Localization Security in Wireless Sensor Networks as a Non-cooperative Game

Nicola Gatti
Politecnico di Milano, DEI
P.za L. da Vinci 32, I–20133 Milan, Italy
Email: ngatti@elet.polimi.it

Mattia Monga
Università degli Studi di Milano, DICo
Via Comelico 39, I–20135 Milan, Italy
Email: mattia.monga@unimi.it

Sabrina Sicari
Università dell'Insubria, DICOM
Via Mazzini 5, I–21100 Varese, Italy
Email: sabrina.sicari@uninsubria.it

***Abstract*—Wireless Sensor Networks (WSN) support data collection and distributed data processing by means of very small sensing devices that are easy to tamper and cloning: therefore classical security solutions based on access control and strong authentication are difficult to deploy. In this paper we look at the problem of assessing security of node localization. In particular, we analyze the scenario in which Verifiable Multilateration is used to localize nodes and a malicious node try to masquerade as non-malicious. We resort to non-cooperative game theory and we model this scenario as a two-player game. We analyze the optimal players' strategy and we show that the Verifiable Multilateration is indeed a proper mechanism able to reduce the profitability of fake positions. Our analysis demonstrates that, when the verifiers play a pure strategy, the malicious node can always masquerade as unknown with a probability of one and the induced deception could be not negligible. Instead, when the verifiers play mixed strategies, the malicious node can masquerade as unknown with a very low probability and the expected deception is virtually negligible.**

I. Introduction

Wireless Sensor Networks (WSN) [1], [2] technologies support data collection and distributed data processing by means of very small sensing devices. Sensors are increasingly used in many contexts such as surveillance systems, systems supporting traffic monitoring and control in urban/suburban areas, military and/or anti-terrorism operations, telemedicine, assistance to disabled and elderly people, environmental monitoring, localization of services and users, and industrial process control. This activities rely greatly on data about the positions of sensor nodes, not necessarily know at design time. In fact, nodes are often deployed randomly or move, and one of the challenges is getting localization data at time of operations. Several localization approaches have been proposed (for example, [3], [4], [5], [6], [7], [8], [9], [10], [11]), but most of them omit to consider that WSNs could be deployed in an adversarial setting, where hostile nodes under the control of an attacker coexist with faithful ones. In fact, wireless communications are easy to tamper and nodes are prone to physical attacks and cloning: thus classical solutions, based on access control and strong authentication, are difficult to deploy.

An approach to localize nodes even when some of them are compromised was proposed in [12] and it is known as *Verifiable Multilateration* (VM). However, in some situations also using Verifiable Multilateration the security localization behavior of a node is undefined, in other words there is not enough information for establishing with certainty whether it is a trusty or a malicious node. This weakness could be exploited by a malicious node to masquerade as an undefined one, pretending to be in a position that is still compatible with all verifiers' information. To the best of our knowledge, the analysis of this scenario has not been explored so far in the literature: we explicitly consider how a malicious node, on the one side, could act and, on the other side, how the system could face it. This constitutes the original contribution of our work.

In this paper, we resort to non-cooperative game theory to study our scenario. More precisely, we model it as a two-player strategic-form game, where the first player is a *verifier* that uses VM and the second player is a *malicious node*. The verifier acts to securely localize the malicious node, while the malicious node acts to masquerade as undefined. As is customary in game theory, the players are considered rational (*i.e.,* maximizers). This amounts to say that the malicious node is modeled as the strongest adversary. We study the game, showing some results concerning the robustness of VM. The paper is organized as follows: Section II provides a short overview about Verifiable Multilateration; Section III shortly describes secure localization game, providing some basic concepts; Section IV introduces strategic game analysis. Section V draws some conclusions and provides hints for future works.

II. Verifiable Multilateration

Multilateration is a technique used in WSNs to estimate the coordinates of some unknown nodes, given the positions of other given landmark nodes, called *anchor* nodes, whose positions are already known. The position of an unknown node U is computed by geometric inference based on the distances between the anchor nodes and the node itself. However, the distances are not measured directly; instead, they are derived by knowing the speed of the signal in the medium used in the transmission, and by measuring the time needed to get the answers to a beacon message sent to U.

Unfortunately, if this computation is carried on without any precaution, U might fool the anchors by delaying the

978-1-4244-7286-4/10/$26.00 © 2010 IEEE

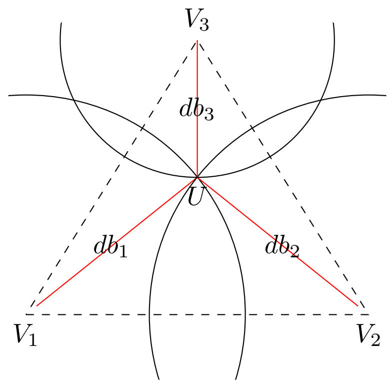


Fig. 1. Verifiable multilateration

beacon message. However, since a malicious node can delay the answer beacon, but not speed it up, under some conditions it is possible to spot malicious behaviors. VM uses three or more anchor nodes to detect misbehaving nodes. In VM the anchor nodes work as *verifiers* of the localization data and they send to a sink node B the pieces of information needed to evaluate the consistency of the coordinates computed for U. The basic idea of VM is shown in Figure 1: each verifier V_i computes its *distance bound* [13] to U; any point $P \neq U$ inside the triangle formed by V_1, V_2, V_3 has necessarily at least one of the distance to the V_i enlarged. This enlargement, however, cannot be masked by U by sending a faster message to the corresponding verifier.

Under the hypothesis that verifiers are trusted and they can securely communicate with B, the following verification process can be used to check the localization data:

1) Each verifier V_i sends a beacon message to U and records the time τ_i needed to get an answer;
2) Each verifier V_i (whose coordinates $\langle x_i, y_i \rangle$ are known) sends to B a message with its τ_i;
3) From τ_i, B derives the corresponding distance bound db_i (which can be easily computed if the speed of the signal is known) and it estimates U's coordinates by minimizing the sum of squared errors
$$\epsilon = \sum_i (db_i - \sqrt{(x - x_i)^2 + (y - y_i)^2})^2$$
where $\langle x, y \rangle$ are the (unknown) coordinates to be estimated[1];
4) B can now check if $\langle x, y \rangle$ are feasible in the given setting by two incremental tests: (a) *δ-test:* For all verifiers V_i, compute the distance between the estimated U and V_i: if it differs from the measured distance bound by more than the expected distance measurement error, the estimation is affected by malicious tampering; (b) *Point in the triangle test:* Distance bounds are reliable only if the estimated U is within at least one verification triangle formed by a triplet of verifiers, otherwise the estimation is considered unverified.

[1]In an ideal situation where there are no measurement errors and/or malicious delays this is equivalent to finding the (unique) intersection of the circles defined by the distance bounds and centered in the V_i (see Figure 1) and $\epsilon = 0$.

If both the δ and the *point-in-the-triangle* tests are positive, the distance bounds are consistent with the estimated node position, which moreover falls in at least one verification triangle. This means that none of the distance bounds were enlarged. Thus, the sink can consider the estimated position of the node as ROBUST; else, the information at hands is not sufficient to support the reliability of the data. An estimation that does not pass the δ test is considered as MALICIOUS. In all the other cases, the sink marks the estimation as UNKNOWN. In an ideal situation where there are no measurement errors, there are neither malevolent nodes marked as ROBUST, nor benevolent ones marked as MALICIOUS. Even in this ideal setting, however, there are UNKNOWN nodes, that could be malevolent or not. In other words, for UNKNOWN nodes there is not enough information for evaluating the trustworthiness of node position. In fact, U could pretend, by an opportune manipulation of delays, to be in a position P that is credible enough to be taken into account. No such points exist inside the triangles formed by the verifiers (this is exactly the idea behind verifiable multilateration), but outside them some regions are still compatible with all the information verifiers have.

Consider N verifiers that are able to send signals in a range R. Let x_0 and y_0 the *real* coordinates of U. They are unknown to the verifiers, but nevertheless they put a constraint on plausible fake positions, since the forged distance bound to V_i must be greater than the length of $\overline{UV_i}$ since delays have to be positive.

Thus, any point $P = \langle x, y \rangle$ that is a plausible falsification of U has to agree to the following constraints, for each $1 \leq i \leq N$:

$$\begin{cases} (y - y_i)^2 + (x - x_i)^2 < R^2 \\ (y - y_i)^2 + (x - x_i)^2 > (y_0 - y_i)^2 + (x_0 - x_i)^2 \end{cases} \tag{1}$$

The constraints in (1) can be understood better by looking at Figure 2, where three verifiers are depicted: the green area around each verifier denotes its power range, and the red area is the bound on the distance that U can put forward credibly. Thus, any plausible P must lay outside every red region and inside every green one.

III. SECURE LOCALIZATION GAME

Our aim is the study of the behavior of a possible malicious node that acts to masquerade itself as an unknown node and, at the same time, how the verifiers can face the malicious node at best. This is a typical non-cooperative setting that can be analyzed by leveraging on game theoretical models. A *game* is described by a couple: *mechanism* and *strategies*. The mechanism defines the rules of the game in terms of number of players and actions available to the players. The strategies describe the behaviors of the players during the game in terms of played actions. Strategies can be pure,

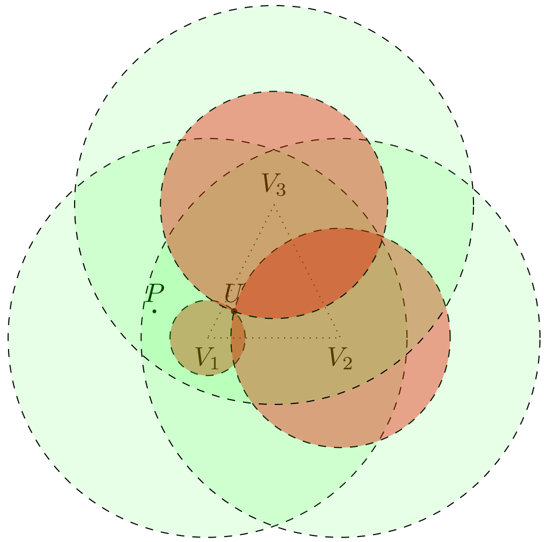


Fig. 2. Plausible falsification region: P is a plausible fake position for U since lays outside every red region and inside every green one (and it is outside the triangle of verifiers).

when a player acts one action with a probability of one, or they can be mixed, when a player randomizes over a set of actions. The players' strategies define an outcome (if the strategies are pure) or a randomization over the outcomes (if mixed). Players have preferences over the outcomes expressed by utility functions and each player is *rational*, acting to maximize its own utility. Solving a game means to find a profile of strategies (*i.e.,* a set specifying one strategy for each player) such that the players' strategies are somehow in equilibrium. The most known equilibrium concept is *Nash* where each player cannot improve its own utility by deviating unilaterally (a detailed treatment of Nash equilibrium can be found in [14]): a fundamental result in the study of equilibria is that every game admits at least one Nash equilibrium in mixed strategies, while a pure strategy equilibrium might not exist.

We now formally state our secure localization game, by focusing on a setting with $N = 3$ verifiers (the minimum number needed to apply VM). A *secure localization game* is a tuple $\langle Q, A, u\rangle$. Set Q contains the players and is defined as $Q = \{\mathbf{v}, \mathbf{m}\}$ ($\mathbf{v}$ denotes the verifiers and $\mathbf{m}$ denotes the malicious node). Set A contains the players actions. More precisely, given a surface $S \subseteq \mathbb{R}^2$, the actions available to $\mathbf{v}$ are all the possible tuples of positions $\langle V_1, V_2, V_3\rangle$ of the three verifiers with $V_1, V_2, V_3 \in S$, while the actions available to $\mathbf{m}$ are all the possible couples of positions $\langle U, P\rangle$ with $U, P \in S$ (where U and P are defined in the previous section). We denote by $\sigma_{\mathbf{v}}$ the strategy (possibly mixed) of $\mathbf{v}$ and by $\sigma_{\mathbf{m}}$ the strategy (possibly mixed) of $\mathbf{m}$. Given a strategy profile $\sigma = (\sigma_{\mathbf{v}}, \sigma_{\mathbf{m}})$ in pure strategy, it is possible to check whether or not constraints (1) are satisfied. The outcomes of the game can be $\{\text{MALICIOUS}, \text{ROBUST}, \text{UNKNOWN}\}$. Set u contains the players' utility functions, denoted $u_{\mathbf{v}}(\cdot)$ and $u_{\mathbf{m}}(\cdot)$ respectively, that define their preferences over the outcomes. We define $u_i(\text{MALICIOUS}) = u_i(\text{ROBUST}) = 0$ for $i \in \{\mathbf{v}, \mathbf{m}\}$, while $u_i(\text{UNKNOWN})$ can be defined differently according to different criteria. A simple criterion could be to assign $u_{\mathbf{v}}(\text{UNKNOWN}) = -1$ and $u_{\mathbf{m}}(\text{UNKNOWN}) = 1$. However, our intuition is that the UNKNOWN outcomes are not the same for the players, because $\mathbf{m}$ could prefer those in which the distance between U and P is maximum. In particular we propose three main criteria to characterize UNKNOWN outcomes:

1) *maximum deception*, $u_{\mathbf{m}}$ is defined as the distance between U and P, while $u_{\mathbf{v}}$ is defined as the opposite;
2) *deception area*, $u_{\mathbf{m}}$ is defined as the size of the region $S' \subseteq S$ such that $P \in S'$ is marked as UNKNOWN, while $u_{\mathbf{v}}$ is defined as the opposite;
3) *deception shape*, $u_{\mathbf{m}}$ is defined as the number of disconnected regions $S' \subseteq S$ such that $P \in S'$ is marked as UNKNOWN, while $u_{\mathbf{v}}$ is defined as the opposite.

Players could even use different criteria, *e.g.,* $\mathbf{v}$ and $\mathbf{m}$ could adopt the maximum deception criterion and the deception shape respectively. However, when players adopt the same criterion, the game is *zero-sum*, the sum of the players' utilities being zero. This class of games is easy and has the property that the maxmin, minmax, and Nash strategies are the same. In this case calculations are simplified by the property that $u_{\mathbf{v}} = -u_{\mathbf{m}}$; in the following we shall adopt this assumption.

IV. Game Analysis

For the sake of simplicity, we focus on the case in which both players adopt the maximum deception criterion. In principle, however, our analysis can be extended to other criteria: in particular, Theorem 4.1 is valid for all the proposed criteria.

A. Analysis with Pure Strategies

In this section, we show that there can be no equilibrium in pure strategies. We discuss also what is the value of the maximum deception when the verifiers adopts a pure strategy. We consider only the case in which $\forall i, j\, \overline{V_iV_j} \leq R$ since otherwise the region in which VM would be applicable is small and no UNKNOWN positions would be possible, thus paradoxically the verifiers would have an incentive to reduce it further to only one point, making the localization procedure worthless.

At first, we can show that for each action of the verifiers, there exists an action of the malicious node such that this is marked as UNKNOWN.

Theorem 4.1: For each tuple $\langle V_1, V_2, V_3\rangle$ such that $\overline{V_iV_j} \leq R$ for all i, j, there exists at least a couple $\langle U, P\rangle$ such that $u_{\mathbf{m}} > 0$.

Proof. Given V_1, V_2, V_3 such that $\overline{V_iV_j} \leq R$ for all i, j, choose a V_i and call X the point on the line $\overline{V_kV_j}$ ($k, j \neq i$) closest to V_i (see Figure 3). Assign $U = X$. Consider the line connecting V_i to X, assign P to be any point X' on this line such that $\overline{V_iX} \leq \overline{V_iX'} \leq R$. Then, by construction $u_{\mathbf{m}} > 0$. □

We discuss what is the configuration of the three verifiers, such that the maximal deception is minimized.

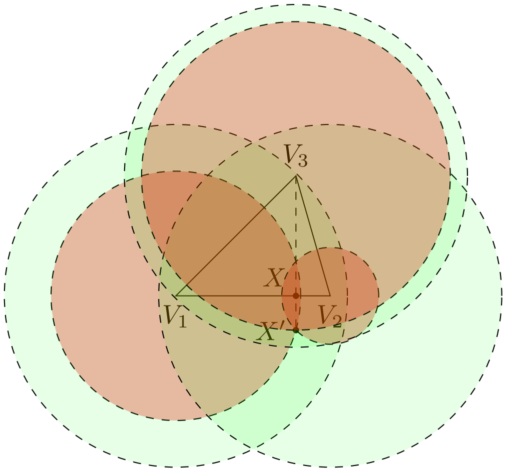


Fig. 3. Construction of plausible positions X'

Theorem 4.2: Any tuple $\langle V_1, V_2, V_3 \rangle$ such that $\overline{V_iV_j} = R$ for all i, j minimizes the maximum deception.

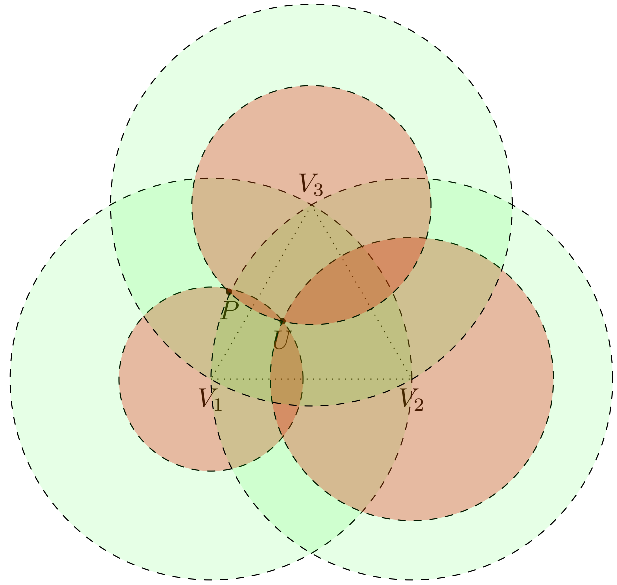
Proof. Since we need to minimize the maximum distance between two points, by symmetry, the triangle whose vertexes are V_1, V_2, V_3 must have all the edges with the same length. We show that $\overline{V_iV_j} = R$. It can easily seen, by geometric construction, that U must be necessarily inside the triangle. As shown in Section 2, P must be necessarily outside the triangle and, by definition, the optimal P will be on the boundary constituted by some circle with center in a V_i and range equal to R (otherwise P could be moved farther and P would not be optimal). As $\overline{V_iV_j}$ decreases, the size of the triangle reduces, while the boundary keeps to be the same, and therefore $\overline{UP}$ does not decrease. $\square$

We are now in the position to find the maxmin value (in pure strategies) of the verifiers, *i.e.,* the action that maximizes the verifiers' utility given that the malicious node will minimize it. The problem of finding the maxmin strategy can be formulated as the following non-linear optimization problem:

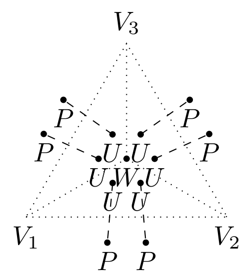
$$\max_{\text{constraints (1)}} \overline{UP} \qquad \begin{array}{c} \text{for some } V_1, V_2, V_3 \text{ with} \\ \overline{V_iV_j} = R \text{ for all } i, j \end{array}$$

We solved this problem by using conjugated subgradients. We report the solution. Called W the orthocenter of the triangle, U and P can be easily expressed with polar coordinates with origin in W. We assume that $\theta = 0$ corresponds to a line connecting W to a V_i. We have, $U = (\rho = 0.1394R, \theta = \frac{\pi}{6})$ and $P = (\rho = 0.4286R, \theta = \frac{\pi}{6} + 0.2952)$, and, for symmetry, $U = (\rho = 0.1394R, \theta = -\frac{\pi}{6})$ and $P = (\rho = 0.4286R, \theta = -\frac{\pi}{6} - 0.2952)$. Therefore, there are six optimal couples $\langle U, P \rangle$s. In Figure 4 depicts the malicious node's best action, by showing on the right all the symmetrical positions. The value of $u_{\mathbf{m}}$ (*i.e.,* the maximum deception) is $0.2516R$. In other words, when the verifiers compose an equilateral triangle, a malicious node can masquerade as unknown and the maximum deception is about 25% of the verifiers' range R.

We consider the verifiers' strategy and we show that for



(a)



(b)

Fig. 4. Malicious node's best responses (maximum deception is $\overline{UP} = 0.2516R$).

each action of the malicious node they can find an action such that the malicious node is marked either as ROBUST or as MALICIOUS.

Theorem 4.3: For each couple $\langle U, P \rangle$, there exists at least a tuple $\langle V_1, V_2, V_3 \rangle$ such that $u_{\mathbf{v}} = 0$.

Proof. If $U \equiv W$ (where W is the orthocenter of the equilateral triangle composed by the verifiers), then, by geometric construction, maximum deception is zero (see Figure 5). $\square$

By combining Theorems 4.1 and 4.3, we have that our game cannot admit any Nash equilibrium in pure strategies. Indeed, for each $\sigma_{\mathbf{v}}$ there exists a best response $\sigma_{\mathbf{m}}$ such that $\sigma_{\mathbf{v}}$ is not the best response to $\sigma_{\mathbf{m}}$.

B. Discrete Approximation Hardness

Finding a mixed strategy equilibrium in a two-player zero-sum finite game is well known to be a polynomial problem in the number of actions available to the players. This is because the problem of finding a minmax strategy can be formulated as a linear mathematical programming problem. However, our problem is not finite, V_1, V_2, V_3, U, P belonging to a continuous space. In this section, we show that finding an approximate solution by discretizing the surface S in a finite number of points is not practically affordable.

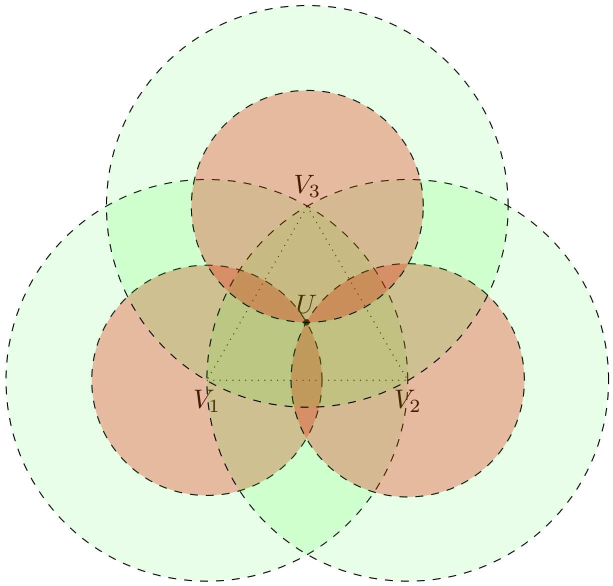


Fig. 5. The only plausible $P \equiv U$ when $U \equiv W$

We discretize S by a finite grid with a given step Δ. We call $S_d \subset S$ the set of points in the grid. The players can choose their position from set S_d. We denote by $A_{\mathbf{v}}$ and $A_{\mathbf{m}}$ the set of actions of the verifiers and malicious node respectively. Supposed S_d to be a square and called l the length of S, the number of points in S_d is $|S_d| = \lceil \frac{l}{\Delta} \rceil^2$. We have that $|A_{\mathbf{v}}| = \sum_{3 \leq i \leq |V|} \binom{|S_d|^2}{i} \sim O(|S_d|^6)$ and $|A_{\mathbf{m}}| = |S_d|^2 \cdot (|S_d|^2 - 1) \sim O(|S_d|^4)$. For each possible profile of players' actions we compute $u_{\mathbf{m}}$ as the maximum deception. Notice that the number of all the possible profiles of players' actions is $\sim O(|S_d|^{10})$. We denote by $p_{\mathbf{v}}(i)$ the probability with which $\mathbf{v}$ plays action $i \in A_{\mathbf{v}}$. The linear programming formulation to find the minmax strategy (and equivalently the Nash equilibrium) is:

$$\min u \tag{2}$$

$$\sum_{i \in A_{\mathbf{v}}} p_{\mathbf{u}}(i) u_{\mathbf{m}}(j,i) \leq u \quad \forall j \in A_{\mathbf{m}} \tag{3}$$

$$p_{\mathbf{u}}(i) \geq 0 \quad \forall i \in A_{\mathbf{v}} \tag{4}$$

$$\sum_{i \in A_{\mathbf{v}}} p_{\mathbf{u}}(i) = 1 \tag{5}$$

Constraints (3) force the expected utility $\mathbf{m}$ receives from taking action j to be not larger than u; constraints (4) and (5) grant probabilities $p_{\mathbf{m}}(\cdot)$ to be well defined. The objective function is the minimization of u that by constraints (3) is the maximal expected utility of $\mathbf{m}$.

We solved the above mathematical programming problem with grids with $3, 4, 5$ points per edge. In all these case studies, the verifiers always mark the malicious node as robust or malicious, and therefore $u_{\mathbf{m}}$ is always equal to zero. We notice that the utility matrix presents a number of non-null values, anyway, there exists at least a configuration of verifiers such that for no action of the malicious node this is marked as unknown. This is because the grid is too loose. However, with a larger number of points per edge, the problem is not computationally affordable because the number of outcomes is excessively large.

C. Mixed Strategies with a Fixed Orthocenter

The hardness result discussed in the previous section pushed us to resort to an analytical approach to find the players' equilibrium strategies. Here, we discuss the strategies in a simplified case study. The idea is that this result can provide insight to solve the general case.

At first we show that any equilibrium strategy prescribes that the players randomize over a continuous space of action. Call $supp(\sigma_i)$ the set of actions played with strictly positive probability by player i in σ_i.

Theorem 4.4: In the secure localization game, no equilibrium strategy $\sigma = (\sigma_{\mathbf{v}}, \sigma_{\mathbf{m}})$ can have $|supp(\sigma_i)| \in \mathbb{N}$ (*i.e.,* $supp(\sigma_i)$ is a continuous space).

Proof. A necessary and sufficient condition such that a game with continuous actions admits an equilibrium where players randomize over a finite number of actions is that the continuous variables in the players' utility functions are separable, *i.e.,* the utility functions can be expressed as the product of terms composed of only sum of variables. This does not hold in our case. □

We consider the situation in which the orthocenter W of the triangle constituted of the three verifiers is a given data. By Theorem 4.2, we know that the optimal verifiers' configuration is the equilateral triangle with edge's length equal to R. Consider the polar coordinate system with pole in the orthocenter W. Call α the angle between the polar axis and the line connecting a vertex V_i to W. Since the verifiers must form an equilateral triangle and the verifiers have distance equal to R from the pole, the verifiers' strategy can be compactly represented as a probability density over α. Instead, the malicious node's strategy can be represented as a probability density over U and P. We can show that the players' equilibrium strategies are the following.

Theorem 4.5: The players' equilibrium strategies are:

$$\sigma_{\mathbf{v}}^* = \alpha \text{ uniformly drawn from } [0, \frac{2\pi}{3}]$$

$$\sigma_{\mathbf{m}}^* = \begin{cases} U & \begin{cases} \rho_U = & 0.1394R \\ \theta_U = & \text{uniformly drawn from } [0, 2\pi] \end{cases} \\ P & \begin{cases} \rho_P = & 0.4286R \\ \theta_P = & \theta_U + 0.2952 \end{cases} \end{cases}$$

and the expected utility of the malicious node is $0.001R$.

Proof. By Theorem 4.4, the players must randomize over a continuous space of actions. We consider the verifiers' strategy. Easily, for symmetry reasons, the verifiers must randomize uniformly over all the possible values of α. In particular, we can safely limit the randomization over $[0, 2/3\pi]$. We consider the malicious node's strategy. For symmetry, it randomize such that θ_u is uniformly drawn from $[0, 2\pi]$. In order to compute the optimal ρ_U and the polar coordinates of P, we solve the following optimization problem. We fix a value for θ_u and we search for the values of ρ_U, ρ_P, θ_P such that the malicious node's expected utility is the maximum one.

$$\max_{\rho_U, \rho_P, \theta_P} \int_0^{\frac{2\pi}{3}} \frac{u_{\mathbf{m}}}{\frac{2\pi}{3}} d\alpha \tag{6}$$

The above optimization problem is non-linear. We solved it by discretizing the value of α with a step of 10^{-3} and by using conjugated subgradients. The result is the strategy reported above. □

Notice that, the expected utility of the malicious node drastically decreases with respect to the situation in which the strategy of the verifiers is pure, as it is $0.001R$ with mixed strategy vs. $0.25R$ with pure strategies. This is because with mixed strategies, the probability that the malicious node is not marked as robust or malicious is very small. Therefore, randomization over their strategies aids the verifiers to increase their expected utility and VM with mixed strategies can be considered to be robust.

V. Conclusion

The assessment of the trustworthiness of wireless sensor node localization information is a fundamental challenge in order to provide further trust to applications and data. Verifiable Multilateration is a secure localization algorithm that defines two tests for evaluating node behavior as malicious, robust or — as a ultimate choice — as unknown. In case of unknown nodes, VM does not have enough information for evaluating the trustworthiness of the node. This lack of information may be exploited by a malicious user. In this paper we modeled VM has as a strategic non-cooperative game, on order to study the overall equilibrium properties of the system. We considered a verifier player against a malicious node and we analyzed the behavior in case of the adoption of both pure strategies and a mixed ones. The conducted analysis demonstrates that, when the verifiers play a pure strategy, the malicious node can always masquerade as unknown with a probability of one and the induced deception could be not negligible. Instead, when the verifiers play mixed strategies, the malicious node can masquerade as unknown with a very low probability and the expected deception is virtually negligible.

Acknowledgment

This research has been partially funded by the European Commission, Programme IDEAS-ERC, Project 227977-SMScom.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on wireless sensor network," *IEEE Wireless Communications*, vol. 40, no. 8, pp. 102 – 114, 2002.

[2] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y.-F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and zigbee standards," *Computer Communications*, vol. 30, no. 7, pp. 1655–1695, 2007.

[3] N. Bulusu, J. Heidemann, and D. Estrin, "Gps-less low-cost outdoor localization for very small devices," *IEEE Personal Communications*, vol. 7, no. 5, pp. 28–34, 2000.

[4] S. Čapkun, M. Hamdi, and J.-P. Hubaux, "Gps-free positioning in mobile ad-hoc networks," *Cluster Computing*, vol. 5, no. 2, pp. 157–167, 2002.

[5] J. Chen, K. Yao, and R. Hudson, "Source localization and beamforming," *IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 30–39, 2002.

[6] L. Doherty, K. Pister, and L. E. Ghaoui, "Convex position estimation in wireless sensor networks," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, 2001.

[7] T.He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MOBICOM)*, 2003.

[8] D. Niculescu and B. Nath, "Ad-hoc positioning system," in *Proceedings of the IEEE Global Communication Conference (GLOBECOM)*, 2001.

[9] V. Ramadurai and M. Sichitiu, "Localization in wireless sensor networks: A probabilistic approach," in *Proceedings of the International Conference on Wireless Networks (ICWN)*, 2003.

[10] A. Savvides, H. Park, and M. Srivastava, "The bits and flops of the n-hop multilateration primitive for node localization problems," in *Proceedings of the ACM International Workshop on Wireless Sensor Networks and Application (WSNA)*, 2002.

[11] B. H. Cheng, L. Vandenberghe, and K. Yao, "Distributed algorithm for node localization in wireless ad-hoc networks," *ACM Trans. Sen. Netw.*, vol. 6, no. 1, pp. 1–20, 2009.

[12] S. Čapkun and J. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[13] S. Brands and D. Chaum, "Distance-bounding protocols," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT)*, 1994.

[14] M. Osborne and A. Rubinstein, *A course in game theory*. MIT Press, 1994.