Shooting to the Stars: Secure Location Verification via Meteor Burst Communications

Savio Sciancalepore*, Gabriele Oligeri, and Roberto Di Pietro*

*College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar

***Abstract*—We introduce *Shooting to the Stars*, in short *SttS*, a secure location verification algorithm leveraging Meteor Burst Communications (MBC)—the ephemeral, ionized stripe generated by meteors. *SttS* leverages intrinsic peculiarities of MBC, such as robustness to both eavesdropping and jamming, while also enjoying ease of deployment and secure authentication of the transmitting source. *SttS* enables the verification of the position of a passive receiver by exploiting the radio reflection properties of ephemeral meteor trails, combined with multiple anchors (N) that can be deployed even hundreds of Km from the receiver itself. We developed a complete theoretical model for our solution—rooted on sound literature and past experimental campaigns—, and fully tested it with extensive simulations. Results show that *SttS* is highly reliable in guaranteeing position verification, and that it can detect a location spoofing attack even when up to $\left(\lceil \frac{N}{2} \rceil - 1\right)$ anchors are compromised by an adversary. Finally, it is completely tunable, trading off accuracy with the number of observed trails—for instance, observing just 200 trails enables to correctly classify the the location as valid or not with a 0.99 probability.**

I. Introduction

Location verification is a challenging task in modern positioning systems. Indeed, given either an indoor or an outdoor positioning system, the adversary might exploit some security flaws of the system to let the user estimate the wrong position. This is particularly true for outdoor localization systems such as Global Positioning System (GPS) and GLObal NAvigation Satellite System (GLONASS), which have been proved to be not secure. In fact, such positioning systems are neither authenticated nor encrypted, and therefore an adversary can easily forge fake messages and force the user to estimate wrong positions [11][22].

Secure location verification aims at providing a security layer to verify the actual position of the user. During the years, several techniques have been developed to deal with this challenging task, either at the client or at the server side. The majority of the solutions mainly resort to information coming from other communications technologies (WiFi, LTE) to cross-check the consistency of the position [3][31]. Unfortunately, none of the above techniques is generally available in rural, desert, or harsh environments, where the station willing to verify its position does not have access to Internet and it is only able to receive the GPS/GLONASS signal. As an example, merchant ships are typical entities with very limited Internet access, where positioning and route computation are estimated only resorting to GPS/GLONASS infrastructure.

To provide a suitable and practical solution for these specific scenarios, this paper proposes a brand new secure location verification system exploiting Meteor Burst Communications (MBC). MBC use as media the ionized trails of meteors—this trail being a collateral effect of the meteors that, colliding with the earth's atmosphere, produce heat, light, and ionization streams. MBC have been already investigated as a communication medium [1][4][6][8][27]. Meteor trails randomly appear on the sky and disappear after few seconds, but still, they last long enough to reflect radio waves and enable the delivery of short messages to long distances. Moreover, MBC feature some intrinsic peculiarities that make them more secure with respect to other communication channels. Indeed, given the opportunistic nature of the channel, it is very difficult to both eavesdrop and jam the messages. Furthermore, MBC is simple to implement, inexpensive and highly reliable [26].

On the down side, MBC provides just low throughput as well as long waiting times. Indeed, given the short duration of the meteor trail and the link noise, the maximum throughput experienced by the link cannot exceed few thousands bits per second. In addition, not all the meteors are suitable for MBC. Small meteors (0.002 mm diameter) do not produce ionized trails, while larger meteors (8 cm diameter) are too rare to be practical for reliable communications. Thus, given a transmitter and a receiver, the communication link will be characterized by a random appearance time and a random duration.

The above considerations make the MBC link particularly suitable for location verification systems in difficult-to-reach scenarios. Firstly, location verification does not require high data rates—a few hundreds bits are sufficient to deliver the required information. Secondly, MBC is particularly suitable to deliver messages to medium/long range distances, i.e., hundreds or even thousands of kilometers. Lastly, since the trails that allow MBC cannot be predicted in advance, eavesdropping and denial of service attacks are more challenging to be performed.

In particular, robustness to denial of service attacks is a key feature of MBC. Indeed, assuming a receiver provided with an omni-directional antenna capable of receiving signals transmitted via an MBC link, jamming this link would be very difficult.

Personal copy of the authors - paper accepted version. Cite as: *S. Sciancalepore, G. Oligeri, R. Di Pietro, Shooting to the Stars: Secure Location Verification via Meteor Burst Communications, in Proc. of IEEE Conference on Communications and Network Security (CNS), Bejing, Jun., 2018.*

Indeed, the radio signal is reflected from a significant height and, for different links, their direction is practically random—being dependent on the orientation of the meteor trail. Even assuming the adversary knows the position of the receiver, given the above geometric characteristics of the link, jamming would be difficult to achieve: the adversary should deploy multiple ”aerial-jammers” around the receiver to prevent the message reception from all the possible directions—the ones generated by the trails.

Contribution. We propose Shooting to the Stars (in short, *SttS*), a location verification protocol exploiting MBC to securely verify the location of a node. *SttS* leverages an analytic framework to translate the received signal strength from a remote node (anchor) to its relative distance. Specifically, *SttS* is characterized by a distributed architecture consisting of multiple anchors helping a receiver node to verify its position. We have developed a complete and sound theoretical model showing how the receiver node can assess the trustworthiness of each link (receiver-to-anchor) and eventually verify its position by exploiting a consensus based approach. Finally, the results of our extensive simulations do prove the effectiveness and viability of our solution.

Organization. The paper is organized as follows. Section II presents the most important related work in the area of secure localization and meteor burst communications; Sec. III introduces the background and the communication model assumed in Meteor Burst Communications; Sec. IV discusses the system model assumed for this work; Sec. V discusses the techniques used to tune the unpredictable parameters in the model, while Sec. VI details the devised secure location verification scheme. Section VII introduces the adversary model and presents some attacks that could be performed over the system. Simulation results are provided in Sec. VIII, while Sec. IX tightens conclusions and draws future direction of our research activities.

II. Related work

In this section we recall the major contributions addressing the topics of secure location verification and meteor burst communications (MBC). To the best of our knowledge, there is no contribution so far exploiting MBC to implement secure location verification.

Secure localization. The localization problem mainly resorts to two family of solutions: *node centric*, where the localization algorithm is run by the node willing to estimate its position, and *infrastructure centric*, where the position of the node is estimated by the infrastructure and then subsequently transmitted to the node. In both of the above approaches, the node resorts to a set of *trusted anchors* for estimating the reciprocal distances. Unfortunately, given the distributed nature of the scenario—most of the time the anchors are unattended and easily accessible— an adversary can either compromise one or more existing anchor or deploy other malicious ones. Both secure localization and location verification received a lot of attention during the recent years [15]. Indeed, several protocols have been proposed to securely locate a device or verify its position.

A classical example is the *spoofing attack* [22][11] to the Global Positioning System (GPS), the most used and widely accepted localization system.

Another family of solutions proposes location based authentication by exploiting distance bounding protocols [12][5]. The main idea is to exploit the user (device) location to grant him (it) the access to restricted services.

Standard techniques resort to location verification by combining the difference between the propagation speeds of radio and sound waves. Authors in [31] proposed a technique based only on the broadcast nature of the radio signal emitted by the prover and the distributed topology of the network. The idea is to part the network nodes in two and detecting if the prover is either inside or outside the protected area. Authors in [33] focus on securing Mobile Location-based Services (MLBS), where services are provided by vendors to a customers based on their reciprocal proximity. To provide position verification, they propose a scheme called Key Distribution-based Position verification (KEPI), which takes advantage of an auxiliary network of transponders to facilitate trustworthy location-based services. Threats and solutions to location spoofing in vehicular ad-hoc networks are considered in [14]. Indeed, information such as position, direction, and speed, is often broadcast by vehicles so as to facilitate fast multi-hop propagation of possible alert messages. Unfortunately, a malicious vehicle can inject bogus information or cheat about its position. Authors in [24] explore the possibility to use the emerging drone technology to replace all the fixed anchors with a single drone that flies through a sequence of way-points. The main challenge consists on finding an optimal path to achieve the above goal. A time-based solution to spoofing attacks is proposed by [16] for the Automatic Dependent Surveillance - Broadcast (ADS-B) protocol. Authors developed a practical method that can reject virtually all spoofed ADS-B messages by monitoring the radio propagation time between senders and receivers.

Our contribution takes advantage of the previously developed techniques, e.g., distance bounding and estimation by exploiting received signal strength, to design a brand new solution exploiting MBC. Meteor bursts have been previously adopted for long-range communication [1][27][4] but, to the best of the authors' knowledge, our solution is the first to propose location verification exploiting distance estimation via MBC.

Meteor Burst Communications. Pioneering research activities on Meteor Burst Communications date back to the 1950s years. In that period, important work such as [7] and [28] dedicated many efforts in providing a precise physical model for Meteor Burst Propagation. Starting from these contributions, many refinements have been formulated. Some researchers focused on improving the throughput of an MBC link: [1] proposed a generalized propagation model valid both for underdense and overdense bursts, and investigated theoretical bit-per-burst performance bounds, while [2] presented experimental considerations on antennas and others design parameters, with emphasis on military systems. Also, [32] demonstrated the predictability of such a phenomena and the complex relationship between the arrival rate of usable meteors and antenna patterns, link parameters, Faraday rotation loss and polarization. A lot of research efforts have been spent in designing coding schemes that can improve the performance of an MBC link while not wasting power. Contributions such as [25], [21], delved into this research area, providing experimental results demonstrating the viability of their approaches. Research activities in these area are still ongoing, as demonstrated by the recent publication [18]. This work proposes an adaptive state reduction scheme, based on the slow-fading characteristic of the meteor burst channel, using a dimension-down per-survivor processing algorithm (ADPSP), characterized by an acceptable overhead. Another recent work [30] demonstrated for the first time the channel non-reciprocity in MBC links, especially when considering overdense meteor trails. Finally, we remark the recent work by Sulimov et al., [29], focusing on the possibility to realize probabilistic key agreement using MBC links.

III. Background and Communication Model

Meteors enter the earth atmosphere every day, burning up in the skies before landing. These meteors vary dramatically in size—ranging from a diameter of a few 0.002 mm to some 8 cm [4]. Even if up to a billion meteors enter the atmosphere on a daily basis, only a small part have the right speed, size, and trajectory (i.e., entry geometry) to be useful as a communication medium.

Specifically, MBC systems leverage the ionization effect of the trails of meteors to guarantee the propagation of radio signals. These trails are formed as the meteors ablate while entering the earth's upper atmosphere, in the region between 80 and 120 km altitude, and the ionization allows for the reflection of the signals back to the earth. Such an high altitude allows for great communication distances, up to 2000 km.

On the one hand, meteors can be either shower or sporadic, according to their periodicity. On the other hand, shower meteors can be further classified in underdense and overdense, according to their electron line density. Trails with an electron line density less than 10^{14} electrons/m are named *underdense*, otherwise they are *overdense*.

The discussion in the following, as in the wider part of the literature dealing with MBC systems, focuses on underdense trails, because they are characterized by a regular behaviour, hence resulting more usable for communication purposes. Even if overdense trails last for longer times than the underdense ones and can provide longer communication distances, they are very rare and exhibit quicker signal strength variations and undesired behaviors [27].

The signal reflected from an underdense trail generally rises up to a peak signal strength in a few hundred microseconds; than, it undergoes an exponential decay with a time constant dependent on the geometry of the link—from a few hundred milliseconds to a few seconds. The decay is due to the spreading and diffusion of the electrons forming the trail [21]. These phenomena are resumed by Eq. 1, considering a single link between a transmitter and a receiver and modeling the received signal strength in time [1]:

$$P_R(t) = P_0 \cdot e^{-\frac{2t}{t_c}}, \tag{1}$$

where t represents the time, P_0 is the received signal strength at $t = t_0$ and t_c is a time constant, i.e., the amount of time it takes to decay by a factor e^2 (8.7dB). More in detail, P_0 and t_c are defined according to Eq. 2 and Eq. 3.

$$\begin{aligned} P_0 &= P_T G R \frac{\delta_0}{16\pi^2} \frac{\sin^2(\alpha)}{1-\cos^2(\beta)\sin^2(\phi)} e^{-\frac{\delta_1}{\sec^2(\phi)}}, & (2) \\ t_c &= \delta_3 \sec^2(\phi), & (3) \end{aligned}$$

where:

- P_T is the transmitted power;
- G is the gain at both the transmitter and the receiver antennas;
- α denotes the angle between the electric field vector at the trail and the direction of the receiver. Usually, at the hot-spots, $sen(\alpha) = 1$.
- β is the angle between the principal axis to the trail and the plane of propagation;
- ϕ is the angle of incidence/reflection of the signal with the trail;
- δ_0, δ_1, δ_2 and δ_3 are physical parameters related to the phenomenon [27], i.e., electron line density, trail radius, electron radius and diffusion coefficient.

while R is a geometrical parameter yielding:

$$R = R_T R_R (R_T + R_R)$$

where R_T (R_R) is the distances between the meteor trail and the transmitter (receiver).

Without loss of generality, we assume the following relations [1]:

$$R_T \cong R_R = \left(\frac{L^2}{4} + \left(h + \frac{L^2}{8R_e} \right)^2 \right)^{1/2}, \tag{4}$$

$$sec(\phi)^2 = 1 + \frac{L^2}{\left(2h + \frac{L^2}{4Re}\right)^2}, \tag{5}$$

where L is the great-circle distance between the transmitter and the receiver, h is the trail altitude and R_e is the radius of the earth, commonly assumed as 6400 km.

IV. Scenario and system model

We consider the reference scenario depicted in Fig. 1.

Our network is constituted by a *receiver node* willing to verify its position and a set of $N \geq 3$ transmitting *anchors*. Moreover, both the receiver node and the anchors are aware of their own positions by resorting to the GPS infrastructure.

The receiver node does not perform any transmission, while the anchors are the only transmitting entities in the network.

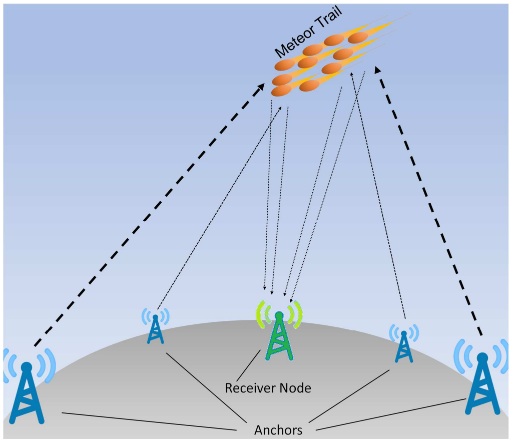

Fig. 1. Reference scenario.

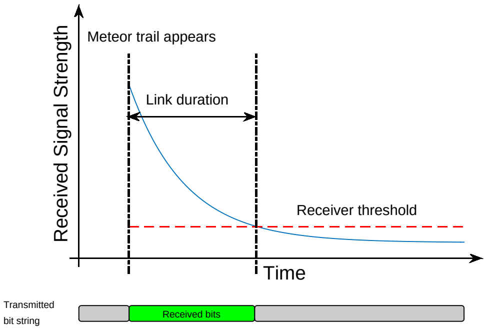

Fig. 2. Meteor burst link: creation and duration of the channel—qualitative representation.

Indeed, the anchors continuously transmit a sequence of 312 bits at a fixed data-rate. The message contains the position of the anchor, i.e., latitude and longitude coordinates, and some other information to enable the receiver to retrieve and verify the transmitted message (more details about the message structure are provided in Section VII-B). When a new trail appears, because of a meteor entering the earth atmosphere, the signal transmitted by the anchor(s) will be partially reflected and forwarded to the receiver, which in turn, will receive the messages. A qualitative description of the meteor burst link is shown in Fig. 2 . When the meteor enters the earth's atmosphere, the link between the anchor and the receiver is established with a certain received signal strength (blue solid line). Therefore, the transmitted bit stream (solid green box) is correctly delivered to the receiver (without loss of generality we do not take into account bits corruption). Finally, we also assume the meteor is colliding with the atmosphere at time $t = 0$. Recalling Eq. 1, we observe that the received signal strength (solid blue line) features a negative exponential decay. Therefore, after a certain amount of time, the receiver will be no more able to detect and receive the transmitted bits, i.e., when the received signal strength will be less than the receiver threshold sensitivity. This actually explains why, in our toy scenario, only a subset of the transmitted bits are received (green box). Indeed, the remaining bits get corrupted and cannot be retrieved by the receiver.

We do not assume any specific modulation scheme for our scenario. Legacy MBC systems use either Binary Phase Shift Keying (BPSK) or Minimum Shift Keying (MSK), while adding advanced error correction codes, such as Turbo Codes [9], can improve the Signal-to-Noise Ratio (SNR) and, consequently, provide more precise location estimates.

In all the simulations performed in this paper, we assume an i.i.d. error model with zero-mean and variance σ_e^2. This assumption is commonly assumed in practical deployments with homogeneous commercial-off-the-shelf (COTS) devices, where power measurement errors are typically limited by the ADC rate [27].

V. Tuning System Parameters

The *SttS* location verification algorithm we propose is based on mapping the received signal strength to a certain distance between the anchor and the receiver. Subsequently, the receiver verifies the previous computed distance with the one estimated from other sources, e.g., GPS/GLONASS. While translating the received signal strength to distance is a relatively easy task in several scenarios, i.e., LTE [23] and WiFi [19], it turns out to be a challenging task in MBC. Indeed, there is an unpredictable parameter associated to the geometry of the scenario that cannot be known in advance to the meteor trail formation. Recalling Eq. 2, we observe that the *meteor trail angle* (β) is a random variable, described in the next paragraph.

Meteor trail angle. The angle β between the meteor trail and the propagation plane between the anchor and the receiver significantly affects the receiver signal strength. This random angle depends on the relative positions of the anchor, the receiver, and the direction of the meteor trail. Since it cannot be predicted in advance, in the following we investigate how β affects the received signal strength as a function of the distance between the anchor and the receiver node.

In Fig. 3 we show how the received signal strength varies as a function of the term $\cos^2(beta)$ (recall Eq.2). Without loss of generality, we assumed a noiseless environment, an anchor-receiver distance spanning between 10 and 100 km, respectively, and finally a transmitter power of 4kW—consistently with other contributions in the literature [27], [10]. Moreover, Fig. 3 highlights that the impact of the angle β on the received signal strength is smaller for smaller distances, while it is higher when distances increase. Indeed, the received signal strength is almost constant and independent of $\cos^2(\beta)$ when the distance is equal to or less than 10 km, while it spans from about 1 to $1.3 \cdot 10^{-10}$ W when the distance is 100 km, experiencing a variation of about 30%.

A. Average waiting time

The average waiting time for a meteoric event enabling a link between a transmitter and the receiver can be computed

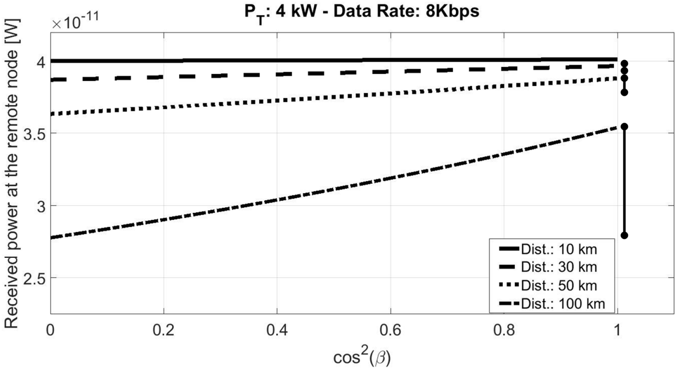

Fig. 3. Impact of the term $cos^2(\beta)$ on the received signal strength as a function of various distances.

according to [27]. The *reference link* method is used to estimate the number of available meteor trails per hour M as follows:

$$M = \left(M_T \cdot \left(\frac{PF}{PF_T} \right)^{1/2} \cdot \left(\frac{f_T}{f} \right)^{3/2} \right) /5.5, \qquad (6)$$

where $M_T = 60$ is the meteor rate per hour of another reference system characterized by an operating frequency of $f_T = 47$ MHz and a power factor $PF_T = 180$ dB, while $f = 48$ MHz represents the system operating frequency and PF represents the new power factor. We remark that the system power factor can be computed as follows:

$$PF = P_T + G_T + G_R - N, \qquad (7)$$

where $P_T = 4$ kW is the transmission power, $G_T = 12$ dBm and $G_R = 12$ dBm are the antenna gains at both the transmitter and the receiver sides, and finally, $N = -116$ dBm is the median level of the noise.

By substituting our values, it turns out an average number of meteors per hour equal to $M = 276.09$, meaning an average waiting time of 13.04 seconds to establish a link between an anchor and a receiver.

VI. Secure Distance Verification

In this section, we show how to leverage the received signal strength associated to the anchors' beacons to verify the actual distance between the receiver and the anchors.

Recalling Eq. 1 and given the considerations discussed in Sec. V, the receiver can verify its distance to the anchors by verifying that the received signal strength associated to the beacons belongs to a pre-determined interval. In the following, we determine the lower and upper bound of such an interval and we provide the algorithm to verify the distance to the anchor.

Lower bound. The received signal strength $P_R(t)$ experienced by the receiver cannot be less than the lower bound $P_R^m(t)$, i.e., $P_R(t) > P_R^m(t)$, where $P_R^m(t) = P_R(\cos^2(\beta) = 0)$. Therefore, we assume the lower bound will be experienced when there will be the minimum value for the $\cos^2(\beta)$, i.e., 0.

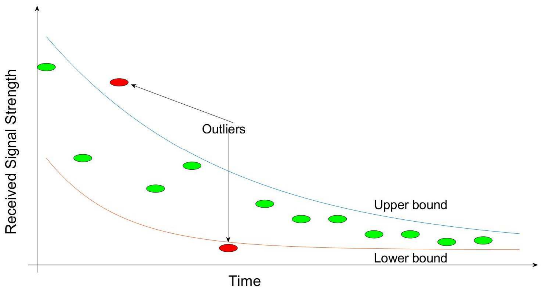

Fig. 4. Verification of the Received Signal Strengths (RSS): our algorithm classifies each RSS sample as either legitimate or outlier—qualitative description.

Upper bound. The received signal strength $P_R(t)$ experienced by the receiver cannot be greater than the upper bound $P_R^M(t)$, i.e., $P_R(t) < P_R^M(t)$, where $P_R^M(t) = P_R(\cos^2(\beta) = 1)$. Indeed, we assume that the upper bound will be experienced when the term $\cos^2(\beta)$ will have the maximum possible value (1). Moreover, we observe that the upper bound is also affected by noise. In fact, assuming that the noise follows a log-normal distribution as stated in [27], each sample of the received power will be affected by a positive power contribution. We take into account the random contribution of the noise by performing a statistical estimation of its maximum value, to be summed up to the maximum received signal strength. In our simulations, we considered the 90-percentile associated to the statistical distribution of the noise power.

Legitimate power interval. In Fig. 4 we show a qualitative example of the *SttS* scheme when a set of beacons are received by the receiver and the associated received signal strengths have been estimated. Our proposed algorithm computes the lower and the upper bounds for each received sample, i.e., red and blue solid line, respectively. Then, each estimated received signal strength is classified as legitimate when it belongs to the interval, while it is classified as an outlier if it lays outside of the interval.

The details of the *SttS* scheme are depicted by Algorithm 1. When a new meteor trail appears, the receiver starts to receive packets from an anchor and it logs the related received signal strength values. We assume M packets (Received Signal Strength (RSS) values) are received (estimated) by the receiver. As stated before, the receiver computes a legitimate power interval for each RSS in the batch. We also assume the receiver is aware of the distance to the anchor and the data rate at which the anchor is transmitting. Note that distance information can also be embedded by the anchor in the message, and therefore retrieved by the receiver during the communication process—this could be useful when new anchors are deployed at run time. Finally, the receiver counts how many estimated RSS values are within the legitimate interval. Eventually the receiver declares the current position of the anchor as *trusted* if the number of legitimate RSS values is the majority of the batch ($i > M/2$), *untrusted* otherwise. In this way, the receiver will be able to spot if the anchor maliciously manipulates the transmitted power to induce a false modification in the receiver

Algorithm 1: Pseudo-code of *SttS*.

```
Input: $M_i$ Packets received from each anchor i (i $\in \{1, \ldots, N\}$).
$counter$ = 0;
for $i$=1:N do
    Compute $P^m_{R_i}(t)$, the minimum receivable power from anchor i;
    Compute $P^M_{R_i}(t)$, the maximum receivable power from anchor i;
    $counter_m$ = 0;
    for m=1:M do
        if $P_{R_i}(t) > P^m_{R_i}(t)$ and $P_{R_i}(t) < P^M_{R_i}(t)$ then
            $counter_m$ = $counter_m$ + 1;
        end
    end
    if $counter_m < M/2$ then
        Untrusted Link $i$, $counter$ = $counter$ + 1;
    else
        Trusted Link $i$;
    end
end
if $counter < N/2$ then
    Output: 0, Location Confirmed;
else
    Output: 1, Location Not Confirmed;
end
```

position.

As said above, we do not assume that packets can be lost—ranging from the loss of few packets to a whole subset of anchors stop functioning. While these assumptions could not seem realistic, it is easy to accommodate them with slight modifications to Algorithm 1; however, due to space constraints, we leave these modifications and related analysis and discussion, for future work. A major threat, as per our adversary model (cfr. Sec. VII-A), is that a compromised anchor might change both the transmitting power and its GPS coordinates consistently; but, in the remaining of the paper, we will show how *SttS* is robust to such an attack.

The above considerations apply for each anchor in the network scenario. Indeed, given the assumption that all the anchors are always transmitting beacon messages, the receiver will opportunistically receive them from different anchors as a function of the position of the meteor trail formation. Indeed, in order to establish a communication link, we recall that the meteor trail should appear in the middle of the scene at the same distance from the receiver and the sender (Eq. 4), as previously assumed by other authors [27]. Now, given the randomness of the meteor trail formation, the receiver will periodically verify its position from all the anchors by exploiting our proposed algorithm.

VII. Secure Location Verification

In this section, we combine the secure distance verification performed by multiple anchors to propose a secure location verification protocol. We first introduce the adversary model, and subsequently we consider the security mechanisms to make the protocol robust to the attacks.

A. Adversary Model

We consider a very powerful adversary able to spoof the GPS/GLONASS signal and also to either compromising already existing anchors or deploying new ones. We envisage a two-stage attack: firstly, the adversary broadcasts fake GPS messages to the receiver, advertising a position different from the real one: this is, indeed, a GPS spoofing attack. Secondly, the adversary wants the receiver to verify the spoofed location and it acts as follows:

- **Malicious anchors deployment.** The adversary can deploy its own malicious anchors in our scenario. Such anchors can be set in place before, during, or after our network deployment. The malicious anchors want to prevent the location verification of the receiver by sending fake information to the receiver itself. In order to achieve the above goal, the anchors might modulate the transmitting power and changing their GPS coordinates (embedded in the beacons) accordingly.
- **Tampering existing anchors.** The adversary is able to tamper a subset of the anchors deployed in the network scenario. The adversary will be therefore able to disclose all the secrets inside the anchor and to use them to inject fake data into the location verification process run by the receiver. To maximize its effectiveness, the adversary maliciously modulates the transmission power of the anchors, simulating a different distance from the target node, thus inducing it not to verify its position.

B. Securing the Location Verification

We assume all the anchors embed the following information in each beacon message they transmit:

- Preamble [24 bits]
- GPS Coordinates [64 bits].
- Sequence number [16 bits].
- Message signature[192 bits].
- Erasure codes [16 bits]

The receiver will check both the integrity and authenticity of the message by verifying the message signature. We assume all the anchors are equipped with a private-public key pair, signed by the system Certification Authority (CA). We suggest to adopt ECDSA-192 for signing the messages. Indeed, given its short size and limited computational costs, it enables to verify the sender of the packets with a negligible overhead [17]. Therefore, when a new message is received and its signature is evaluated as not trusted, the message is discarded. Moreover, a sequence number is embedded in the message to prevent the message reply attack. The *SttS* secure location verification scheme is a multiple rounds protocol: one round per anchor. As depicted in Fig. 5, the receiver establishes a link for each anchor when the meteor trail appears. At each round, the receiver verifies the consistency of the received GPS/GLONASS coordinates from the anchor with the estimated distance exploiting the received signal strength. If the majority of the anchors are trusted, the receiver will be able to verify its position.

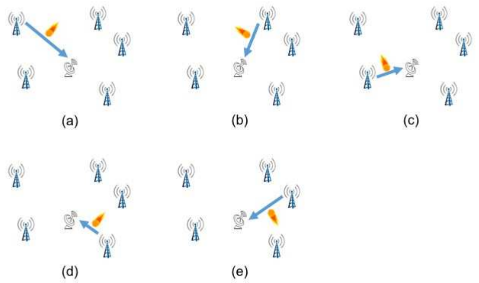

Fig. 5. Network scenario: 5 anchors and 1 receiver. A link is established when a new meteor trail appears in the middle between the communicating parties. The receiver takes a sequence of beacon messages and checks if the received signal strength is consistent with the GPS/GLONASS coordinates embedded in the messages.

Join and leave of anchors. *SttS* supports dynamic join and leave of anchors. Indeed, anchors enabling secure localization in a certain area might fail due to either malicious or non malicious causes, and need to be replaced. We envisage a different behaviour (*set-up*) of the anchor just after its deployment. During the set-up phase, the anchor broadcasts its public key certificate—signed by the CA, whose public key is also stored on the receiver—allowing the receiver to receive, verify, and store the new anchor public key. After the set-up, the anchor will start the standard broadcast procedure depicted in Section VII-B. Conversely, the leave of an anchor is not affecting the network, since the receiver will keep using the public keys of the transmitting anchors.

VIII. Simulation Analysis and Discussion

In this section we provide the results of an extensive simulation campaign aimed at investigating the performance of *SttS*, while varying different system parameters. We also demonstrate how our solution is robust against the adversarial model introduced in Sec. VII-A.

A. Scenario setup

We fully implemented our solution in the Matlab© environment. Our simulation scenario is constituted by 20 anchors deployed over an area of $11.570km^2$ (coincidental with the Qatar peninsula), while the receiver has been located at the HBKU Research Complex building in Doha, within the convex hull of the region delimited by the anchors. In Fig. 6 we show the topology of the considered scenario. We fixed the beacon data rate for the anchors to $8kb/s$ and we deployed a total of 20 anchors at 5 different distances from the remote node, which are 5, 10, 30, 50 and 100 kilometers, respectively. Finally, we observe that, for each trail, the receiver is able to perform a number of RSS estimations between 39 and 50 when the anchor-receiver distance spans between 5Km and 100Km, respectively (see Tab. I). The above estimation can be done by recalling Fig. 2 and computing the number of packets delivered within the trail (green box in Fig. 2). The number of RSS estimations is $t_c * br$, where br is the bit-rate (8 kb/s) and t_c is the time constant introduced by Eq. 3. We recall that the value of the time constant depends on the anchor-receiver distance: specifically, it spans between 39.8 ms and 50.7 ms, for a receiver-anchor distance between 5 km and 100 km, respectively.

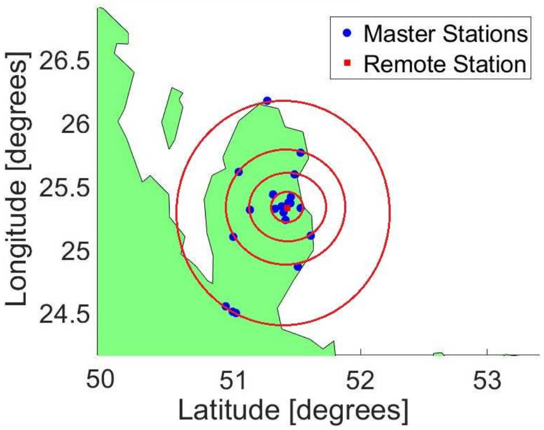

Fig. 6. Topology used for the simulation analysis.

TABLE I
Number of RSS samples per trail as a function of the receiver-anchor distance.

Distance (Km)	RSS Samples per Trail
5	39
10	39
30	40
50	42
100	50

B. Benign scenario

In order to verify the effectiveness of our location verification algorithm, we first investigate its performance in a benign scenario, i.e., without the attacker.

Figure 7 shows the false positive attack detection probability assuming the transmission power P_T takes on the values in the range $\{1, \ldots, 20\}$ kW. We consider a transmission bit-rate equal to 8 kb/s and a noise model suitable for the rural environment (-111dBm) [27].

We observe that our solution is significantly affected by the transmitting power of the anchors; indeed, when the trans-

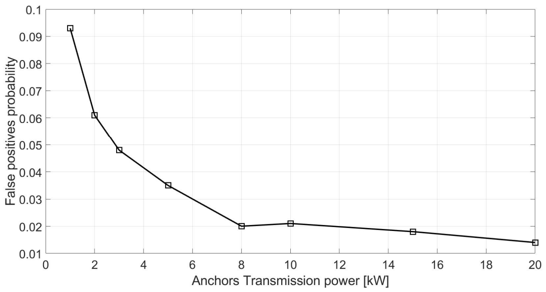

Fig. 7. False positive attack detection with a data rate of 8 kb/s (-111dBm) and different transmission powers.

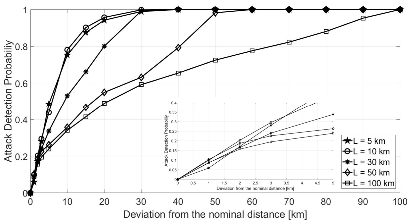

Fig. 8. Attack detection rate while varying the distance advertised by the anchor from its nominal position.

mitting power increases, the received signal strength is less prone to fluctuations and therefore it falls (with a high level of assurance) within the legitimate power interval (recall Sec. VI), yielding a low probability of false positive.

As a rule of thumb, we highlight that the proposed location verification algorithm is able to successfully confirm the location of the receiver node until the noise level is less than the power of the received signal from a given anchor. When the noise level rises up and becomes closer to the signal level, the percentage of false detection increases. In this case, either the transmission power or the bit-rate must be tuned accordingly in order to reach the desired value of false detection rate.

C. Scenario with malicious anchors

We now consider the adversarial behaviour introduced in Sec. VII-A. In particular, we investigate the *sensitivity* of the *SttS* scheme to a single anchor advertising a distance different from the reality by modulating the transmitting power in a malicious way.

Figure 8 shows the attack detection rate as a function of the anchors' displacement. The simulations have been performed by assuming a transmission power of 4 kW and a data-rate of 8 kb/s with a link noise level of -111 dBm. Each sample represents the median of 300 simulations. The choice to have a transmission power of 4 kW (instead of higher and more favorable values) has been performed in order to investigate the performance of *SttS* in a conservative scenario.

We can observe that the anchors closer to the receiver node are easier to be detected when they change their transmission power. In fact, we can detect a deviation of 3 Km (generated by properly tuning the transmitted power) for an anchor located 5 km far away from the receiver in the 69% of the cases, while the attack detection probability decreases to 32.5% when the same deviation is applied to an anchor located 30Km far away from the receiver node.

Cluster of malicious anchors. Let us consider an adversary able to both spoof the GPS/GLONASS signal and compromise a subset of the deployed anchors. Figure 9 depicts the considered scenario constituted by a receiver located at the coordinate (x, y) computed from a legitimate GPS/GLONASS infrastructure. We assume the adversary is able to perform a GPS spoofing attack [13] and to change the position measured by the receiver to (x', y'). Moreover, we assume the adversary is able to compromise a subset of the anchors, e.g., 3 out of 7 in Fig. 9. The anchors in the malicious cluster $3, 4, 6$ collaborate to confirm the receiver's position at (x', y') and preventing the actual location verification of the receiver.

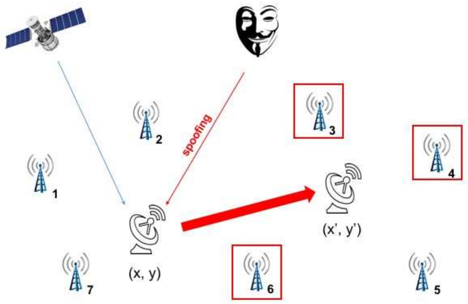

Fig. 9. The adversary spoofs the GPS/GLONASS signal and compromises the anchors $\{3, 4, 6\}$. The receiver is able to detect such a behaviour by receiving trusted information from anchors $\{1, 2, 5, 7\}$, leveraging majority voting.

Conversely, the receiver will run our secure location verification algorithm. Now, the receiver is assuming its new position as (x', y') while anchors 3, 4, and 6 will confirm such a position by sending beacon messages properly forged, i.e., with fake anchors coordinates and consistent transmission powers. *SttS* will be still able to spot the attack. Indeed, 4 out of 7 anchors, i.e., $\{1, 2, 5, 7\}$ will keep broadcasting authentic information, i.e., their real GPS/GLONASS coordinates and consistent transmission powers. Therefore, assuming that the majority of the deployed anchors is not-compromised, *SttS* guarantees the secure location verification of the receiver node.

D. Strengthening accuracy - Amplification

The approach discussed in previous sections becomes very effective when analyzing multiple consecutive trails. Indeed, we can dramatically improve accuracy in declaring a violation in location verification leveraging known results related to the concentration of measure.

Let x_i be the random variable that takes on the output of Algorithm 1 and assumes the value 0 when the location is not verified, 1 otherwise. Then, let $X = \sum_n x_i$ be the random variable counting the number of times the location is verified over a batch of n trails. Since the trails are independent, we can assume the x_i to be i.i.d random variable, where p is the probability of an attack detection event. Hence, the random variable X obeys to a binomial distribution. By looking at N consecutive trails, according to the Chernoff inequality for the binomial distribution [20]:

$$P\left(X \leq (1-\gamma)\,\mu\right) \leq e^{-\frac{\mu \cdot \gamma^2}{2}}, \tag{8}$$

where μ is the mean of the distribution and γ is a deviation factor from the mean.

For a given assumed value for γ, it is possible to compute the Chernoff bound for false positives and obtain the probability to observe a given number of attacks. This let us obtain the error probability in a taking a decision, given the number of observed trails.

Assuming a false positive rate of 0.03 (obtained with a transmission power of 4 kW and a bitrate of 8 kbps, as depicted

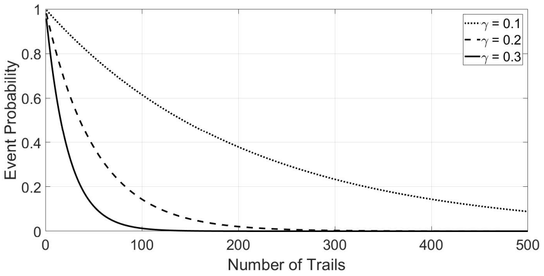

Fig. 10. Chernoff bound on False Positives assuming different values of γ.

in Fig. 7), Fig. 10 shows the probability of false positive events that exceed $\gamma * 0.03$, while increasing the value of γ.

As expected, results demonstrate that the accuracy in taking a decision about the presence of a spoofing attack strictly depends on the number of observed trails. For instance, with 100 trails, the probability to have a number of valid location verification lower than 20% with respect to the expected value is less than 0.178; this value decreases to around 0.01 with just 200 trails. These probabilities being the assurance of a false positive—that we can reject, declaring a true positive (i.e., a location spoofing attack) with probabilities 0.822 and 0.99 respectively.

IX. Conclusions and Future Work

In this paper we have introduced *SttS*, a new secure location verification protocol that exploits Meteor Burst Communications (MBC). For instance, *SttS* can be used to verify the coordinates received from other positioning systems such as GPS or GLONASS. Based on past experimental campaign and sound scientific results, we provided a thorough analysis of the proposed solution. Moreover, we have fully implemented *SttS* and proved its effectiveness as a location verification solution. *SttS* also enjoys a couple of relevant properties: it is resilient to an active adversary able to compromise any non-majority subset of the existing anchors; and, it is completely tunable—trading off accuracy in attack detection with the number of observed trails.

Ongoing work include an experimental verification of our findings in the Qatari desert.

References

[1] M. Abel. Meteor Burst Communications: Bits per Burst Performance Bounds. *IEEE Trans. on Commun.*, 34(9):927–936, Sep. 1986.

[2] D. Brown. A Physical Meteor-Burst Propagation Model and Some Significant Results for Communication System Design. *IEEE Journal on Sel. Areas in Commun.*, 3(5):745–755, Sep. 1985.

[3] J. T. Chiang, J. J. Haas, and J. C. et al. Secure Location Verification Using Simultaneous Multilateration. *IEEE Trans. on Wirel. Commun.*, 11(2):584–591, Feb. 2012.

[4] B. C. Cumberland, J. S. Valacich, and L. M. Jessup. Understanding Meteor Burst Communications Technologies. *Commun. ACM*, 47(1):89–92, Jan. 2004.

[5] D. E. Denning and P. F. MacDoran. Location-based authentication: Grounding cyberspace for better security. *Computer Fraud & Security*, 1996(2):12 – 16, 1996.

[6] T. Ericson and J. Zander. Meteor burst communication without feedback. *IEEE Trans. on Commun.*, 43(2/3/4):851–857, Feb. 1995.

[7] V. R. Eshleman and L. A. Manning. Radio Communication by Scattering from Meteoric Ionization. *Proceedings of the IRE*, 42(3):530–536, Mar. 1954.

[8] A. Fukuda and al. Experiments on meteor burst communications in the antarctic. *Advanced Polar Upper Atmosphere Research*, 17:120–136, 2003.

[9] K. Gracie and M. H. Hamon. Turbo and Turbo-Like Codes: Principles and Applications in Telecommunications. *Proceedings of the IEEE*, 95(6):1228–1254, Jun. 2007.

[10] J. Hackworth. Meteor Burst Communication Study. Report a228641, DSTO Australia, Jul. 1990.

[11] Z. Haider and S. Khalid. Survey on effective GPS spoofing countermeasures. In *Int. Conf. on Innovative Comput. Tech.*, pages 573–577, Aug. 2016.

[12] J. Hightower and G. Borriello. Location Systems for Ubiquitous Computing. *Computer*, 34(8):57–66, Aug. 2001.

[13] R. T. Ioannides, T. Pany, and G. Gibbons. Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. *Proceedings of the IEEE*, 104(6):1174–1194, Jun. 2016.

[14] W. B. Jaballah, M. Conti, and M. M. et al. Secure Verification of Location Claims on a Vehicular Safety Application. In *Int. Conf. on Comput. Commun. and Netw.*, pages 1–7, Jul. 2013.

[15] C. Javali, G. Revadigar, K. B. Rasmussen, and et al. I Am Alice, I Was in Wonderland: Secure Location Proof Generation and Verification Protocol. In *Conf. on Local Comput. Netw.*, pages 477–485, Nov 2016.

[16] Y. Kim, J. Y. Jo, and S. Lee. A secure location verification method for ADS-B. In *Digital Avionics Systems Conf.*, pages 1–10, Sep. 2016.

[17] M. Knežević, V. Nikov, and P. Rombouts. Low-Latency ECDSA Signature Verification - A Road Toward Safer Traffic. *IEEE Trans. on Very Large Scale Integr. Syst.*, 24(11):3257–3267, Nov. 2016.

[18] Z. Li, F. Zhou, X. Chen, Y. Li, and F. Gao. An Adaptive State Assignment Mechanism Based on Joint Data Detection and Channel Estimation on Fading Meteor Channel. *IEEE Trans. on Veh. Technol.*, 66(6):4627–4635, Jun. 2017.

[19] H. Liu, J. Yang, and S. S. et al. Accurate WiFi Based Localization for Smartphones Using Peer Assistance. *IEEE Trans. on Mob. Comput.*, 13(10):2199–2214, Oct. 2014.

[20] M. Mitzenmacher and E. Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005.

[21] K. Mukumoto, S. Nagata, and T. W. et al. Proposal of Go-Back-i-symbol ARQ Scheme and its Performance Evaluation in Meteor Burst Communications. *IEEE Transac. on Commun.*, 60(8):2336–2343, Aug. 2012.

[22] G. Panice, S. Luongo, and G. G. et al. A SVM-based detection approach for GPS spoofing attacks to UAV. In *Int. Conf. on Automation and Comput.*, pages 1–11, Sep. 2017.

[23] G. Pecoraro, S. D. Domenico, and E. C. et al. LTE signal fingerprinting localization based on CSI. In *IEEE Int. Conf. on Wirel. and Mob. Comput., Netw. and Commun.*, pages 1–8, Oct. 2017.

[24] P. Perazzo, F. B. Sorbelli, M. Conti, G. Dini, and C. M. Pinotti. Drone path planning for secure positioning and secure position verification. *IEEE Transactions on Mobile Computing*, 16(9):2478–2493, Sept 2017.

[25] M. Pursley and S. Sandberg. Variable-rate coding for meteor-burst communications. *IEEE Trans. on Commun.*, 37(11):1105–1112, Nov. 1989.

[26] RTL-SDR.com. Meteor detection with the RTL-SDR. https://www.rtl-sdr.com/meteor-detection-rtl-sdr/, 2014. [Online accessed 12-12-2017].

[27] J. Schanker. *Meteor Burst Communications*. Artech House, 1990.

[28] G. R. Sugar. Radio propagation by reflection from meteor trails. *Proceedings of the IEEE*, 52(2):116–136, Feb. 1964.

[29] A. I. Sulimov and A. V. Karpov. Performance evaluation of Meteor Key Distribution. In *Int. Conf. on e-Business and Telecommun.*, volume 4, pages 392–397, Jul. 2015.

[30] A. I. Sulimov, A. V. Karpov, and I. R. L. et al. Analysis and Simulation of Channel Nonreciprocity in Meteor-Burst Communications. *IEEE Trans. on Antennas and Propagation*, 65(4):2009–2019, Apr. 2017.

[31] A. Vora and M. Nesterenko. Secure Location Verification Using Radio Broadcast. *IEEE Trans. on Depend. and Sec. Comput.*, 3(4):377–385, Oct. 2006.

[32] J. A. Weitzen. Predicting the arrival of meteors useful for meteor burst communication. *Radio Science*, 21(06):1009–1020, Nov. 1986.

[33] J. Yang, Y. Chen, and S. M. et al. Securing Mobile Location-based Services through position verification leveraging key distribution. In *IEEE Wirel. Commun. and Netw. Conf.*, pages 2694–2699, Apr. 2012.