DOI: 10.5769/C2015004 or http://dx.doi.org/10.5769/C2015004

Continuous Authentication via Localization Using Triangulation of Directions of Arrival of Line of Sight Components

Marco A. M. Marinho, Paulo Roberto de Lira Gondim, and João Paulo C. L. da Costa

***Abstract*—A larger number of users work from a desktop computer and use their smartphones, tablets, and home computers to communicate, buy, organize, and store sensitive information. With the growth of the adoption of the Internet for tasks such as online banking and shopping, an increased focus has been given on the development of tools that enable secure transactions.**

This manuscript proposes the usage of direction of arrival estimation tools to provide continuous authentication. The location of a user within the network can be estimated by using triangulation of the user's wireless signal. The location estimates can be used to track a user's movement within a wireless network. The movement pattern can then be analyzed for possible indicators of fraud.

***Index Terms*—Continuous authentication, DOA estimation, MIMO**

I. Introduction

Verifying one's identity electronically has become the focus of extensive research. Not only does the user need to be authenticated to use a given system, but also the system itself so that the user can trust it. A picture of the importance of electronic authentication in the recent landscape is given by the revenue lost by companies due to Internet fraud. According to [1], approximately 3.4 billion dollars were lost in the year of 2011 due to on-line fraud. Therefore, considerable attention has been devoted by the scientific community to the development of new ways of improving security at every part involved in Internet transactions.

Most of the systems that rely on electronic authentication verify the user's identity in a single authentication step and then allow them to freely use the system either until they log out or for a given amount of time when they must be re-authenticated. The process of constant re-authentication in a system is known as continuous authentication. For systems that rely on continuous authentication users must constantly prove to the system who they are in order to continue operating it. Although these types of re-authentication improve security, they will most likely result in a negative impact on the perception a user has of the ease-of-use of a system.

Most of the modern user's systems are connected to core networks by wireless access networks. Such networks have become omnipresent in today's large cities and most of today's workplaces. They enable user mobility while delivering satisfactory data rates, and can be an economic choice in comparison to cabling of an entire floor or building. To keep up with the demand for higher networking speeds, most wireless networking standards have adopted the Multiple Input Multiple Output (MIMO) technology. Systems that employ MIMO also provide the physical requirements for the application of mathematical tools of array signal processing.

Array signal processing has developed many techniques towards the estimation of the direction of arrival (DOA) of a radio signal. Knowledge of the DOA offers outstanding benefits, such as spatial filtering. We refer here to many important DOA estimation methods, such as Iterative Quadratic Maximum Likelihood (IQML) [2], Root-WSF [3] and Root-MUSIC [4], Expectation Maximization (EM) [5], [6], [7], [8], the space Alternating Generalized Expectation Maximization (SAGE) [9], [10], [11] and Estimation of Signal Parameters via Rotational Invariance (ESPRIT) [12], which can be applied.

This manuscript proposes taking advantage of using components present at modern MIMO wireless communication systems for the estimation of the user location by means of DOA estimation. By obtaining the location of the user when he/she first authenticates, for example, using biometrics or a password, it is possible to enforce authentication on multiple levels.

The remainder of this work is divided into five sections. In Section II the problem of DOA estimation is detailed and explained. The localization of a user within a network is shown in Section III. In Section IV three ways of employing the estimated location to user authentication are discussed. In Section V numerical simulations are presented considering mobility models and the average location error as a metric. Finally, in Section VI conclusions are drawn.

II. Direction of Arrival Estimation

This section describes the steps involved in estimating the DOAs of a set of received signals in an antenna array. Subsection II-A details the data model. In Subsection II-B the estimation of the DOAs using the ESPRIT algorithm is presented.

A. Data Model

The baseband signal received at the m-th antenna of an antenna array composed of M antennas at time snapshot t

Marco Antonio Marques Marinho, Paulo Roberto de Lira Gondim, and João Paulo Carvalho Lustosa da Costa, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília-DF, Brasil, E-mails: marco.marinho@ieee.org, pgondim@ene.unb.br, joaopaulo.dacosta@ene.unb.br.

can be represented as

$$x_m(t) = \sum_{i=1}^{d} s_i(t) e^{j\cdot(m-1)\cdot\mu(\theta_i)} + n_m(t), \quad (1)$$

where $s_i(t)$ is the complex symbol transmitted by the i-th source at time snapshot t and $n(t)$ is the zero mean circularly symmetric (ZMCS) additive white Gaussian noise present at the antenna m at time snapshot t. $\mu(\theta_i)$ represents the spatial frequency of the signal transmitted by the i-th source. For this work the spatial frequencies of a signal impinging over the uniform linear array (ULA) are given by

$$\mu(\theta_i) = 2\pi \frac{\Delta}{\lambda} \cos(\theta_i), \quad (2)$$

where θ_i is the direction of arrival of the i-th signal, Δ is the separation between the antenna elements and λ is the wavelength of the incoming signal.

Equation (1) can be rewritten in matrix notation as

$$\mathbf{X} = \boldsymbol{AS} + \boldsymbol{N} \in \mathbb{C}^{M\times N}, \quad (3)$$

where $\boldsymbol{S} \in \mathbb{C}^{d\times N}$ is the matrix containing the N symbols transmitted by each of the d sources, $\boldsymbol{N} \in \mathbb{C}^{M\times N}$ is the noise matrix with its entries drawn from $\mathcal{CN}(0, \sigma_n^2)$, and

$$\boldsymbol{A} = [\boldsymbol{a}(\theta_1), \boldsymbol{a}(\theta_2), ..., \boldsymbol{a}(\theta_d)] \in \mathbb{C}^{M\times d}, \quad (4)$$

where θ_i is the azimuth angle of the $i-$th signal and $\boldsymbol{a}(\theta_i) \in \mathbb{C}^{M\times 1}$ is the array response, obtained by measurements, whose elements are $e^{j\cdot(m-1)\cdot\mu(\theta_i)}$.

The received signal covariance matrix $\boldsymbol{R_{XX}} \in \mathbb{C}^{M\times M}$ is given by

$$\boldsymbol{R_{XX}} = \mathrm{E}\{\boldsymbol{XX}^{\mathrm{H}}\} = \boldsymbol{AR_{SS}A}^{\mathrm{H}} + \boldsymbol{R_{NN}}, \quad (5)$$

where $(\centerdot)^{\mathrm{H}}$ stands for the conjugate transposition, and

$$\boldsymbol{R_{SS}} = \begin{bmatrix} \sigma_1^2 & \gamma_{1,2}\sigma_1\sigma_2 & \cdots & \gamma_{1,d}\sigma_1\sigma_d \\ \gamma_{1,2}^*\sigma_1\sigma_2 & \sigma_2^2 & & \vdots \\ \vdots & & \ddots & \\ \gamma_{1,d}^*\sigma_1\sigma_d & \gamma_{2,d}^*\sigma_2\sigma_d & \cdots & \sigma_d^2 \end{bmatrix}, \quad (6)$$

where σ_i^2 is the power of the $i-$th signal and $\gamma_{a,b} \in \mathbb{C}$, $|\gamma_{a,b}| \leq 1$ is the cross correlation coefficient between signals a and b. $\boldsymbol{R_{NN}} \in \mathbb{C}^{M\times M}$ is a matrix with σ_n^2 over its diagonal and zeros elsewhere. An estimate of the signal covariance matrix can be obtained by

$$\hat{\boldsymbol{R}}_{\boldsymbol{XX}} = \frac{\boldsymbol{XX}^{\mathrm{H}}}{N}. \quad (7)$$

B. ESPRIT

For DOA estimation this works uses the ESPRIT method since it is a closed form algorithm that can be very easily extended to multidimensional scenarios.

The ESPRIT parameter estimation technique is based on subspace decomposition. Matrix subspace decomposition is usually done by applying the Singular Value Decomposition (SVD). The SVD of the matrix $\boldsymbol{X} \in \mathbb{C}^{M\times N}$ is given by

$$\boldsymbol{X} = \boldsymbol{U\Lambda V}^{\mathrm{H}}, \quad (8)$$

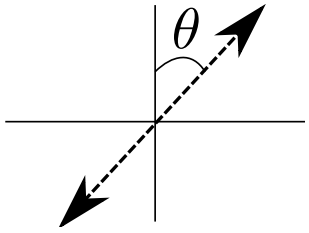

Figure 1. Depiction of possible ambiguity in signal propagation direction.

where $\boldsymbol{U} \in \mathbb{C}^{M\times M}$ and $\boldsymbol{V}^{N\times N}$ are unitary matrices called the left-singular vectors and right-singular vectors of $\boldsymbol{X}$ and $\boldsymbol{\Lambda} \in \mathbb{C}^{M\times N}$ is pseudo diagonal matrix containing the singular values of $\boldsymbol{X}$. The signal subspace $\boldsymbol{E}_S \in \mathbb{C}^{M\times \hat{L}}$ of $\boldsymbol{X}$ can be constructed by selecting only the left singular vectors related to the d largest singular values. The remaining singular vectors form the noise subspace $\boldsymbol{E}_N \in \mathbb{C}^{M\times M-d}$ of $\boldsymbol{X}$.

Equivalently, eigenvalue decomposition can be applied on the auto correlation matrix $\hat{\boldsymbol{R}}_{\boldsymbol{XX}}$ of $\boldsymbol{X}$ spanning the same subspace

$$\hat{\boldsymbol{R}}_{\boldsymbol{XX}} = \boldsymbol{E\Sigma E}^{-1}, \quad (9)$$

where $\boldsymbol{E} \in \mathbb{C}^{M\times M}$ and $\boldsymbol{\Sigma} \in \mathbb{C}^{M\times M}$ contains the eigenvectors and eigenvalues of $\boldsymbol{R}_{\boldsymbol{XX}}$. The eigenvectors related to the $\hat{L}$ largest eigenvalues span the same signal subspace $\boldsymbol{E}_S$ of the single value decomposition. The same holds for the noise subspace of the EVD and left singular vectors of the SVD, $\boldsymbol{E}_N$. With this subspace estimate at hand the Total Least Squares (TLS) ESPRIT [12] is applied.

The high accuracy provided by the ESPRIT algorithm is capable of yielding very precise results for the position estimation.

For multidimensional arrays another option is to employ methods based on the PARAFAC decomposition such as [13] [14] instead of ESPRIT.

III. Localization

It is important to notice that the DOA is given with respect to the reference of the $\boldsymbol{x}-$axis and cannot distinguish between front or back. Figure 1 displays this ambiguity.

The result is that each sensor possesses an estimated line in the ground plane where the transmitting node may be located. However, the acquisition of a set of line estimates enables obtaining a single estimate of the transmitting user localization. Figure 2 shows an example of imprecise estimates from three receiving nodes being used to estimate the position of the transmitter node. The problem is reduced to the least squares problem of finding the point of minimum distance from any of the possible combination of line estimates.

By writing the representing the line estimates as line equations of the type $Ax + By + C = 0$ in the sensor coordinate system, an estimate of the sensor position is given by

$$\{\hat{x}_0, \hat{y}_0\} = \min_p \frac{|A_{p_1}x_0 + B_{p_1}y_0 + C_{p_1}|}{\sqrt{A_{p_1} + B_{p_1}}} + \frac{|A_{p_2}x_0 + B_{p_2}y_0 + C_{p_2}|}{\sqrt{A_{p_2} + B_{p_2}}} + ..., \quad (10)$$

where p is an index set containing the possible combinations of estimated lines. While more than three sensors can be used to obtain increased accuracy, it also results in a higher

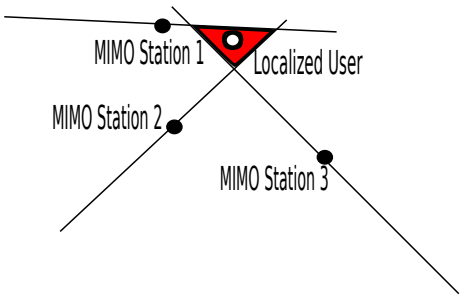

Figure 2. Example of a sensor triangulation using only the DOAs of the reference nodes.

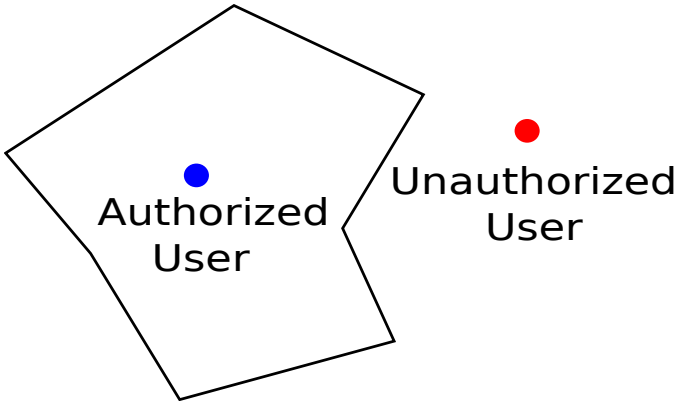

Figure 3. Example of border control via user localization.

computational load involved in the calculation of the minima. Once the lines have been choosen the final location estimate $S_0 = [x_0, y_0]$ can be found by taking the derivative of the above with respect to x_0 and y_0 and finding the point where it is equal to zero.

Furthermore, this technique may be used in conjunction with other localization methods such as the received signal strength indicator (RSSI). A set of candidate locations can be selected to choose the candidate that best fits the RSSI information.

IV. Authentication Mechanism

This section presents ways of using an estimation of the user's position for continuous authentication. Subsection IV-A shows how position estimation can be used to assure that a user only accesses a system when he/she is in an authorized area. In Subsection IV-B the position estimation is used to ensure a user has a speed compatible with network access metrics. Finally, Subsection IV-C shows how postion estimation can be used together with behavioaral movement metrics to provide continuous authentication.

A. Border Enforcing

Depending on the type of information being accessed, it may be important to enforce that the user only accesses a certain system or information if he/she is within a given area or set of areas. For instance, such approach could be beneficial to ensure that a user accessing a system is being monitored by a system of cameras. Thus, an unauthorized access could be registered on tape for further inquiry in the future. This is the simplest method for providing continuous authentication since there is only a single metric: the user is within the authorized access area. Figure 3 shows an example of an area constituted by a single polygon.

While the problem of verifying whether a point is inside a polygon or not has been thoroughly studied, the solution, in the case of irregular polygons, is resorting to ray tracing. Ray tracing may become complex depending on the nature and number of polygons, and the computational load can easily grow if the system needs to ensure proper location for a large number of users. However, since such calculations can be performed in a centralized authentication structure, large computational capacity can be provided.

As an example application, let us consider that a cellular system is divided into switching centers, and each switching center is divided into location areas, used for location of mobile terminals, when a mobile terminating call is presented to the cellular system. Each mobile terminal has some identities, e.g, International Mobile Subscriber Identity (IMSI) and Temporary MSI (TMSI). There is an association between location and security functions, since for each Location Area (LA) there is an assignment of a TMSI. In this sense, for each LA transition that occurs during the terminal movement, a new TMSI is assigned. Thus it is possible to reduce the area to be searched for localization purposes, limiting the search to cells included in the current LA.

B. Verification of Movement Speed

In networks that are not encrypted the problem of spoofing, i.e when a user pretending to be someone else, appears. Even when the system is encrypted, if the security key has been compromised an adversary may act as a spoofer in the network. This is a critical security problem and can be avoided by using the proposed method for user localization.

When a user first accesses the system or data he/she performs a standard authentication method to prove his/her identity to the system. During the process of authentication the users location is estimated by the system. The user must then transmit a set of pilot symbols at a fixed time interval so that his location can be reestimated at each transaction. By checking if the user is moving at a reasonable speed, the system can ensure that the one transmitting is still the original user who was authenticated.

Since, for this type of security, we assume that the system is either not encrypted or that the encryption key has been compromised, once the system detects an adversary operating as a spoofer, it must then warn the user of the presence of the spoofer, and, provide the estimated localization of the adversary to the authority in charge. Thus, in the case of an encrypted system, the user can obtain a new encryption key, and in unencrypted networks, the transactions are halted until the spoofer has been dealt with, avoiding any potential danger.

By measuring the distance between the current estimate A and the previous estimate B with

$$D_{\overrightarrow{AB}} = \sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}, \qquad (11)$$

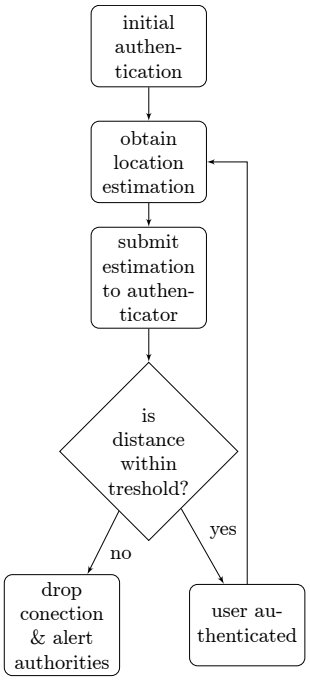

Figure 4. Flowchart of the proposed authentication method.

and defining a distance threshold between estimates it is possible to identify spoofers. Figure 4 shows a flowchart of the proposed authentication method. This simple estimation method can properly identify intruders posing as authorized users in MIMO wireless networks.

C. Analysis of Behavioral Movement

The last proposed method for providing continuous authentication while relying on the estimation of a user location analyzes the user movement behavior over the network coverage. Consider, for instance, a working environment. Most people have a frequent routine within their workspace. They remain seated in their workspace most of their working hours, they may approach their nearby colleagues at a given frequency, go to the bathroom, to the lunchroom, and visit the manager's desk. All this information defines the behavior of a person.

The first part of this approach is to obtain a statistical model of a person's movement within the coverage of a wireless network. This statistical model can be obtained, for instance, as a heat-map of a discretized grid of the coverage of the wireless network. This heat-map would represent a statistical model of the placement behavior of a given user. Figure 5 shows an example of the heat-map of a person that remains at a desk within a room. The comparison between the stored statistical model ant the heat-map obtained from a user during the day can provide the means of authenticating the user.

Although this approach requires a training stage, it is, possibly, the one of capable of enforcing the most efficient authentication. If a person's movement within a given space is enough to provide unique identification, this approach provides unique identification without requiring any user's input.

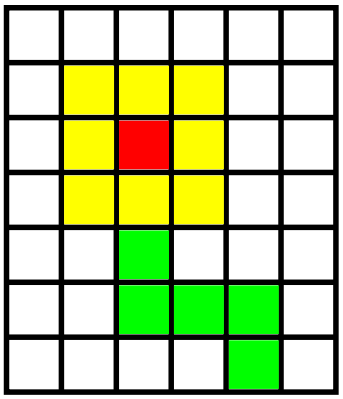

Figure 5. Example of movement heat-map

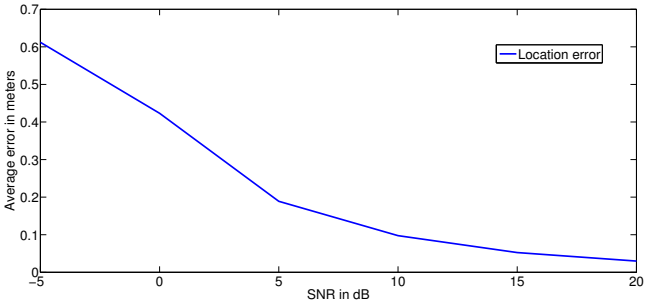

Figure 6. Average location error using the DOA based triangulation technique.

V. Numerical Simulations

In order to study the performance of the proposed solution in the presence of noise a set of numerical simulations was performed. The scenario tries to simulate an area of 45×45 m covered by three WiFi hotspots equipped with three antennas each. The number of snapshots used for the DOA estimation at each hotspot is $N = 50$. The snapshots used for the DOA estimation do not depend on the symbols transmitted over the 802.11 protocol, since the DOA estimation depends only on the narrow-band carrier signal.

We analyze the average location error for the given scenario in different SNR conditions. To perform this simulation a user is placed at a random location within the simulation area and its location is estimated. Figure 6 shows the average location error for 10000 random points.

For a SNR of 20 dB the technique proposed in Subsection IV-A is precise to within approximately 3 cm, i.e, the method can provide precise and online border enforcing for wireless system users under the simulated scenario. The precision of the method varies according to the number of WiFi hotspots and antennas present at each hotspot. The results shown in Figure 6 also validate the approach proposed in Subsection IV-B.

VI. Conclusion

This manuscript addressed an initial discussion on possible methods for providing continuous authentication while relying on DOA estimation in MIMO wireless networks. The mathematical tools for providing a precise DOA estimation

in antenna arrays were presented. Once a DOA estimate has been obtained, the system can then estimate the user's location within the network coverage.

By using the estimated user position, a set of rules can be enforced for the sake of obtaining a robust authentication system. The first set of rules regards the containment of the user within a set of boundaries. This can be easily implemented with the estimate of the users location. The second set regards the analyzes of the movement speed of the user within the network coverage. If the speed exceeds a certain value, the system considers the transaction is no longer safe due to the possible existence of a spoofer within the network. The third set of rules is the most complex, yet the one of highest potential for continuous authentication. By analyzing the behavior of a user's movement within the network, the authentication system could measure the difference between the momentary movement of the user and the stored behavior. If the user's movement is not similar enough to the stored behavior, the authentication fails. This is interesting, for instance, when a smartphone is lost or stolen. A user that has taken the smartphone will probably be distant from the owner of the phone. The system is then notified that the actions taken at the device are suspicious and should probably not be authorized.

The methods proposed in this work are still hard to be implemented in real systems, since the application of MIMO is in its infancy. The goal of the work is to lay down the foundation for providing continuous authentication based on user location inside a wireless network. Although it may not be efficient enough to provide precise authentication by itself, it can be a useful tool for improving the accuracy of a multimodal continuous authentication system that relies on other inputs, such as movement gait.

Acknowledgments

The authors wish to thank the Brazilian research and innovation Agencies CAPES (FORTE Project, CAPES Forensic Science Notice 25/2014) and FINEP (Grant RENASIC/PROTO 01.12.0555.00), for their support to this work.

References

[1] CyberSource, "2012 online fraud report," Tech. Rep., 2012.

[2] Y. Bresler and A. Macovski, "Exact Maximum Likelihood Estimation of Superimposed Exponentials Signals in Noise," *IEEE ASSP Magazine*, vol. 34, pp. 1081–189, 1986.

[3] P. Stoica and A. Nehorai, "A Novel Eigenanalysis Method for Direction Estimation," in *Proceedings IEEE F.*, 1990.

[4] A. J. Barabell, "Improving the Resolution Performance of Eigenstructured Based Direction-Finding Algorithms," in *Proceedings of ICASSP 83*, 1983.

[5] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum Likelihood from Incomplete Data via the EM Algorithm," *J. Royal Statistical Soc. B.*, vol. 39, no. 1, 1977.

[6] T. K. Moon, "The Expectation-Maximization Algorithm," *IEEE Signal Processing Magazine*, November 1996.

[7] G. J. McLachlan and T. Krishnan, *The EM Algorithm and Extensions*. John Wiley & Sons, Inc., New York, 1997.

[8] M. Miller and D. Fuhrmann, "Maximum-Likelihood Narrow-Band Direction Finding and the EM Algorithm," *IEEE Transactions on Acoustics Speech and Signal Processing*, vol. 38, pp. 1560–1577, 1990.

[9] J. A. Fessler and A. O. Hero, "Space-Alternating Generalized Expectation-Maximization Algorithm," *IEEE Transactions on Signal Processing*, vol. 42, no. 10, October 1994.

[10] F. A. Dietrich, "A Tutorial on Channel Estimation with SAGE," *Technical Report TUM-LNS-TR-06-03*, 2006.

[11] F. Antreich, J. Nossek, G. Seco-Granados, and A. Swindlehurst, "The Extended Invariance Principle for Signal Parameter Estimation in an Unknown Spatial Field," *IEEE Transactions on Signal Processing*, vol. 59, no. 7, pp. 3213–3225, July 2011.

[12] R. Roy and T. Kailath, "ESPRIT - estimation of signal parameters via rotation invariance techniques," *IEEE Transactions on Acoustics Speech and Signal Processing*, vol. 17, 1989.

[13] J. P. C. L. da Costa, D. Schulz, F. Roemer, M. Haardt, and J. A. A. Jr., "Robust R-D Parameter Estimation via Closed-Form PARAFAC in Kronecker Colored Environments," in *Proc. 7-th International Symposium on Wireless Communications Systems (ISWCS 2010)*, 2010.

[14] J. P. C. L. da Costa, F. Roemer, M. Weis, and M. Haard, "Robust R-D parameter estimation via closed-form PARAFAC," in *Proc. ITG Workshop on Smart Antennas (WSA'10)*, 2010.