequencies. In this paper, an initial study has been performed where authentication is done based upon a pathloss model (empirically deduced by co-authors of this paper in their previous work [10]).

The main contributions of this work are the following: i) the proposal of exploiting *distance-dependent pathloss* as transmitter fingerprint for physical layer authentication at a nano receiver node, ii) experimental verification of i) via THz time-domain spectroscopy setup at QMUL, UK, iii) the algorithmic solution for the proposed authentication method, iv) investigation of performance of proposed method

(i.e., detection performance, feasible and non-feasible regions).

The rest of this paper is organized as follows. Section-II introduces the system model. Section-III outlines the details of the proposed authentication method, while Section-IV investigates its performance via two different performance metrics. Numerical results are presented in Section-V. Finally, concluding remarks are drawn in Section VI.

II. SYSTEM MODEL

The envisioned architecture for nano-network based in-vivo healthcare is given in [5], and is shown in Fig. 1.

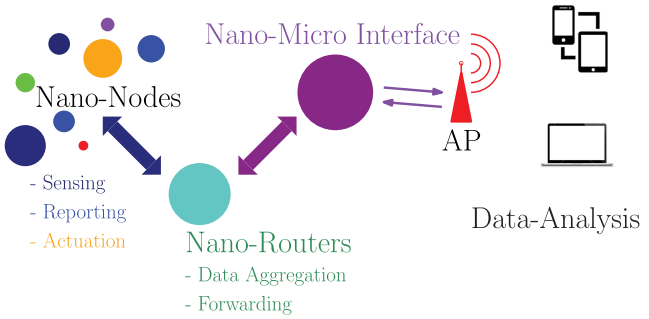

FIGURE 1. Envisioned architecture for nano-healthcare [5].

The main components of the envisioned architecture include:

- Nano-nodes: simplest devices composed of sensor and communication units, which can transmit to short distance the output of a simple computation.
- Nano-routers: can collect data from a multitude of nano nodes and are capable to send a limited number of commands.
- Nano-micro interface: are hybrid devices able to communicate at both nano and micro/macro paradigm.
- Gateway: or Access point (AP) makes system to work remotely over the Internet.

Based on the architecture given in Fig. 1, a system model is established to study the authentication problem in nano-networks. Fig. 2 shows the system model used in this study. The model consists of three nano nodes: Alice, Bob and Eve. *Alice* is the legitimate transmit node, envisioned as an on-body nano-node which sends some control command every once in a while to a legitimate receive node *Bob*, envisioned as a nano-node present inside the human body. Under the envisioned nano-healthcare scenario, one potential task of the Bob node could be *targeted drug delivery*. To this end, Bob will perform certain sensing (e.g., measuring cell temperature, blood suger level etc.) periodically, and report it to the on-body nano-node Alice. Then, whenever Bob receives a control command from Alice, it performs targeted drug delivery (by injecting prescribed amount of drug into the target cells).

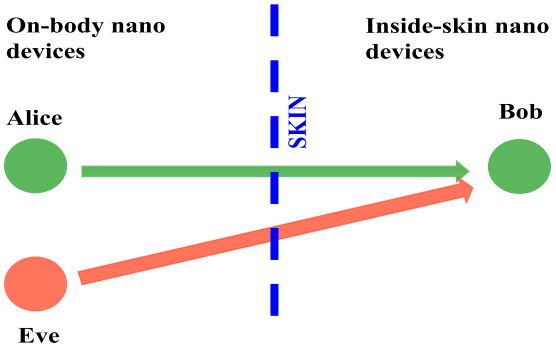

FIGURE 2. Authentication in a nano-scale body-centric communication network.

Having motivated a potential nano-healthcare scenario, imagine now a situation, where an intruder node *Eve* attempts to break into the system by pretending to be Alice and sending a malicious control command to Bob. Such intrusion/impersonation attack, if not thwarted properly, could lead to severe (life threatening) consequences. Therefore, the Bob node must authenticate each and every data packet/control command it receives, in a systematic manner.

III. THE PROPOSED AUTHENTICATION METHOD

This work studies the *feature-based* authentication problem in nano healthcare networks. Specifically, this work proposes to exploit *distance-dependent pathloss* as device fingerprint to discriminate the data sent by Alice from that of intruder Eve. At this point, it is worth mentioning that the authentication problem at hand is in principle very similar to the classical problems of detection and classification. Nevertheless, the only important distinction is that in case of authentication problem, the device fingerprint of Eve is unknown. This limitation renders the classical methods (e.g., likelihood ratio test etc.) not applicable to authentication problem. Bayesian methods are also not applicable for the exact same reason. Therefore, Neyman-Pearson based binary hypothesis testing is typically implemented to carry out the authentication task at Bob.

In operational terms, the proposed authentication method consists of two distinct phases, training phase and authentication phase. During the training phase, Bob learns the pathloss of Alice's transmission PL_{AB} (a.k.a the ground truth) via training with Alice on a secure channel.[1] Then later, during the authentication phase, Eve could transmit as well. Therefore, Bob's task is then to authenticate each and every packet it receives on the shared channel. Bob does the authentication by performing binary hypothesis testing on the pathloss measurement extracted from currently received packet. This way, Bob systematically accepts (rejects) the data from Alice (Eve).

[1]This assumption is inline with the previous literature (see, e.g., [19], [20]).

This work assumes that all the three nodes (Alice, Bob and Eve) of the considered system model as well as the composition of the fluid medium in between remain stationary. A consequence of this assumption is that the ground truth (PL_{AB}) becomes a relatively static quantity. This in turn implies that, for the proposed method, the ratio of training phase duration to authentication phase duration (i.e., the training overhead) is very small. However, when either Alice or Bob is mobile (e.g., floating inside blood), or, the composition of the fluid channel between Alice and Bob is dynamic, the ground truth becomes time-varying. In this case, one simple yet elegant approach is that Bob should acquire the ground truth more often. This in turn signifies that the training overhead becomes proportional to the mobility rate of the legitimate nano nodes (Alice and/or Bob). A more sophisticated approach will be to model the mobility of each of the three nano nodes via some appropriate dynamical model (e.g., Brownian motion/Random walk is a well-known and well-acclaimed model to emulate the movement of gas molecules trapped in a box etc.). Nevertheless, we note that the mobility of nano-nodes (and/or the case of dynamic fluid environment) is out of scope of this work.

Before we outline the more fine-grained details of the proposed method, in the next subsection, we first present the rationale behind using pathloss as device fingerprint for discrimination between the transmit nodes (Alice and Eve) as well as the experimental validation of the rationale.

A. PATHLOSS AS DEVICE FINGERPRINT: RATIONALE & EXPERIMENTAL VALIDATION

For a point-to-point, on-body/inside-skin, THz Communication system, an (experimentally deduced and thus) accurate pathloss model was recently presented (by the co-authors of this paper) in [10]:

$$PL(d,f,N) = -0.2*N+3.98+(0.44*N+98.48)d^{(0.65)} + (0.068*N+2.4)f^{(4.07)} \quad (1)$$

where d is the distance (in mm) between transmit node and receive node, f is the center frequency (in THz), and N is number of sweat ducts. Let's denote by d_{AB} (d_{EB}) the distance between Alice (Eve) and Bob. Eq. (1) then suggests that pathloss, being distance-dependent, can indeed be used as device fingerprint provided that $|d_{AB} - d_{EB}| \geq \eta$ where η is a threshold.

Fig. 3 shows the pathloss measurements as a function of frequency (obtained from the THz-TDS setup at QMUL, UK) for two skin samples with different thickness values. Fig. 3 corroborates the pathloss model of Eq. (1) and attests to the fact that the pathloss is indeed distance (thickness) dependent.

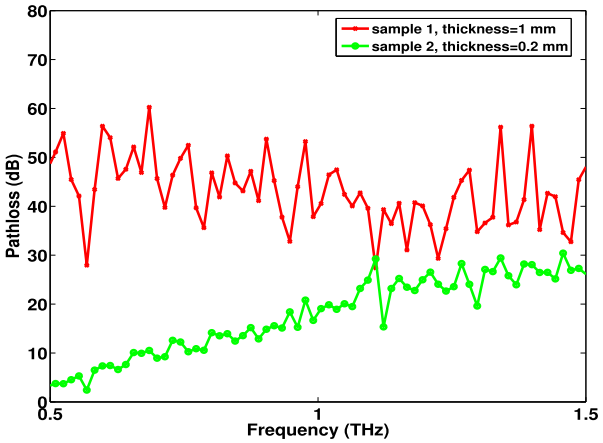

FIGURE 3. Pathloss as Device Fingerprint: Experimental Validation. Pathloss measurements were obtained via THz-TDS setup at QMUL, UK. More details about the THz-TDS setup can be found in [10].

B. BINARY HYPOTHESIS TESTING

At time t_m, when Bob receives a packet from the shared channel, it makes a noisy measurement $z(m)$ of the pathloss (this could be done, e.g., using the pulse-based method discussed in [21]). With $z(m)$ in hand, Bob constructs the following binary hypothesis testing problem:

$$\begin{cases} H_0: & z(m) = PL_{AB}(d_{AB}) + \epsilon(m) \\ H_1: & z(m) = PL_{EB}(d_{EB}) + \epsilon(m) \end{cases} \quad (2)$$

where $PL_{AB}(d_{AB})$ ($PL_{EB}(d_{EB})$) is the distance-dependent pathloss of the channel between Alice (Eve) and Bob, and follows Eq. (1). Moreover, $\epsilon(m)$ is the estimation error assumed to be zero-mean Gaussian with variance $\sigma^2(m)$. Typically, $\sigma^2(m) = \frac{c.\sigma_B^2}{K(m).P_{Tx}(m)}$ where σ_B^2 is the variance of white Gaussian noise at Bob, $K(m)$ is the length of the preamble preceding the data, $P_{Tx}(m)$ is the transmit power of the sender node[2] and c is a constant.

Dropping the time index m for simplicity, it is straightforward to see that $z|H_0 \sim \mathcal{N}(PL_{AB}, \sigma^2)$ while $z|H_1 \sim \mathcal{N}(PL_{EB}, \sigma^2)$. If $H_0 = 1$, received packet is accepted by Bob; if $H_1 = 1$, received packet is rejected by Bob.

Next, since the ground truth PL_{AB} is known with sufficient accuracy (via prior training in the beginning, on a secure channel), Bob applies the following test:

$$T = |z - PL_{AB}| \underset{H_0}{\overset{H_1}{\gtrless}} \delta \quad (3)$$

where δ is the comparison threshold (a design parameter) whose value is to be determined.

C. ALGORITHMIC IMPLEMENTATION

The only thing further required to implement the hypothesis test of Eq. (3) is the value of threshold δ. In this work, we utilized Neyman-Pearson method which systematically computes the value of δ once provided with a maximum tolerable value of the probability of false alarm P_{fa} (i.e., incorrectly identifying Alice's packet as if it is from Eve).

[2] P_{Tx}, K are the system parameters, pre-known to (and fixed for) all the nodes in the network; therefore, they remain the same no matter who among Alice or Eve transmits on the shared channel.

Let $y = z - PL_{AB}$. Then, $y|H_0 \sim \mathcal{N}(0, \sigma^2)$ and $y|H_1 \sim \mathcal{N}(PL_{EB} - PL_{AB}, \sigma^2)$. Then, P_{fa} is given as:

$$P_{fa} = Pr(|y| > \delta|H_0) = 2Q\left(\frac{\delta}{\sigma}\right) \quad (4)$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$ is the complementary cumulative distribution function (CCDF) of standard normal distribution.

By setting P_{fa} to the pre-specified value, δ can be calculated using Eq. (4) as:

$$\delta = \sigma Q^{-1}\left(\frac{P_{fa}}{2}\right) \quad (5)$$

At this point, it is worth mentioning that the computation of δ in Eq. (5) requires only the knowledge of variance σ^2 (of the pathloss measurement error ϵ) which could be easily computed offline (i.e., before the authentication phase commences). Moreover, one can infer from Eq. (5) that the hypothesis of Eq. (3) remains effective as long as Eve doesn't adapt its transmit power which is indeed assumed in this work.

The proposed authentication method is summarized in Algorithm 1.

Algorithm 1 The Proposed Authentication Method

Phase-I: Training ($H_0 = 1$)
Bob learns the ground truth (i.e., PL_{AB}) on a secure channel
Phase-II: Authentication
while (1) **do**
  Bob computes the threshold δ from Eq. (5)
  Bob implements the binary hypothesis test in Eq. (3) to systematically accept/reject data packets
end while

IV. PERFORMANCE OF THE PROPOSED METHOD

A. DETECTION RATE

While carrying out hypothesis testing, Bob could make two kind of errors: i) Bob discards the data of Alice thinking that it came from Eve, the so-called probability of false alarm P_{fa}, ii) Bob accepts the data coming from Eve thinking that it came from Alice, the so-called probability of missed detection P_{md}.

In this work, we have employed Neyman-Pearson method which guarantees to minimize (maximize) P_{md} ($P_d = 1 - P_{md}$), for a fixed/given value of P_{fa}. Therefore, we proceed to compute the probability of missed detection P_{md} (success probability of Eve) which is as follows:

$$P_{md} = Pr(|y| < \delta|H_1) \quad (6)$$

Assuming that unknown pathloss PL_{EB} is uniformly distributed within a reasonable range $PL_{EB} \sim \mathcal{U}(\Delta_{min}, \Delta_{max})$, we have the following expression:

$$P_{md} = \frac{1}{\Delta_{max} - \Delta_{min}} \int_{\Delta_{min}}^{\Delta_{max}} \left[Q\left(\frac{-\delta - PL_{EB} + PL_{AB}}{\sigma}\right) - Q\left(\frac{\delta - PL_{EB} + PL_{AB}}{\sigma}\right)\right] dPL_{EB} \quad (7)$$

A closed-form solution of Eq. (7) cannot be obtained because it involves the integration of the Q-function.

It is worth mentioning that Eq. (7) is typically solved offline (before the authentication phase commences) to obtain receiver operating characteristic (ROC) curves. The only information missing to solve Eq. (7) are the limits of integration, i.e., Δ_{min} and Δ_{max}, which one can compute in a relatively straightforward manner provided that Bob knows the fixed transmit power P_{Tx} used by the transmit nodes (Alice and Eve) which is indeed assumed in this work.

B. DEFLECTION COEFFICIENT

Another important performance metric of interest in Detection theory is Deflection coefficient, which quantifies the separation between two conditional probability densities of the test statistic under consideration. Larger the value of the deflection coefficient, better is the detection performance and vice versa. Specifically, the deflection coefficient for any binary hypothesis testing scheme is defined as:

$$\xi = \frac{(\mathbb{E}[T|H_1] - \mathbb{E}[T|H_0])^2}{Var(T|H_0)} \quad (8)$$

where T is the test statistic of interest (defined in Eq. (3) for our proposed method). Then, one can verify that T in Eq. (3) has a *folded* normal distribution; therefore, $\mathbb{E}[T|H_0] = \sigma.\sqrt{2/\pi}$ and:

$$\mathbb{E}[T|H_1] = \sigma.\sqrt{2/\pi}.\exp\left(\frac{-(PL_{EB} - PL_{AB})^2}{2\sigma^2}\right) - (PL_{EB} - PL_{AB}).(1 - 2\Phi(-(PL_{EB} - PL_{AB})/\sigma)) \quad (9)$$

where $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt$ is the cumulative distribution function (CDF) of standard normal distribution. Finally, $Var(T|H_0) = \sigma^2(1 - 2/\pi)$.

C. FEASIBLE AND NON-FEASIBLE REGIONS

As is suggested by Fig. 3, pathloss, being distance-dependent, can indeed be used as device fingerprint provided that $|d_{AB} - d_{EB}| \geq \eta$ where η is a threshold. This in turn implies that $|d_{AB} - d_{EB}| \geq \eta$ corresponds to the feasible region (where the proposed authentication method meets the pre-specified performance requirements), while $|d_{AB} - d_{EB}| < \eta$ corresponds to the non-feasible region (where the proposed authentication method breaks down).

Eqs. (8), (9) together reveal that ξ is solely a function of the two fingerprints PL_{AB} and PL_{EB} which in turn means ξ is a function of two distances, i.e., the distance between Alice

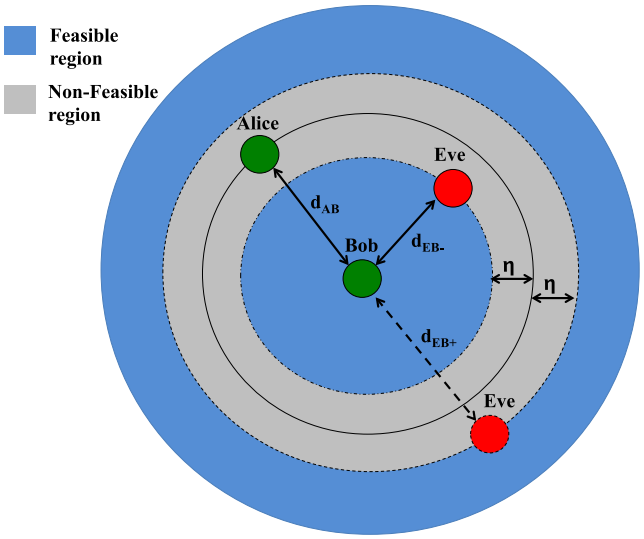

FIGURE 4. *The feasible and non-feasible regions for the proposed method:* **In this 2D map/layout, Bob is placed at origin, while Alice is located at a distance d_{AB} from origin. Then if the Eve lies anywhere within the grey region, i.e., $|d_{AB} - d_{EB}| < \eta$, then $\xi < \beta$, and thus, α-level detection using proposed method is not feasible. However, when Eve is is anywhere in blue region, i.e., $|d_{AB} - d_{EB}| \geq \eta$, then $\xi \geq \beta$, and thus, α-level detection using proposed method is feasible. ($d_{EB-} = d_{AB} - \eta$; $d_{EB+} = d_{AB} + \eta$.)**

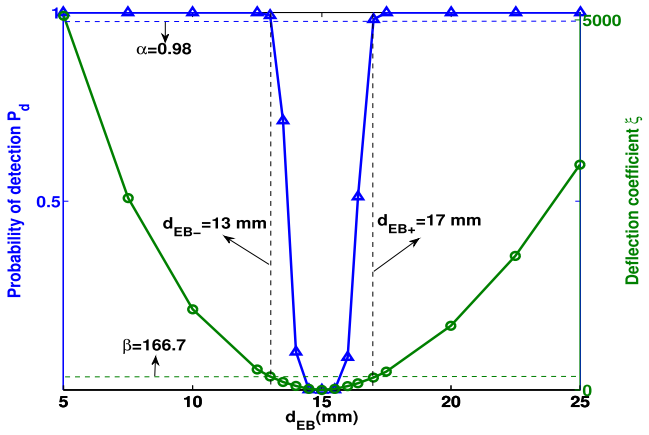

FIGURE 5. *The feasible and non-feasible regions for the proposed method:* **In this simulation, $d_{AB} = 15$ mm, while d_{EB} is varied. It shows that when Eve lies anywhere within the grey region of Fig. 4, i.e., when $|d_{AB} - d_{EB}| < \eta = 2$ mm, then $\xi < \beta = 166.7$, and thus, ($\alpha = 0.98$)-level detection using proposed method is not feasible. However, when Eve lies anywhere in blue region of Fig. 4, i.e., $|d_{AB} - d_{EB}| \geq \eta$, then $\xi \geq \beta$, and thus, α-level detection using proposed method is feasible. (Other system parameters were set to the following values: $N = 4$, $f = 1.2$ THz, $P_{fa} = 10^{-6}$, $\sigma = 7.07$ mm.)**

and Bob d_{AB}, and the distance between Eve and Bob d_{EB} (see Eq. (1)). Similarly, from Eq. (7), one could deduce the same, i.e., P_{md} is solely a function of the two fingerprints PL_{AB} and PL_{EB} (and hence a function of two distances d_{AB} and d_{EB}). Fig. 4 then graphically illustrates that Deflection coefficient ξ and detection rate P_d together could be utilized to identify the feasible and non-feasible regions for our proposed authentication scheme. Specifically, for a desired/pre-specified minimum detection performance α (i.e., $P_d \geq \alpha$), the following relations hold:

$$P_d \geq \alpha \Leftrightarrow \xi \geq \beta \Leftrightarrow |d_{AB} - d_{EB}| \geq \eta \quad \text{(feasible region)} \tag{10}$$

$$|d_{AB} - d_{EB}| < \eta \Leftrightarrow \xi < \beta \Leftrightarrow P_d < \alpha \quad \text{(non-feasible region)} \tag{11}$$

(where β and η are the thresholds).

V. NUMERICAL RESULTS

Owing to the fact that there aren't any nano-devices manufactured to date which could be leveraged to investigate the performance of the proposed authentication method in a real-time setting, this section provides extensive simulation results.

Fig. 5 provides a quantitative example to illustrate that Deflection coefficient ξ and detection rate P_d could indeed help us identify the feasible and non-feasible regions for our proposed authentication scheme (as discussed in Section IV-C earlier). Specifically, Fig. 5 states that the relations (10),(11) indeed hold with $\alpha = 0.98$, $\beta = 166.7$, $\eta = 2$ mm. In other words, Fig. 5 reveals that the proposed authentication algorithm successfully detects the intrusions (i.e., Eve's transmissions) $> 98\%$ of times provided that Eve's distance to Bob d_{EB} is off by at least 2 mm from Alice's distance to Bob d_{AB}.

Fig. 6 plots the receiver operating characteristic (ROC) curves for various values of $|d_{AB} - d_{EB}|$ (or, equivalently Deflection coefficient ξ). Specifically, the locations of Alice and Bob are fixed such that $d_{AB} = 15$ mm, while Eve is placed at five different locations such that $d_{EB} \in [13, 14, 15, 16, 17]$ mm. The black ROC curve representing the case $\xi = 0$ coincides with the 45^0 line which implies that the proposed method ceases to be effective when $d_{AB} = d_{EB}$. In such situation, flipping a coin to observe its output for decision making performs equally well as the proposed scheme. Fig. 6 also confirms the hypothesis that greater the ξ is, so is P_d[3] (for a given P_{fa}). Finally, the zoomed-in plot representing the case $\xi = 166.71$ (within Fig. 6) shows the typical trade-off between P_d and P_{fa}; i.e., it is not possible to increase P_d without sacrificing P_{fa} and vice versa.

Fig. 7 provides the graphical illustration of the working of Hypothesis test of Eq. (3) for 100 uses of the shared channel (we assume $P(H_0) = P(H_1) = 0.5$, i.e., we assume that at any given time-slot, Alice and Eve are equally likely to transmit). Since the hypothesis test of Eq. (3) essentially computes the absolute deviation of each (pathloss) measurement z from the ground truth PL_{AB} and compares it with a pre-set threshold δ to make a decision, Fig. 7 provides us a way to visually spot and segregate the transmissions from the intruder node Eve (the transmissions with large magnitude/value of the test statistic T), and the transmissions from

[3] In other words, greater disparity between d_{AB} and d_{EB} helps authentication cause, as explained in Fig. 4.

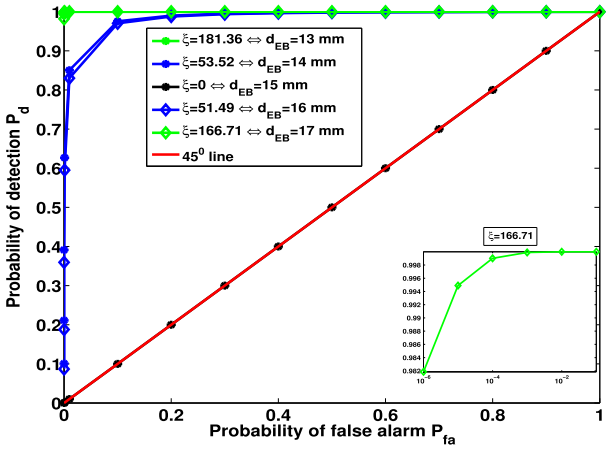

FIGURE 6. ROC curves for the proposed scheme: $d_{AB} = 15$ mm, $d_{EB} \in [13, 17]$ mm, $\sigma = 7.07$ mm, $N = 4$, $f = 1.2$ THz.

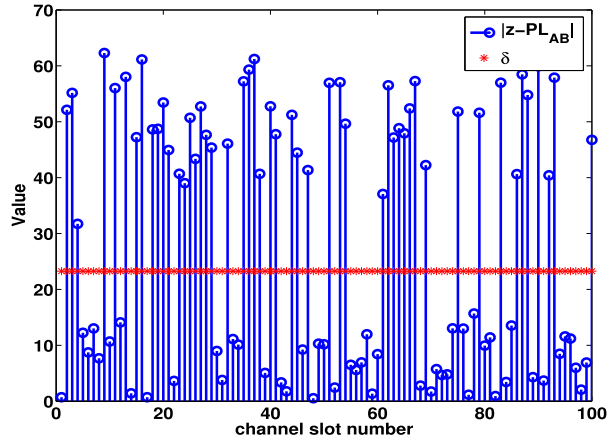

FIGURE 7. Hypothesis test of Eq. (3) in action ($P_{fa} = 10^{-3}$, $N = 4$, $f = 1.2$ THz, $\sigma = 7.07$ mm, $d_{AB} = 15$ mm, $d_{EB} = 13$ mm).

the legitimate sender Alice (the transmissions with smaller magnitude/value of the test statistic T).

VI. CONCLUSION

In this paper, a physical layer authentication scheme based on distance-dependent pathloss is studied for in-vivo nano networks at terahertz frequencies. For the proposed authentication scheme, detection performance has been investigated, and feasible and non-feasible regions are identified.

It is anticipated that this work will pave a way for designing secured, authenticated links for the future nano-networks. For example, this study has already pointed towards several directions for future research, e.g., incorporating the mobility of the nano nodes into the proposed authentication framework, design of cross-layer authentication schemes, combining multiple features for improved authentication performance etc.

ACKNOWLEDGMENT

The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] I. F. Akyildiz and J. M. Jornet, "Electromagnetic wireless nanosensor networks," *Nano Commun. Netw.*, vol. 1, no. 1, pp. 3–19, Mar. 2010.
[2] I. F. Akyildiz, F. Brunetti, and C. Blázquez, "Nanonetworks: A new communication paradigm," *Comput. Netw.*, vol. 52, no. 12, pp. 2260–2279, 2008.
[3] S. Balasubramaniam and J. Kangasharju, "Realizing the Internet of nano things: Challenges, solutions, and applications," *Computer*, vol. 46, no. 2, pp. 62–68, Feb. 2013.
[4] I. F. Akyildiz and J. M. Jornet, "The Internet of nano-things," *IEEE Wireless Commun.*, vol. 17, no. 6, pp. 58–63, Dec. 2010.
[5] Q. H. Abbasi *et al.*, "Nano-communication for biomedical applications: A review on the state-of-the-art from physical layers to novel networking concepts," *IEEE Access*, vol. 4, pp. 3920–3935, Aug. 2016.
[6] T. Nakamura and A. Terano, "Capsule endoscopy: Past, present, and future," *J. Gastroenterol.*, vol. 43, no. 2, pp. 93–99, 2008.
[7] M. Sitti *et al.*, "Biomedical applications of untethered mobile milli/microrobots," *Proc. IEEE*, vol. 103, no. 2, pp. 205–224, Feb. 2015.
[8] Q. H. Abbasi, K. Qaraqe, A. Alomainy, and M. U. Rehman, *Advances in Body-Centric Wireless Communication: Applications and State-of-the-Art*. London, U.K.: IET, Jul. 2016.
[9] M. Nafari and J. M. Jornet, "Metallic plasmonic nano-antenna for wireless optical communication in intra-body nanonetworks," in *Proc. 10th EAI Int. Conf. Body Area Netw. (ICST)*, Brussels, Belgium, 2015, pp. 287–293. [Online]. Available: http://dx.doi.org/10.4108/eai.28-9-2015.2261410
[10] Q. H. Abbasi, H. E. Sallabi, N. Chopra, K. Yang, K. Qaraqe, and A. Alomainy, "Terahertz channel characterisation inside the human skin at the nano-scale," *IEEE Trans. THz Sci. Technol.*, vol. 6, no. 3, pp. 427–434, May 2016.
[11] C. Cvetkovic *et al.*, "Three-dimensionally printed biological machines powered by skeletal muscle," *Proc. Nat. Acad. Sci. India A, Phys. Sci.*, vol. 111, no. 28, pp. 10125–10130, 2014.
[12] J. M. Jornet, J. Capdevila-Pujol, and J. Sole-Pareta, "PHLAME: A physical layer aware MAC protocol for electromagnetic nanonetworks in the terahertz band," *Nano Commun. Netw. (Elsevier) J.*, vol. 3, no. 1, pp. 74–81, 2012.
[13] G. Piro, K. Yang, G. Boggia, N. Chopra, L. A. Grieco, and A. Alomainy, "Terahertz communications in human tissues at the nanoscale for healthcare applications," *IEEE Trans. Nanotechnol.*, vol. 14, no. 3, pp. 404–406, May 2015.
[14] Q. H. Abbasi, A. Sani, A. Alomainy, and Y. Hao, "Numerical characterization and modeling of subject-specific ultrawideband body-centric radio channels and systems for healthcare applications," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 2, pp. 221–227, Mar. 2012.
[15] T. Binzoni, A. Vogel, A. Gandjbakhche, and R. Marchesini, "Detection limits of multi-spectral optical imaging under the skin surface," *Phys. Med. Biol.*, vol. 53, no. 3, p. 617, 2008.
[16] A. Gupta, M. Medley, and J. M. Jornet, "Joint synchronization and symbol detection design for pulse-based communications in the thz band," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–7.
[17] C. Han, J. M. Jornet, E. Fadel, and I. F. Akyildiz, "A cross-layer communication module for the Internet of things," *Comput. Netw.*, vol. 57, no. 3, pp. 622–633, 2013.
[18] J. M. Jornet and I. F. Akyildiz, "Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3211–3221, Oct. 2011.
[19] M. M. U. Rahman, A. Yasmeen, and J. Gross, "PHY layer authentication via drifting oscillators," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 716–721.
[20] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body area network authentication exploiting channel characteristics," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1803–1816, Sep. 2013.
[21] R. G. Cid-Fuentes, J. M. Jornet, I. F. Akyildiz, and E. Alarcon, "A receiver architecture for pulse-based electromagnetic nanonetworks in the terahertz band," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 4937–4942.

MUHAMMAD MAHBOOB UR RAHMAN (M'16) received the B.Sc. degree in electrical engineering from the University of Engineering and Technology (UET), Lahore, Pakistan, in 2007, and the Ph.D. degree in electrical & computer engineering from The University of Iowa, Iowa City, IA, USA, in 2013. During the summer of 2013, he worked as a Research Intern with the Wireless Systems Laboratory, Nokia Research Center, Berkeley, CA, USA. He then joined the Communication Theory Laboratory, KTH Royal Institute of Technology, Stockholm, Sweden, as a Post-Doctoral Researcher where he worked till April 2016. Since June 2016, he has been an Assistant Professor with the Electrical Engineering Department, Information Technology University, Lahore, Pakistan. Before undertaking his Ph.D. studies, he was a Lecturer/Lab Engineer with Faisalabad Campus, UET Lahore, Pakistan, from 2007 to 2009.

QAMMER H. ABBASI (S'08–M'12–SM'16) received the B.Sc. and M.Sc. degrees (Hons.) in electronics and telecommunication engineering from the University of Engineering and Technology (UET), Lahore, Pakistan, and the Ph.D. degree in electronic and electrical engineering from the Queen Mary University of London (QMUL), London, U.K., in 2012. From 2012 to 2012, he was a Post-Doctoral Research Assistant with the Antenna and Electromagnetics Group, QMUL. From 2012 to 2013, he was an International Young Scientist under National Science Foundation China, and an Assistant Professor with UET. From 2013 to 2017, he was with the Center for Remote healthcare Technology and Wireless Research Group, Department of Electrical and Computer Engineering, Texas A&M University (TAMUQ) initially as an Assistant Research Scientist and later was promoted to Associate Research Scientist and Visiting Lecturer, where he was the leading multiple Qatar National Research Foundation Grants (worth U.S. 3 million). He is currently a Lecturer (Assistant Professor) with the University of Glasgow in the School of Engineering in addition to a Visiting Research Fellow with QMUL and a Visiting Associate Research Scientist with TAMUQ. He has been mentoring several undergraduate, graduate students, and postdocs. He has contributed to a patent, over 100 leading international technical journal and peer-reviewed conference papers, and five books and received several recognitions for his research. His current research interests include compact antenna design, RF design and radio propagation, nano communication, biomedical applications of terahertz communication, antenna interaction with human body, implants, body centric wireless communication issues, wireless body sensor networks, noninvasive health care solutions, cognitive and cooperative network, and multiple-input-multiple-output systems. He has been a member of the technical program committees of several IEEE flagship conferences and technical reviewer for several IEEE and top notch journals. He contributed in organizing several IEEE conferences, workshop and special sessions in addition to European school of antenna course. He is an Associate Editor of the IEEE Access Journal and acted as a Guest Editor for numerous special issues in top notch journals.

NISHTHA CHOPRA (S'13) received the B.S. degree in electrical engineering from SRM University, Tamil Nadu, India, in 2010, the M.S. degree in nano-electronics from the University of Manchester, Manchester, U.K., in 2012, and the Ph.D. degree in electronics engineering from the School of Electronics Engineering and Computer Sciences, Queen Mary University of London, London, U.K., in 2017. She is currently a High Radiation Protection Scientist in public health england (NHS). Her research mainly focuses on THz technology, skin modeling and characterization, and nano-communication.

KHALID QARAQE (SM'00) was born in Bethlehem. He received the B.S. degree (Hons.) in electrical engineering from the University of Technology, Bagdad, Iraq, in 1986, the M.S. degree in electrical engineering from the University of Jordan, Amman, Jordan, in 1989, and the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 1997. From 1989 to 2004, he held a variety positions in many companies and has over 12 years of experience in the telecommunication industry. He was involved with numerous GSM, CDMA, and WCDMA projects and has experience in product development, design, deployments, testing, and integration. He joined the Department of Electrical and Computer Engineering, Texas A&M University at Qatar, in 2004, where he is currently a Professor. He has authored or co-authored 13 book chapters, two books, and four patents, and presented five tutorials and talks. He has authored or co-authored 90 journal papers in top IEEE journals, and published and presented 194 papers at prestigious international conferences. His research interests include communication theory and its application to design and performance, analysis of cellular systems and indoor communication systems. Particular interests are in mobile networks, broadband wireless access, cooperative networks, cognitive radio, diversity techniques, and beyond 4G systems. He has been awarded 15 research projects consisting of over USD 9.0 M from local industries in Qatar and the Qatar National Research Foundation (QNRF). He received the Itochu Professorship Award, 2013–2015, the Best Researcher Award, QNRF 2013, the Best Paper Award, the IEEE First Workshop On Smart Grid And Renewable Energy, in 2015, the Best Paper Award, IEEE Globecom 2014, the Best Poster Award at the IEEE Dyspan Conference, in 2012, the TAMUQ Research Excellence Award in in 2010, the Best Paper Award, ComNet, in 2010, the Best Paper Award, CROWNCOM, in 2009, and the Best Paper Award, ICSPC'0, in 2007.

AKRAM ALOMAINY (S'04–M'07–SM'13) received the M.Eng. degree in communication engineering and the Ph.D. degree in electrical and electronic engineering (specialized in antennas and radio propagation) from the Queen Mary University of London (QMUL), London, U.K., in 2003 and 2007, respectively. He joined the School of Electronic Engineering and Computer Science, QMUL, in 2007, where he is currently an Associate Professor (Senior Lecturer) with the Antennas and Electromagnetics Research Group. He has managed to secure various research projects funded by research councils, charities and industrial partners on projects ranging from fundamental electromagnetic to wearable technologies. He is the lead of Wearable Creativity Research at QMUL and has been invited to participate at the Wearable Technology Show 2015, Innovate UK 2015 and also in the recent Wearable Challenge organized by Innovate U.K. IC Tomorrow as a leading challenge partner to support SMEs and industrial innovation. He has authored and co-authored a book, five book chapters and over 150 technical papers (2800+ citations and h-index 25) in leading journals and peer-reviewed conferences. His current research interests include small and compact antennas for wireless body-area networks, radio propagation characterization and modeling, antenna interactions with human body, computational electromagnetic, advanced antenna enhancement techniques for mobile and personal wireless communications, and advanced algorithm for smart and intelligent antenna and cognitive radio system. He is a member of the Institute of Bioengineering and Centre for Intelligent Sensing at QMUL. He has won the Isambard Brunel Kingdom Award, in 2011, for being an outstanding young science and engineering communicator. He was selected to deliver a TEDx talk about the science of electromagnetic and also participated in many public engagement initiatives and festivals. He is a member of the IET, a Fellow of the Higher Education Academy (U.K.) and also a College Member for Engineering and Physical Sciences Research (EPSRC, U.K.) and its ICT prioritization panels. He is an Elected Member of U.K. URSI (International Union of Radio Science) panel to represent the U.K. interests of URSI Commission B (from 2014 to 2017). He is also a Reviewer for many funding agencies around the world, including the Expert Swiss National Science Foundation Research, the Engineering and Physical Sciences Research Council, U.K., and the Medical Research Council, U.K.