Li, Yilin; Liu, Shushu; Yan, Zheng; Deng, Robert H.

# Secure 5G Positioning with Truth Discovery, Attack Detection and Tracing

*Published in:*
IEEE Internet of Things Journal

*DOI:*
10.1109/JIOT.2021.3088852

E-pub ahead of print: 14/06/2021

*Document Version*
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

*Please cite the original version:*
Li, Y., Liu, S., Yan, Z., & Deng, R. H. (2021). Secure 5G Positioning with Truth Discovery, Attack Detection and Tracing. *IEEE Internet of Things Journal*. Advance online publication.
https://doi.org/10.1109/JIOT.2021.3088852

# Secure 5G Positioning with Truth Discovery, Attack Detection and Tracing

Yilin Li, Shushu Liu, *Student Member, IEEE,* Zheng Yan, *Senior Member, IEEE,* and Robert H. Deng, *Fellow, IEEE*

**Abstract**—The fifth-generation (5G) cellular network is expected to provide sub-meter positioning accuracy without draining the battery of user equipment. As a solution, ultra-dense network (UDN) deployment and network-based positioning were proposed. However, the openness of UDN and the vulnerability of network devices (e.g., access nodes) make it easy for attackers to poison such a positioning system. However, no existing work explores how to overcome this issue. This paper concentrates on jamming and collusion attacks in the network based positioning system. Specifically, we design a novel scheme that contains three functional modules to erase the influence of these attacks. A truth discovery module applies a clustering-based method aiming to generate the most approximate position value and find out suspicious signals. Based on neural network models, we further develop an attack detection module and an attack tracing module to perceive attacked user equipment and locate malicious or attacked access nodes. Through simulation, we conduct extensive experiments to illustrate the effectiveness of our scheme. The result shows high detection and tracing accuracy with very simple neural network models, which also implies the potential of our proposed scheme in practical deployment.

**Index Terms**—5G positioning, neural network, clustering, truth discovery, attack detection and tracing

## 1 INTRODUCTION

The development of network and communication technology stimulates positioning technology to a centimetre level and brings precise location-based services to mobile users. To further reduce power consumption at terminal equipment, the fifth generation (5G) network adopts network-based positioning technology [1] with a data fusion center (FC) deployed by the network. The data fusion center first collects parameters from facilities that have a direct communication with user equipment (UE) and then estimates the position of the UE based on these parameters. Since positioning computation is allocated at network side, the energy consumption at UE can be greatly released.

Despite of its advantage, such a positioning system is actually threatened by various attacks [2]. Due to the openness and vulnerability of involved devices, positioning accuracy will be decreased if the signals sent to access nodes (AN) are interfered by an attacker. In a worse case, if the attacker is capable of hacking or setting up malicious access nodes, it is likely to result in regional service failure. Thus, it is essential to investigate an effective scheme to solve these problems.

Traditional solutions mainly focus on improving the accuracy of positioning by eliminating the influence of non-line-of-sight (NLoS) signals. For example, Qi et al. [3] treated NLoS as random variables added to line-of-sight (LoS) components and used both to estimate position. Based on millimeter wave (mm-wave) and multiple-input-multiple-output (MIMO) technologies, Talvitie et al. [4] proposed new channel parameter extraction algorithms that enable precise orientation calculation even in an NLoS scenario. In general, NLoS mitigation techniques can be summarized into three categories according to the types of localization solutions: machine learning by utilizing NLoS statistics, weighted least squares algorithms, and robust estimators [5]. By employing these techniques, they can identify and discard NLoS signals. However, these techniques are unable to attain position accuracy when the positioning system is under attacks, not mention how to find an attack and locate the source of the attack. While there are some related work on attack detection and defence, they are designed case-by-case and not suitable for network-based positioning.

In this paper, we propose a novel scheme that consists of three modules to erase the influence of above attacks in the network-based positioning system. Specifically, our scheme contains a truth discovery module, an attack detection module and an attack tracing module. The truth discovery module aims to recognize abnormal data and generates the most approximate position value. In each positioning, we suppose that limited by the attacker's ability, the attacks only influence part of the collected data of the FC, normally below 50% of the total. Thus, the uninfluenced clean data should be over half and can be easily gathered together through optimal measurement. As a solution, a clustering algorithm is applied to classify the positioning data uploaded by multiple access nodes, and the data not included in the final cluster is labelled as abnormal and eliminated in the process of estimating the most approximate position. Based on comparison, density-based spatial clustering of applications with noise (DBSCAN) [6] is selected as our default clustering algorithm for its superiority in performance and configuration convenience.

*The first two authors contribute equally to the work.*
*Y. Li is with the State Key Lab of Integrated Services Networks, School of Cyber Engineering, Xidian University, 710071, Xi'an, China (email:upclin@qq.com).*
*S. Liu is with the department of Communications and Networking, Aalto University, Konemiehentie 2, 02150 Espoo, Finland (email:liu.shushu@aalto.fi).*
*Z. Yan is with the State Key Lab of Integrated Services Networks, School of Cyber Engineering, Xidian University, 710071, Xi'an, China and the Department of Communications and Networking, Aalto University, Konemiehentie 2,, 02150 Espoo, Finland (e-mail: zheng.yan@aalto.fi).*
*R. H. Deng is with the School of Information Systems, Singapore Management University, Singapore 188065, Singapore(emial: robertdeng@smu.edu.sg).*

The attack detection module detects whether UE is under attacks and the attack tracing module helps locate attack sources (e.g., attacked ANs) for troubleshooting. Concretely, we train two neural network models with attack detection and attack tracing ability, respectively. The training data is the historical data collected by the (FC) in the positioning system. Based on these data, distinctive features are extracted and adopted for separately training the two models. These two trained models can be respectively used to predict the status of UE and AN by directly applying the observed data related to them during positioning. Owing to the effectiveness of feature extraction, both modules can achieve high accuracy by applying simple neural network models. The simplicity of the adopted model also makes our scheme very practical due to the ease of training towards future deployment in the positioning system.

Additionally, we evaluate the performance of our scheme through simulations in terms of positioning accuracy, attack detection accuracy and tracing accuracy focusing on overcoming jamming and collusion attacks, the two most typical attacks on network-based positioning. The experimental results show that the proposed scheme has good robustness and can effectively resist the above attacks. In summary, the contribution of this paper can be summarized as below.

- We are the first to study the security of 5G network-based positioning and propose clustering-based truth discovery to provide high positioning accuracy under two most typical attacks.
- We are also the first to employ two neural network models to detect potential attacks and trace attack sources in the context of 5G network-based positioning.
- We conduct extensive simulation-based experiments to prove the effectiveness of our proposed scheme, considering the lack of 5G positioning datasets and for the convenience of simulating various attacks for performance test.

The organization of this paper is as follows. Section 2 briefly reviews related work to show the novelty of our paper work. Section 3 specifies the architecture and threat model of the 5G network-based positioning system, followed by the details of our proposed scheme including the design of three functional modules in Section 4. The simulation and experimental results are presented in Section 5. Finally, we conclude this paper in the last section.

## 2 RELATED WORK

### 2.1 Positioning Accuracy

Many works have been focusing on improving positioning accuracy to fulfil the sub-meter requirement proposed in a 5G white paper [7]. By exploiting the sparsity of 5G millimetre wave channel, Talvitie et al. [4] proposed new algorithms for accurate channel parameters estimation to achieve precise estimation of device position and orientation. Similar idea was also proposed by Shahmansoori et al. [4]. To eliminate errors in wifi-based localization, Liu et al. [8] presented a peer-assisted localization approach by leveraging peer range as a constraint in location mapping. Menta et al. [9] provided sub-meter positioning accuracy through arrival-of-angle based localization in 5G UDNs. Koivisto et al. [10] concentrated on continuous positioning of cars in UDNs. Instead of the global positioning system (GPS), Zhao et al. [11] solved the positioning and identification of unmanned aerial vehicles (UAV) depending on a 5G millimeter wave radar technology.

The above works greatly improve positioning accuracy in areas with poor network coverage, such as indoor or a high-speed environment where the usage of GPS is limited. However, these techniques are unable to attain the accuracy when the positioning system is under attacks, which is an crucially important issue that we aim to solve in this paper.

### 2.2 Attack Detection and Defence

Apart from accuracy, attack detection and defence is another crucial issue in positioning. Several works focused on GPS spoofing attack. Kai et al. [12] leveraged crowdsourced air traffic monitoring sensor networks to detect and locate GPS spoofing attacks in aviation. The proposed system can globally detect GPS spoofing attacks in two seconds and locate an attacker within 15 minutes. Likewise, Manesh et al. [13] proposed to detect GPS spoofing signals by using a model trained with features like pseudo-range, doppler shift and signal-to-noise ratio (SNR). Wang et al. [14] presented a GPS signal reconstruction technology by adopting edge computing as a backup to resist GPS spoofing attacks. Obviously, the above works relate to GPS attacks and defence, not about 5G network-based positioning. Thus, they cannot be directly applied into it or their application need additional investigation.

For other works, Singh et al. [15] designed the first secure ranging system that is resilient to both distance enlargement and reduction attacks. Besides, the designed system can be implemented directly on top of existing 5G-NR transceivers. Abdalla et al. [16] summarized the attacks and corresponding mitigation strategies of 5G networks by leveraging UAVs. A mutual authentication scheme aiming at improving data privacy in vehicle positioning was proposed by Ometov et al. [17]. As we can see, although many efforts have been devoted in attack detection and defence, they are designed case-by-case and not suitable for solving our targeting problems.

## 3 SYSTEM OVERVIEW AND THREAT MODEL

### 3.1 5G Positioning System

According to the 5G white paper [1], [18], we consider 5G UDNs as high spatial density where ANs are attached to lamp posts with a couple of tens of meters between each other, which in result greatly increases the LoS condition between UEs with multiple ANs at a time [19]. Normally, each AN is equipped with an antenna array allowing for estimating the direction of arrival (DoA) of a signal and AN locations are fixed and known from the GPS. Due to the dense network of ANs, the signal from UE is likely measured by 5 or more ANs, which normally outnumbers signals required. But thanks to this, redundant information

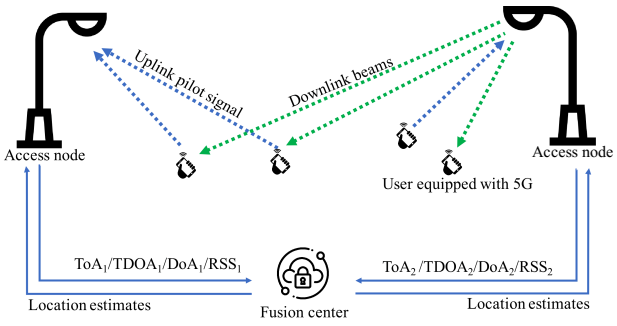


Fig. 1. Illustration of a 5G UDN where the ANs are attached to lamp posts, and UEs transmit periodical uplink pilot signals to the ANs. The position estimation is carried out by a FC and send back to UEs through downlink beams.

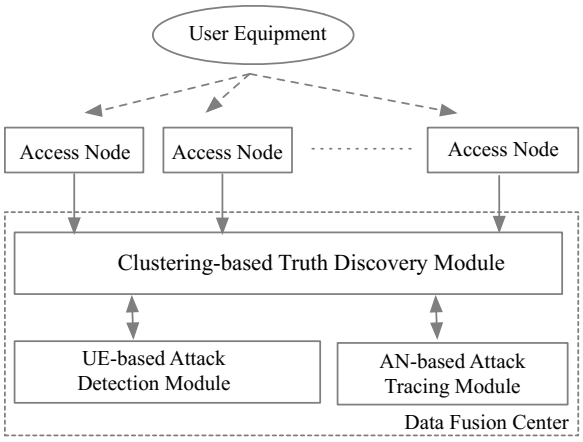


Fig. 2. Scheme Overview

can be leveraged to detect measurement errors and improve positioning accuracy.

The positioning process is illustrated in Fig. 1. UE transmits periodical uplink pilot signals to ANs. Each AN selects the ones in a LoS condition by measuring their Rician K factors of the received signal strength indicator (RSSI), which is typically 10-20 dB in UDNs [20]. Based on selected signals, the directional and temporal parameters, i.e. time of arrival (ToA) and DoA of UE are extracted and delivered to a FC that carries out the computation of UE position. Note that the FC is a networked device with capability of computation, storage and communication connection. It can be a road side unit, a base station or even an outsourced cloud service provider. Eventually, the position information is sent back to UE through downlink beams or by FC directly.

### 3.2 Threat Model

#### 3.2.1 Assumptions

We assume ANs are semi-trusted parties that could transmit erroneous parameters to FC and deteriorate the positioning system. Since ANs are in the open-access network and poorly equipped with defence strategies, they are easily hacked and controlled by malicious attackers. On the contrary, we suppose FC is a fully trusted party run by a positioning service provider like Google Maps or a network operator. It is against its benefits to be a malicious party. We also assume that the connection between UE and ANs is based on wireless communications with the risk of intentional and unintentional interference, while the connection between ANs and FC is based on a stable channel with a security guarantee by employing a highly secure communication protocol. Noted that UE is a service receiver that has no direct access to the positioning process except initiating positioning and receiving a positioning result. Thus, it is legitimate to take UE as a trusted party.

#### 3.2.2 Attacks

Based on the assumption, we consider two main active attacks. The first is *radio jamming attack* (also known as man-in-the-middle attack), in which we assume the adversary can intercept the positioning signalling path between UE and AN, thereby an attacker can alter the signalling by transmitting energy to disrupt reliable data communications, normally through a jammer. It is notable that by resisting this attack, the positioning system will become more robust to unintentional interference also. The second is *collusion attack*, in which we assume an adversary can hack or even set up fake ANs in 5G networks and send wrong or erroneous signal measurements to deteriorate the positioning system. By detecting the collusion attack, we can eliminate the presence of malicious nodes in the system effectively.

We also suppose that the signals and ANs are partially influenced by attacks, limited by attackers' ability. This is a reasonable assumption as the radio jamming attack normally influences the signals in one direction and the effort to conduct collusion attack by hacking ANs limits the number of attacked ANs. The percentage of influenced signals and ANs under both attacks is variable and influenced by many factors. By experience, we suppose that the percentage is normally below 50% of the total signals and ANs. Another thing to notice is that the percentages of influenced signals and ANs also impact the setting of abnormal positioning status in the feature extraction of attack detection. When the percentage of influenced signals and ANs increases, the threshold to decide abnormal positioning status should be updated accordingly also.

**Remark.** *In this paper, we emphasize active attacks that could deteriorate the accuracy of the positioning system. Since passive attacks like eavesdropping normally violate the privacy of UE, but make no harm to positioning accuracy, thus, they are out of the scope of this paper. Eavesdropping can be solved by enhancing communication channel security with signal protection.* [21].

## 4 SECURE POSITIONING WITH TRUTH DISCOVERY, ATTACK DETECTION AND TRACING

Based on 5G UDN, this section describes our proposed scheme in detail. Fig. 2 overviews the scheme. In the network-based positioning, the whole scheme process is operated by the FC. It contains three modules: truth discovery, attack detection and attack tracing. The truth discovery module is initiated once all required parameters are collected from ANs. It aims to cluster collected parameters

and calculate their true value by leaving out outliers. Based on the clustering result, attack detection and tracing can be further performed. The detailed design of each module is described below.

### 4.1 Truth Discovery

The main idea of truth discovery is to label the data collected from ANs with a clustering algorithm and then calculate the position only based on non-noise data. The process is composed of three phases:

#### 4.1.1 Position Parameter Collection

To obtain the positioning service, UE periodically transmits uplink pilot signals to surrounding ANs. Once receiving the pilot signals, ANs extract position parameters like ToA and DoA from them and upload the estimated parameters to the FC through a secure communication channel. The transmitted message between an AN and the FC is represented as

$$\{(X_i, Y_i), (ToA_{i,j}, DoA_{i,j}, AN_i, UE_j, ID\}$$

, where $i$ and $j$ are the identifications of AN and UE, respectively; $(X_i, Y_i)$ denotes the coordinate location of $AN_i$; $(ToA_{i,j}, DoA_{i,j})$ denotes the extracted parameters of $UE_j$ from $AN_i$ and $ID$ is the signal identification. For $UE_j$ positioning, we suppose there are multiple ANs included for its position calculation and ANs' signals related to $UE_j$ are labelled with same $ID$.

#### 4.1.2 True Value Detection

Based on the received parameters from $AN_i$, the FC estimates the position of $UE_j$ with the following formula:

$$\begin{cases} x_j = (ToA_{i,j} * c) * cos(DoA_{i,j}) + X_i \\ y_j = (ToA_{i,j} * c) * sin(DoA_{i,j}) + Y_i \end{cases} \quad (1)$$

Thus, for every $UE_j$, there will be a location set $D = \{(x_{j,1}, y_{j,1}), (x_{j,2}, y_{j,2}), \ldots, (x_{j,n}, y_{j,n})\}$ where $n$ is the number of ANs involved in the positioning process.

However, the above locations may be inaccurate as the existence of various attacks. To eliminate their influence, we use a clustering algorithm to detect outliers. The algorithm is presented in Alg. 1. It is designed based on DBSCAN [6] for its sound performance and adaptability in clustering. We also justify our choice by comparing different clustering methods in the experiments in Section 5. For the distance measurement in clustering, we adopt Euclidean distance [22], which has been widely used in distance measurement in highly dimensional scenarios.

In the algorithm, we firstly initialize scan radius $\epsilon$ and minimum items $min$ as required. Also, all the locations are labelled as $'Initial'$ when they are not processed. Then we iterate over every estimated point in $D$. For each point $P \neq 'Initial'$, we calculate the number of points included in a circle with $P$ as a center and $\epsilon$ as its radius by calling function RangeQuery (in Alg. 2), which returns a point set noted as $RQ$. If the number of points in $RQ$ is smaller than $min$, point $P$ is labelled as $'Noise'$, otherwise, a new cluster $C_{new}$ is created with $P$ as an included item. Then, another round of RangeQuery is conducted on all the neighbours of $P$, which are stored in $RQ$. The process stops when all the points in $D$ are processed and the result of the algorithm is returned as the $K$ clusters in $C$.

**Algorithm 1:** Clustering-based True Value Detection

**Input:** $D = \{(x_1, y_1), (x_2, y_2), \ldots, (x_N, y_N)\}$
**Output:** $C = \{C_1, C_2, \ldots, C_K\}$

intial $\epsilon$, $min$, $C$
**for** each point $P$ in $D$ **do**
  **if** $P \neq 'Initial'$ **then**
    $continue$
  **end if**
  Neighbors $RQ$ = RangeQuery($D$, $P$, $\epsilon$)
  **if** $|N| \leq min$ **then**
    $label(P) = 'Noise'$
    $continue$
  **end if**
  $C = C + C_{new}$
  $C_{new} = C_{new} + P$
  $S = RQ \backslash P$
  **for** each point $Q$ in S **do**
    **if** $Q = 'Noise'$ **then**
      $C_i = C_i + Q$
    **end if**
    **if** $Q \neq 'Noise'$ **then**
      $continue$
    **end if**
    $C_{new} = C_{new} + Q$
    Neighbors $RQ$ = RangeQuery($D$, $P$, $\epsilon$)
    **if** $|N| \leq min$ **then**
      $label(P) = 'Noise'$
      $continue$
    **end if**
  **end for**
**end for**

**Algorithm 2:** RangeQuery

**Input:** $D$, $P$, $\epsilon$
**Output:** $RQ$

Neighbors $RQ$ = null
**for** each point $Q$ in $D$ **do**
  **if** $Euclidean(Q, P) \leq \epsilon$ **then**
    $RQ = RQ \cup \{P\}$
  **end if**
**end for**
$return\ RQ$

#### 4.1.3 Position Calculation

Since we suppose the number of affected data caused by interference or corrupted ANs are always less than half of total data in each positioning ($\leq n/2$), the parameter data with high accuracy should be over 50%. Thus, the clusters in $C$ with the most items is the one containing clean data. The real location of $UE_j$ can be calculated by averaging the points from this cluster and returned to $UE_j$. The rest points not included in the calculation are labelled as noise data and will be used as input for attack detection and tracing.

**Note:** For simplicity, the presented truth discovery module is designed according to the positioning method based on ToA and DoA, where a position can be inferred from the

signal of one AN. However, the truth discovery module can be extended to other methods that involve more than one AN. For example, in the traditional ToA based method that involves three ANs in positioning. In this case, different positions can be firstly estimated from the combination of ANs. Based on these estimated positions, the clustering algorithm is applied to find out the outliers. The real location can be calculated by averaging the positions without the outliers. Further in the attack detection and tracing, all the ANs contributing to the outliers will be labelled as suspicious and counted as abnormal. For other positioning methods, our scheme can work similarly by using the applied positioning method.

### 4.2 Attack Detection

Radio jamming attack intercepts the communication channel between UE and AN by injecting noise signals through a jammer. It is especially dangerous when the attacker knows UE's movement, as it can follow UE and keep it under attack all the time. The attack detection module is designed for finding attacked UEs so that the attacked UEs can be alerted as soon as possible.

Our solution is to train a machine learning model with the ability to perform attack detection. The training dataset $U$ is historical positioning data collected by the FC. For simplicity, we denote the record of $U$ as $u = \{(x_1, y_1, l_1), (x_2, y_2, l_2), \ldots, (x_n, y_n, l_n)\}$, where $(x, y)$ is the position information of UE estimated by the $n$th ANs and $l$ is the label generated by truth discovery. Based on the training dataset, feature extraction, model training are conducted.

#### 4.2.1 Feature Extraction for Attack Detection

Feature extraction is an essential step to generate formatted, non-redundant and informative data to facilitate model training. Four distinctive features are applied for attack detection as described below with justification.

**(a) Abnormal Positioning Data Ratio (APDR)**

It refers to the percentage of "Noise" signals in each UE positioning. For each record, it is calculated as $APDR = t \ / \ n$, where $t$ is the number of "Noise" data and $n$ is the total number of ANs participated in positioning. Owing to the density distribution of ANs in 5G UDN, UE keeps LoS signals communication with ANs when no interference appears, which keeps APDR at a low level. When UE is under attacks, APDR increases with increased "Noise" data related to the attacked UE. Obviously, APDR is a good indicator to reflect the status of UE.

**(b) Abnormal Positioning Status (APS)**

It is set as 1 when noise data is over 20% in each positioning, otherwise, it is 0. Normally, APS is activated as 1 when the communication channel between UE and AN is under attack. This feature is selected to complement APDR. When an attack only influences one or two data and APDR is relatively small, the attack may be ignored. APS is designed to capture this situation. Besides, the setting of percentage in APS can be adjusted according to real demands. A smaller setting indicates a more sensitive model, which leads to more strict attack detection.

**(c) Positioning Error Mean (PEM)**

It refers to the mean error between the measured positions and the FC estimated approximate position from truth discovery in each record. The computation of PEM is:

$$PEM = \frac{\sum_{j=1}^{n} ||(x_i, y_i) - (\bar{x}, \bar{y})||}{n},$$

Where, $(x_i, y_i)$ is the measured position and $(\bar{x}, \bar{y})$ is the FC estimated approximate position. Similar to APDR, PEM is also a good indicator of UE status, which changes when UE is in different status. It keeps low when UE is in a normal state while increases when UE is attacked.

**(d) Positioning Error Variance (PEV)**

It refers to the mean variance between measured and estimated positions. PEV is a necessary feature as it reflects the deviation of position data when PEM is relatively small. However, PEM detection is invalid when the attackers try to control PEM at a low level by turning off the attack from time to time. When PEV is included in the feature set, we can detect such a smart attack.

**Remark.** *These features are selected with experiences. The effectiveness of the selected features can be proved with the accuracy (98.10%) of attack detection, as shown in table 5. Better feature combination can be further explored in future work.*

#### 4.2.2 Model Training

We design the neural network model with 4 inputs and 1 output. The training data is composed of the above specified features and labelled as 0 or 1 according to UE status. 0 indicates a normal state while 1 indicates that UE is under attack. Normalization is applied to each feature so that the difference between features can be balanced, thus they contribute similarly to UE status prediction. After training, the trained model can be used directly. When in use, we collect the observation data of UE and generate the same features from these data. With these features as input, the trained model outputs 0 or 1 corresponding to a normal or attacked status of UE. Note that it is possible to simply compose these features into a function and predict the status with function output. However, an explicit function that can best simulate the input and output is hard to define and it is also challenging to find the optimal parameters in the function. While neural network model solves these two tricky problems easily. It can simulate the relationship between input and output with high accuracy without an explicit function required and it can automatically learn the best weights for each feature through training.

### 4.3 Attack Tracing

Another crucial implementation is attack tracing aiming to detect corrupted ANs. It is very essential as it helps relocate the sources of attacks. Likewise, the problem can be solved by applying machine learning. The training dataset $A$ contains the historical data of ANs. We denote each record as $a = \{(x_1, y_1, l_1, t_1), (x_2, y_2, l_2, t_2), \ldots, (x_n, y_n, l_n, T)\}$, which includes the positioning data uploaded by an AN in a time period $T$.

#### 4.3.1 Feature Extraction for Attack Tracing

Based on dataset $A$, we extract and train the model of attack tracing according to the following three typical features.

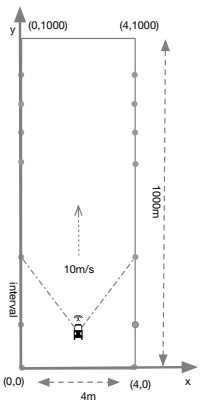


Fig. 3. Simulation framework

**(a) Abnormal Upload Ratio (AUR)**

It refers to the percentage of "Noise" data uploaded by an AN. When an AN is attacked or corrupted, its data uploaded is dirty with high probability. The value of AUR is relatively small when AN is in a normal state but increases when AN is under attack or malfunctions. Thus, it is a good indicator to reflect the status of AN.

**(b) AN Positioning Error Mean (APEM)**

APEM refers to the error mean between the estimated and approximate position. It is calculated as

$$APEM = \frac{\sum_{i=1}^{M} ||(x_i, y_i) - (\bar{x}, \bar{y})||}{M}$$

, where $(x_i, y_i)$ is the position measured by AN, $(\bar{x}, \bar{y})$ is the approximate position of UE estimated by FC, and $M$ is the number of uploaded signals from the AN in the time period $T$. APEM is chosen as a typical feature because attacks on AN results in big deviation between the position measured by AN and the approximate position, which causes APEM increase.

**(c) AN Positioning Error Variance (APEV)**

It refers to the error variance between the estimated and approximate positions. For malicious ANs, they can evade the detection based on APEM by acting an on-and-off attack, so that the APEM can be controlled within an acceptable range. When APEV is included in the feature set, it overcomes the shortcoming of APEM for detecting the on-and-off attack.

**Remark.** *Similarly, these features are selected with experiences. The effectiveness of the selected features can be proved by the accuracy (98.24%) of attack tracing, as shown in table 6. Better feature combination can be further investigated in future work.*

#### 4.3.2 Model Training

We design a neural network with 3 inputs and 1 output. The training data are also labelled as 0 or 1 according to the status of an AN, where 0 means that the AN is normal and 1 means it is attacked. When in use, for each AN involved in the positioning of UE, the FC extracts the features from its uploaded data in time period $T$ and inputs them into the trained model. A set of values $\{r_1, r_2, \ldots, r_n\}$ is obtained as the output with regard to a number of $n$ ANs. $AN_i$ is normally functioned when $r_i$ is 0 and under attack if $r_i$ is 1. In this way, we can locate all the ANs under attacks and fix them in time.

### 4.4 The Discussion Of Implementation

The practical implementation of our solutions should be conducted by the position service provider that is normally a Telecom operator. The proposed modules should be integrated into its fusion center and operated whenever a positioning request is generated. Since the truth discovery module is just an algorithm with no special requirements, it can be deployed directly. For attack detection and attack tracing, difficulty resides in the training of neural network models. These two models can be trained directly if there is historical data available. For the situation when the region is newly built and there are no historical data available, we can train the model with simulated data and keep the model updated once new data available. The simulated data can be generated through Ultra-Dense Network (UDN) simulation platforms like OTDoA provided by Liu et al. [23]. With the trained model, the whole scheme can be operated smoothly as we describe above. In addition, transfer learning, federated learning and other learning methods can also be investigated to support scheme deployment in practice to overcome lacking data issue.

## 5 Experimental Evaluation

### 5.1 Simulation Framework

5G UDN is still unavailable at the moment of our paper work. Our experiment is conducted based on simulations. Besides, a simulated testbed is flexible to arrange the distribution of ANs and simulate attacks that are necessary in studying the performance of our scheme.

**Experimental Environment** The simulation is performed on a laptop equipped with macOS system, 3.1GHz Intel Core i5 and 8GB RAM. Specifically, we simulate the 5G UDN positioning system with MATLAB and generate the positioning data under different attack scenarios. The modules for truth discovery, attack detection and tracing are implemented with python.

TABLE 1
Parameter settings

| Parameters | Values |
|---|---|
| Interval distance (m) | 20,40,**60**,80,100,120 |
| Number of ANs participated | 2,4,6,**8**,10,12 |
| Standard deviation of ToA noise (ns) | 8,**9**,10 |
| Standard deviation of DoA noise (°) | 1,**2**,3 |

**Experiment Setup** The simulation setup is as shown in Fig. 3. We assume the whole region is a one-way lane with $4m$ width and $1000m$ length and all the positions are relative coordinates to the origin of coordinate as labeled in Fig. 3. ANs denoted as grey circles are distributed along the road sides with even interval between each other. There is one car, denoted as UE, moving along the $y$ axis with a constant speed of $10m/s$. UE keeps sending positioning signals at a frequency of $20s^{-1}$ to all the ANs, which means it can get positioning service every $0.05s$.

TABLE 2
Example of simulated dataset

| | $AN_1$ | $AN_2$ | $\cdots$ | $AN_N$ |
|---|---|---|---|---|
| $t_1$ | $(ToA, DoA)$ | $(ToA, DoA)$ | $\cdots$ | $-$ |
| $t_2$ | $(ToA, DoA)$ | $(ToA, DoA)$ | $\cdots$ | $-$ |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |
| $t_l$ | $-$ | $-$ | $\cdots$ | $(ToA, DoA)$ |

$t$ represents the time when UE moves along y-aix. $(ToA, DoA)$ is the time of arrival and direction of arrival between UE and each AN, $-$ means no signal collected when UE is out of the range of AN

### 5.2 Dataset and Evaluation Metrics

**Dataset** We adopt the positioning method based on ToA and DoA. Thus, the ToA and DoA signals between UE and each AN at every position of UE is recorded as the raw data for further experiments. The example of dataset is listed in Table 2. $t$ represents the time when UE moves along y-aix. $(ToA, DoA)$ is the time of arrival and direction of arrival between UE and each AN. $-$ means no signal collected when UE is out the coverage of AN. We suppose that each AN can only reach UE within a distance of 200m.

Our simulation data are collected by rounds. Each round includes 1641 items collected in a period of 82s with 0.05s sampling frequency when UE moves from the beginning to the end. Besides, to simulate the influence of channel noise, we also add random noise according to Gaussian distribution to the collected ToA and DoA signals. Without specification, we generate the random noise from Gaussian distribution with mean equals 0 and variable standard deviation.

**Evaluation Metrics** For the truth discovery module, Mean Square Error (MSE) is used as the evaluation metric to measure the positioning error according to the following formula.

$$MSE = \frac{1}{M}\sum_{m=1}^{M}(x_m - \bar{x_m})^2 + (y_m - \bar{y_m})^2$$

where, $(x_m, y_m)$ is the real position of UE and $(\bar{x_m}, \bar{y_m})$ is the estimated approximate position from truth discovery. $M$ is the total sampling number. A smaller MSE indicates a more accurate position estimation.

For the attack detection and tracing modules, we evaluate their performance with prediction accuracy, which is the percentage of true prediction to total instances. A higher accuracy indicates a better detection and tracing result.

### 5.3 Analysis of Truth Discovery

This part studies the performance of truth discovery under the effects of the interval distance of ANs and the number of involved ANs. We also compare the performance of different clustering methods. We ran the truth discovery module based on the experimental data generated through simulation and then compared estimated approximate positions with corresponding real positions. Mean square error (MSE) is used as the evaluation metric to measure positioning error. Table 1 lists the set of parameters involved in the experiments with the bold as their default values.

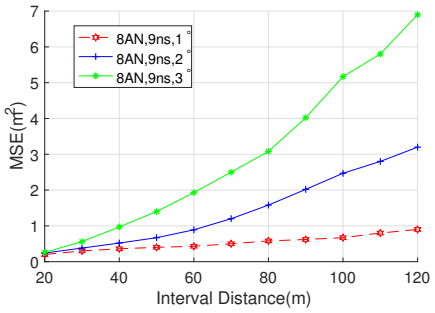


Fig. 4. Performance of truth discovery with varying interval distance

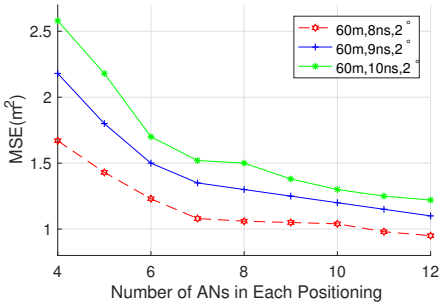


Fig. 5. Performance of truth discovery with varying number of ANs

#### 5.3.1 *Effect of Interval Distance*

Fig. 4 illustrates the performance of truth discovery with the interval distance varying from 20m to 120m under different DoA noise settings. As we can see from the figure, the positioning performance decreases with the increase of interval distance. This can be explained by the fact that the interval distance determines the density of ANs. A smaller interval distance indicates denser ANs and promises more available LoS signals, thus, the positioning accuracy can be well guaranteed under a small interval distance. However, on the other side, a dense distribution also incurs an increasing cost of fundamental equipment. A trade-off between density and positioning performance should be considered.

#### 5.3.2 *Effect of the Number of ANs Involved in Positioning*

Fig. 5 presents the positioning performance under a varying number of ANs. The performance presents an increasing tendency with more ANs included but remains steady after the number of AN reaches 8. The reason is that clustering-based positioning with multiple ANs improves accuracy by reducing the noise from each AN. However, when the number of AN is over 8, the included ANs may introduce additional noise other than reduce it as they are far from UE. Thus, the positioning accuracy can even drops.

#### 5.3.3 *Effect of Different Clustering Methods*

Additionally, we compare the positioning performance by applying different clustering methods. We focus on three most frequently used clustering methods: DBSCAN, K-means and C-means. Table 4 presents our results with

TABLE 3
Performance of multiple UEs

| Module | Performance |
|---|---|
| Truth Discovery | $1.2m^2$ (MSE) |
| Attack Detection | 86% (accuracy) |
| Attack Tracing | 82.5% (accuracy) |

TABLE 4
Performance of truth discovery with different clustering methods

| Clustering | Parameters | MSE ($m^2$) |
|---|---|---|
| DBSCAN | $\epsilon = 5.9, min = 2$ | 1.0 |
| K-Means | K=3 | 1.52 |
| C-Means | $C = 3$ | 1.29 |

parameter settings. The parameters are determined with experiences at the beginning of our experiments and we present herein the results with optimal parameter settings tested in our experiments. The other parameters are set to their defaults as shown in Table 1. We also inject a radio jamming attack to generate data by adding random noises. It is concluded from the table that DBSCAN shows the best performance with $\epsilon = 5.9, min = 2$ in terms of MSE.

Apart from MSE on average, the positioning detail is also recorded in Fig. 6. The X-axis represents time and Y-axis represents the positioning error at each time. The line $y = 1.0$ in the figure indicates the average MSE of DBSCAN. From the figure, we can see that though three methods both show a low positioning error most of the time, DBSCAN achieves the most robust performance in positioning accuracy when attacked. For K-Means and C-Means, the positioning error is unstable and can go over 7m sometimes, which is highly risky for users.

Based on the above experiment, we can conclude that DBSCAN not only shows good performance in general but also is the most robust algorithm under attacks since it can preserve positioning accuracy. Thus, DBSCAN based truth discovery is adopted to evaluate the performance of attack detection and tracing in the following experiments.

### 5.4 Performance of Attack Detection

#### 5.4.1 Data Generation

We simulate a radio jamming attack on UE by adding extra random noise to its positioning signals before they are sent to ANs. Since we assume that the attack capability is limited by 50%, the altered signals in each positioning should be less than half of the total. The attack is applied on and off randomly when UE moves along the y-axis. We repeat the simulation 10 rounds and split them into a training dataset (7 rounds) and a testing dataset (3 rounds). In data collection, ToA noise and DoA noise are also added to simulate a real communication channel. The UE attack detection model is learned from the training dataset and the performance is assessed based on the testing dataset.

#### 5.4.2 Analysis of Attack Detection

The experiment is conducted by testing performance with different combination of neural network factors. The setting of different neural networks and corresponding detection accuracy are listed in Table 5. As we can see, our scheme achieves the highest accuracy (99.40%) with a two-layer neural network and learning speed is 0.008. The results also provide us guidance in training the neural network: (1) the increase of neural units in its hidden layer can improve the accuracy, but should be controlled to avoid overfitting; (2) similarly, the increase of hidden layers can improve the accuracy, but should be controlled to avoid overfitting; (3) a slower learning speed implies a better prediction accuracy.

### 5.5 Performance of Attack Tracing

#### 5.5.1 Data Generation

We simulate a collusion attack on AN by adding extra random noise to its signals before they sent to the FC. Similarly, we repeat the simulation 10 rounds and split them into two parts: a training dataset (7 rounds) and a testing dataset (3 rounds). In each round, we randomly choose some ANs (less than 50%) as malicious attackers in advance. These ANs sent poisoned signals with a probability of 80%, while the others send normal signals. Note that the distribution of attacked ANs is changed in different rounds.

#### 5.5.2 Analysis of Attack Tracing

Attack tracing aims to find the source of an attack, i.e., the malicious ANs that provide erroneous positioning parameters in our case. The effectiveness of attack tracing is also measured by prediction accuracy. The setting of different neural networks and corresponding tracing accuracy are listed in Table 6. The best accuracy (98.24%) is achieved by a neural network with one hidden layer and 20 neural units at a learning rate of 0.004.

As a conclusion, we can see that owing to the limited number and effectiveness of extracted features, both attack detection and tracing can achieve high accuracy with very simple neural network models. At the same time, the simplicity of the adopted model makes it very practical for the ease of training and further deployment at the FC.

### 5.6 Performance of Multiple UEs

To test the performance of a complex scenario with multiple UEs, we deploy 10 UEs evenly on the lane and collected their data for test. We repeat the experiment for 10 times and take the average as the final result. The result of each module is presented in Table 3. As we can see, performance of each module decreased a bit but still acceptable. It shows that our scheme is applicable for supporting secure positioning for multiple UEs.

## 6 Conclusions

Concentrating on the positioning in 5G UDN, this paper spots its vulnerability under radio jamming attacks and collusion attacks. To mitigate the influence of these attacks, we proposed a scheme composed of three modules. In the process of positioning, the truth discovery module is firstly applied to effectively label 'Noise' signals tampered by attackers and then estimate the most approximate position based on "Non-Noise" signals. The attack detection module and the attack tracing module are two neural network

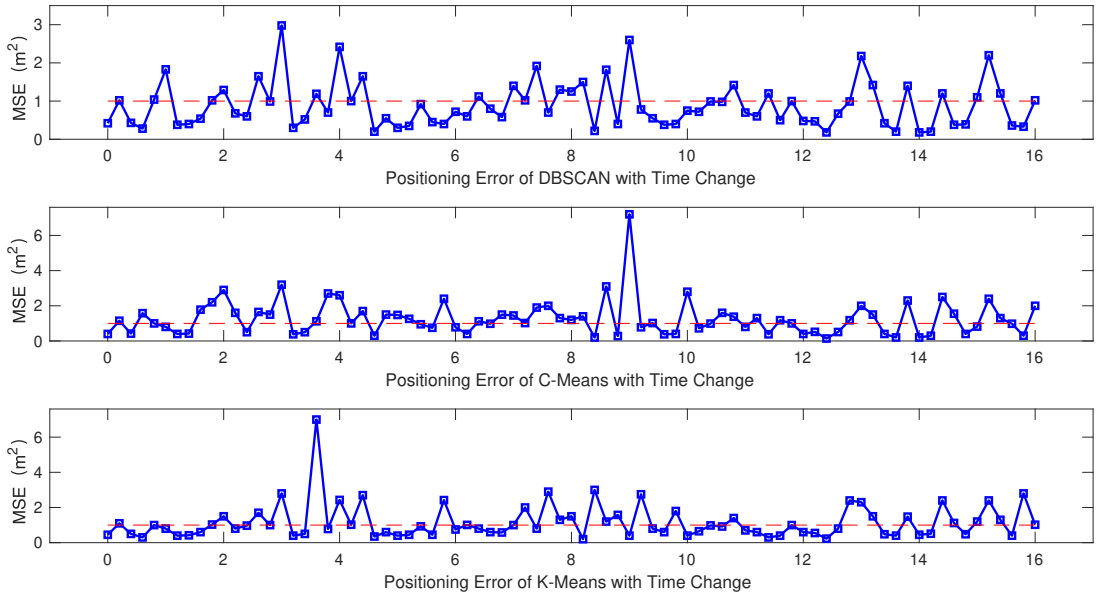


Fig. 6. Positioning error records of different clustering methods

TABLE 5
Performance of attack detection with different neural networks

| Experiment ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Hidden layer | 10 | 20 | 35 | $25+20$ | $10+10+10$ | $20+10+10$ | $25+20$ |
| Learning speed | 0.01 | 0.01 | 0.01 | 0.01 | 0.01 | 0.01 | 0.008 |
| Accuracy | 84.00% | 91.50% | 88.90% | 98.10% | 97.40% | 84.00% | 99.40% |

TABLE 6
Performance of AN based attack tracing with different neural networks

| Experiment ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Hidden layer | 10 | 15 | 20 | 25 | 30 | $10+20$ | $30+20$ | 20 |
| Learning speed | 0.01 | 0.01 | 0.01 | 0.01 | 0.01 | 0.01 | 0.01 | 0.004 |
| Accuracy | 65.00% | 84.71% | 92.35% | 87.94% | 86.47% | 86.18% | 64.71% | 98.24% |

models with the ability of finding which UE is under attacks and tracing the sources of attacks, i.e., the ANs that provide erroneous positioning parameters to FC. Extensive experiments based on simulation were conducted to verify the effectiveness of our proposed scheme.

## ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grant 62072351; in part by the Academy of Finland under Grant 308087 and Grant 335262; in part by the Shaanxi Innovation Team Project under Grant 2018TD-007; and in part by the 111 Project under Grant B16037, as well as Huawei Technologies Group Co., Ltd.

## REFERENCES

[1] N. Alliance, "5g white paper," *Next generation mobile networks, white paper*, vol. 1, 2015.

[2] E. S. Lohan, A. Alén-Savikko, L. Chen, K. Järvinen, H. Leppäkoski, H. Kuusniemi, and P. Korpisaari, "5g positioning: security and privacy aspects," *A Comprehensive Guide to 5G Security*, pp. 281–320, 2018.

[3] Y. Qi, H. Kobayashi, and H. Suda, "Analysis of wireless geolocation in a non-line-of-sight environment," *IEEE Transactions on wireless communications*, vol. 5, no. 3, pp. 672–681, 2006.

[4] A. Shahmansoori, G. E. Garcia, G. Destino, G. Seco-Granados, and H. Wymeersch, "5g position and orientation estimation through millimeter wave mimo," in *2015 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2015, pp. 1–6.

[5] I. Guvenc and C.-C. Chong, "A survey on toa based wireless localization and nlos mitigation techniques," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 3, pp. 107–124, 2009.

[6] E. Schubert, J. Sander, M. Ester, H. P. Kriegel, and X. Xu, "Dbscan revisited, revisited: why and how you should (still) use dbscan," *ACM Transactions on Database Systems (TODS)*, vol. 42, no. 3, pp. 1–21, 2017.

[7] J. del Peral-Rosado, G. Granados, R. Raulefs, E. Leitinger, S. Grebien, T. Wilding, D. Dardari, E. Lohan, H. Wymeersch, J. Floch *et al.*, "Whitepaper on new localization methods for 5g wireless systems and the internet-of-things," 2018.

[8] H. Liu, J. Yang, S. Sidhom, Y. Wang, Y. Chen, and F. Ye, "Accurate

wifi based localization for smartphones using peer assistance," *IEEE Transactions on Mobile Computing*, vol. 13, no. 10, pp. 2199–2214, 2013.
[9] E. Y. Menta, N. Malm, R. Jäntti, K. Ruttik, M. Costa, and K. Leppänen, "On the performance of aoa–based localization in 5g ultra–dense networks," *IEEE Access*, vol. 7, pp. 33 870–33 880, 2019.
[10] M. Koivisto, A. Hakkarainen, M. Costa, J. Talvitie, K. Heiska, K. Leppänen, and M. Valkama, "Continuous high-accuracy radio positioning of cars in ultra-dense 5g networks," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2017, pp. 115–120.
[11] J. Zhao, X. Fu, Z. Yang, and F. Xu, "Radar-assisted uav detection and identification based on 5g in the internet of things," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.
[12] K. Jansen, M. Schäfer, D. Moser, V. Lenders, C. Pöpper, and J. Schmitt, "Crowd-gps-sec: Leveraging crowdsourcing to detect and localize gps spoofing attacks," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 1018–1031.
[13] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of gps spoofing attacks on unmanned aerial systems," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2019, pp. 1–6.
[14] Q. Wang, Z. Lu, M. Gao, and G. Qu, "Edge computing based gps spoofing detection methods," in *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*. IEEE, 2018, pp. 1–5.
[15] M. Singh, P. Leu, A. Abdou, and S. Capkun, "Uwb-ed: distance enlargement attack detection in ultra-wideband," in *28th {USENIX} Security Symposium Security 19)*, 2019, pp. 73–88.
[16] A. S. Abdalla, K. Powell, V. Marojevic, and G. Geraci, "Uav-assisted attack prevention, detection, and recovery of 5g networks," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 40–47, 2020.
[17] A. Ometov, S. Bezzateev, V. Davydov, A. Shchesniak, P. Masek, E. S. Lohan, and Y. Koucheryavy, "Positioning information privacy in intelligent transportation systems: An overview and future perspective," *Sensors*, vol. 19, no. 7, p. 1603, 2019.
[18] W. Mohr, "5g empowering vertical industries," in *Tech. Rep.* 5G PPP, 2016.
[19] A. Dammann, R. Raulefs, and S. Zhang, "On prospects of positioning in 5g," in *2015 IEEE International Conference on Communication Workshop (ICCW)*. IEEE, 2015, pp. 1207–1213.
[20] V. Nurmela *et al.*, "Deliverable d1. 4 metis channel models," in *Proc. Mobile Wireless Commun. Enablers Inf. Soc.(METIS)*, 2015, p. 1.
[21] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, and H. Li, "Lsaa: A lightweight and secure access authentication scheme for both ues and mmtc devices in 5g networks," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5329–5344, 2020.
[22] I. Dokmanic, R. Parhizkar, J. Ranieri, and M. Vetterli, "Euclidean distance matrices: essential theory, algorithms, and applications," *IEEE Signal Processing Magazine*, vol. 32, no. 6, pp. 12–30, 2015.
[23] Q. Liu, R. Liu, Z. Wang, and Y. Zhang, "Simulation and analysis of device positioning in 5g ultra-dense network," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2019, pp. 1529–1533.

**Yilin Li** received the M.Eng. degree in information security from Xidian University, Xi'an China in 2020. His research interests are in privacy preservation, machine learning and VANET security and privacy.

**Shushu Liu** received the B.Sc. and M.Sc. degrees in computer science from Soochow University, Suzhou, China, in 2014 and 2017, respectively. She is currently pursuing the Ph.D. degree with the Department of Communication and Networking, Aalto University, Espoo, Finland. Her research interests are in social network, machine learning, and data security and privacy.

**Zheng Yan** received the B.Eng. degree in electrical engineering and the M.Eng. degree in computer science and engineering from the Xi'an Jiaotong University, Xi'an, China, in 1994 and 1997, respectively, the second M.Eng. degree in information security from the National University of Singapore, Singapore in 2000, and the Licentiate of Science and the Doctor of Science in Technology in electrical engineering from Helsinki University of Technology, Helsinki, Finland in 2005 and 2007. She is currently a professor at the Xidian University, Xi'an, China and a visiting professor at the Aalto University, Espoo, Finland. She authored about 300 peer-reviewed publications and solely authored two books. She is the inventor and co-inventor of 60+ patents and PCT patent applications. Her research interests are in trust, security and privacy, and data analytics. Prof. Yan served and is serving as an associate editor of IEEE Internet of Things Journal, IEEE Access Journal,Information Sciences, Information Fusion, JNCA, Security and Communication Networks, etc. She served as a steering, organization and program committee member for over 80 international conferences. She is a senior member of the IEEE.

**Robert H. Deng** is AXA Chair Professor of Cybersecurity, Director of the Secure Mobile Centre, and Deputy Dean for Faculty Research, School of Information Systems, Singapore Management University. He has been Professor of Information Systems at SMU since 2004. Prior to that, he was Principal Scientist and Manager of Infocomm Security Department, Institute for Infocomm Research, Singapore. Since April 2019, he has been Programme Director of the National Satellite of Excellence in Mobile Systems Security and Cloud Security, a five-year research initiative sponsored by NRF's National Cybersecurity RD programme. His research interests are in the areas of data security and privacy, cloud security, network and distributed systems security. He serves/served on many editorial boards and conference committees, including the editorial boards of ACM Transactions on Privacy and Security, IEEE Security and Privacy, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, Journal of Computer Science and Technology, and Steering Committee Chair of the ACM Asia Conference on Computer and Communications Security. He received the Outstanding University Researcher Award from National University of Singapore, Lee Kuan Yew Fellowship for Research Excellence from Singapore Management University, Asia-Pacific Information Security Leadership Achievements Community Service Star from International Information Systems Security Certification Consortium in 2010. He is a Fellow of IEEE and Fellow of Academy of Engineering Singapore.