SecAT-Dist: A Novel Secure AT-Dist Localization Scheme for Wireless Sensor Networks

Amal Abdelkarim*, Abderrahim Benslimane*, Issam Mabrouki† and Abdelfettah Belghith*
*HANA Research Group, University of Manouba, Tunisia
Email: amal.abdelkarim@hanalab.org, issam.mrabrouki@hanalab.org, abdelfattah.belghith@ensi.rnu.tn
†LIA/CERI, University of Avignon, Agroparc BP 1228, 84911 Avignon, France
Email: abderrahim.benslimane@univ-avignon.fr

***Abstract*—In the last few years, the localization issue in wireless sensor networks has gained a lot of popularity for providing flexible and novel location-aware applications. However, throughout the variety of research works in this topic, most interests focused purely on the localization scheme itself rather than the security issue of the localization. In this paper, we propose a new and original secure version of AT-Dist, a distance-based multihop localization algorithm previously explored but under a non-adversarial environment. This version, called SecAT-Dist, proposes a lightweight security scheme that combines RC4-based hash function and symmetric encryption system to enable sensor nodes to authenticate received beacon location information and protects hop-count information from being arbitrary or selfishly changed. Furthermore, we introduce a trust model based on a set of confidence index taking benefits from specific characteristics of distance-based multihop localization algorithms. Analytically, we show that the number of trust anchors, among the total number including malicious anchors, is reduced. Simulation results show that our security scheme is more resistant to external attacks and allows great number of nodes to be located with accuracy.**

***Index Terms*—WSN, Localization, Security**

I. Introduction

Wireless sensor networks (WSN) are formed by a large number of small, simple, battery-operated and resource-constrained nodes. WSNs have a wide range of applications including civilian and military operations such as target tracking and battlefield surveillance. For many applications, sensors' *locations* play a crucial role to accomplish their tasks. Such a requirement arises for example in geographical routing, network security and energy efficient management. However, due to the cost reasons, it is not practical to have a GPS receiver on every sensor node. Faced to this challenge, several localization algorithms for WSN have been proposed [5], [2].

Despite the substantial advances in this issue, many proposed localization algorithms in WSN suffer from the lack of a global vision where localization and security are *jointly* addressed. This stems from the fact that WSN are generally deployed in unattended and even hostile environments, thereby exposing the localization process to many attacks making the estimated locations incorrect. In order to defend against location attacks, some secure localization schemes have been recently proposed, among which are location verification, distance verification, or distance-bounding to name a few.

Throughout the variety of existing security schemes, no matter how they are designed to operate, we observe that they aim to achieve one or more of the following tasks: preventing, detecting, diagnosing, and isolating malicious attacks. These operations could enable the achievement of good results, but that could compromise other issues such as simplicity and energy efficiency. In the contrary, one of the recent approach is to *tolerate* the presence of malicious node instead of eliminating or detecting them while minimizing their impact on the localization process. Although such an approach can be acceptable for applications that do not require too stringent location accuracy, the number of tolerated malicious anchors in distance-based localization algorithms should be *limited* to guarantee a bounded localization error for all cases. Indeed, for distance-based localization algorithms family the authors in [1] derived an upper bound k_{max} on the number of malicious anchors k, that may be involved in localizing the target while still not being able to undermine its accurate localization. If n stands for the total number of anchors, then $k_{max} = \frac{n-3}{2}$. Moreover, when this condition holds, to be located with a bounded error a target requires at least $k+3$ anchors among them there are at least three honest anchors. This condition is referred to as the "$k+3$" *condition*.

Motivated by the previous research work, we develop in this paper a *secure extension* framework for AT-Dist [5], a well-known based-distance multihop localization algorithm but where the security issue has been mostly overlooked. To this end, we propose two techniques that represent our main contributions. In the first one, we give some prevention-oriented security features for AT-Dist based on *encryption* and *authentication* operations. Our second technique, which tolerates the presence of malicious anchors rather than explicitly identifying, detecting and eliminating them, is based on the use of a *trust model* that can efficiently localize the target with an acceptable bounded error while reducing the number of required anchors compared with the "$k+3$" *condition*.

The remainder of this paper is organized as follows. In Section II, we provide some background on how AT-Dist does work and analyze some potential security threats against it. In Section III, we propose our first technique to secure AT-Dist by combining symmetric encryption with RC4-based hash function. Section IV develops our second technique which is based on a trust model. We verify the performance of the second technique by means of extensive simulations in Section V. Finally, conclusions and some directions for future works

978-1-4673-1881-5/12/$31.00 ©2012 IEEE

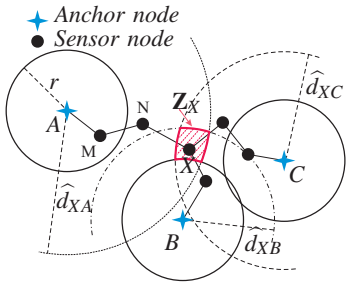


Fig. 1: Principle of the localization process in AT-Dist.

are given in Section VI.

II. AT-Dist localization Algorithm

A. Basic Ideas

We consider a multihop WSN composed of two kinds of nodes: *sensor* nodes that want to compute their own locations and *anchor* nodes that know their locations for example by GPS. The AT-Dist localization algorithm [5] is based on three-phase approach for determining the individual sensor node positions. In the first phase, AT-Dist starts at the anchors, who send a message, called a *beacon*, including their identity, position, and a path length set to 0. Each receiving node calculates the range from the sender, adds it to the path length and forwards (broadcasts) the message if the flood limit allows it to do so (*i.e.,* hop count limit). The end result is that each node will have stored the position and minimum path length to at least flood limit anchors. As illustrated in Figure 1, sensor node X estimates its distance $\widehat{d}_{XA}$ from anchor node A as the sum of ranges d_{XN}, d_{NM} and d_{MA}. In the second phase, each node restricts the zone where it can be localized based on the distance estimates to a number of anchors provided by the first step. As we can see from Figure 1, node X estimates distances $\widehat{d}_{XA}$, $\widehat{d}_{XB}$ and $\widehat{d}_{XC}$. Since all anchors are not neighbors of X, then X is not inside disks centered respectively in A, B and C with radius r but it is inside disks with radii equal to $\widehat{d}_{XA}$, $\widehat{d}_{XB}$ and $\widehat{d}_{XC}$ respectively. The intersection of those domains defines a zone $\mathbf{Z}_X$. Then, X determines its position as the centroid of that zone with a position error bound, and when this position error bound goes below a given threshold on a node, this node is considered as an estimated anchor. The objective of the third phase is to refine the initial node positions computed during the second phase by using information from estimated anchors to improve the knowledge of their positions.

B. Security Threats Against AT-Dist

WSNs are generally exposed to two types of attacks: inside and outside attacks. The inside attack concerns a node in the network that has turned on to be malicious and replays a wrong data through the network. This inside adversary knows all security parameters shared in the network which exposes to risks the whole network. However, the outside attacks are made by external nodes. They can jam, inject false data and eavesdrop on communication. Note that we only restrict ourselves here to security threats that can compromise the localization process and not other network protocols. Due its multihop nature, many attacks can be launched against the localization process in AT-Dist. For example, an attacker can decrease or increase the hop counts or distort the range measurements in each single hop. In another attack, the attacker may impersonate anchor nodes to broadcast false locations. More complicated attacks can occur such as the *Wormhole* or the *Sybil* attacks [3], [6]. For a more comprehensive review on this issue, the reader should refer to [7].

III. Prevention-Oriented Security Features for AT-Dist

In order to enable secure location computation by AT-Dist protocol in an untrusted environment, we propose some security features under the following model threat based on two assumptions: (*i*) An adversary can only launch external attack whereas insider attacks are not possible. (*ii*) There can be malicious anchors that can cheat by broadcasting their own location inaccurately or by manipulating the distance estimation process.

A. Encryption

While being broadcast from node to node, all the beacons initially transmitted by anchor nodes are encrypted with a globally shared symmetric key K_0, preloaded in every sensor node and anchor before deployment. We don't consider here asymmetric key encryption because sensor nodes are generally intended to be hardware and power limited, whereas symmetric cryptography solutions are light and thus, more relevant to WSN [4]. This security feature is efficient to protect the localization information.

B. Authentication

The core of AT-Dist algorithm is the use of inter-node distance measurements to locate the entire network. Unlike single-hop localization algorithms [2] in which a sensor node has to authenticate only the beacons received from anchor nodes, in AT-Dist there is a need to ensure authentication between all neighboring nodes, both non-anchors and anchors. Therefore, a node should only accept and/or forward location messages from authenticated neighbors. Otherwise, there could be malicious nodes that give false location information to sensor nodes compelling them to compute incorrect location. We propose here an authentication scheme, which provides basic security guarantees, namely confidentiality and authenticity of the location message and prevents from external non-anchor nodes.

This scheme describes a lightweight mechanism similar to digital signature based on the use of a global key K_0 and an RC4-based hash function, h [8]. At the beginning, anchor node A_i appends a hop count field n initialized to 1 to the beacon message denoted by $Beacon_1$. This data is encrypted with the global key K_0 and then appended into its hash value according to the following format: $\{1||Beacon_1\}_{K_0}||h(1||Beacon_1)$. Finally, the resulting message is forwarded to all neighbor nodes. While being broadcast, the first part is updated at

each hop whereas the hash function h is applied successively to the second part. At the n^{th} hop, a receiving sensor node decrypts the first part of this message and then extracts the hop count field n. It is then possible to create the n-order hash value from the first part of the received message, namely $h^n(n||Beacon_n)$ and then compare it with the second part of the received message. If the hash codes match, then the message has not been altered. Otherwise, the message is dropped. After successful verification, the sensor node updates the beacon message, increments by one the hop count, calculates the new hash value and finally broadcasts the following message: $\{n+1||Beacon_{n+1}\}_{K_0}||h^{n+1}(n+1||Beacon_{n+1})$.

Applying the hash function repeatedly n times ensures that even that an attacker succeeds to compromise a message at the n^{th} hop, it would be very hard to do so at the next hops as the hop count changes hop by hop. For external attacks where adversary may eavesdrop, copy and re-play the broadcast messages, this method guarantees confidentiality and authenticity of the message. However, this method does not prevent from *insider attacks*, where the adversary compromises one or more valid sensor nodes in the WSN, and thus can obtain all cryptographic information stored on the compromised sensor nodes.

IV. SecAT-Dist: An Attacks-Tolerant Security Scheme for AT-Dist

We propose here a security scheme called SecAT-Dist that *tolerates*, to some extent, the presence of malicious anchors or insider attacks rather than explicitly identifying, detecting and eliminating them. Our motivation for considering this issue comes from the fact that AT-Dist relies on using all the available anchor nodes. The common assumption that using more anchors could enhance the accuracy of location estimation should be reconsidered in untrusted environment because one or more malicious anchor nodes could deliberately provide incorrect location. Therefore, it is necessary to reduce the number of malicious anchors actively participating in the localization process. This is possible as long as the "$k+3$" *condition* allows it to do so. We show in the following that this threshold can be improved by introducing a trust model.

A. Trust Model

To this end, we introduce a confidence index, a metric that captures the intuitive idea that the further a beacon message comes from, the less it is trusted by a recipient. This observation stems from the fact that while traveling from hop to hop, a beacon message is susceptible to be compromised by an intermediary sensor node. For an arbitrary sensor node that proceeds to locate itself, there is no difference to consider that the received beacon message is originally compromised by a cheating anchor node or has been altered on behalf while traveling. Therefore, for the sake of simplicity, we consider only cheating anchors.

Confidence index is defined as follows. For an arbitrary sensor node, a beacon message which is received from anchor node A_i, carries out a confidence value that is inversely proportional to the distance in hop number separating anchor node A_i from this sensor node. Thus, for a given sensor node, each anchor node can be assigned a confidence index (referred to as CI) to indicate its level in providing reliable beacon message. The CI is a real number between zero and one. An anchor with $CI = 1$ is certainly deemed honest whereas a one with $CI = 0$ is certainly deemed a malicious node, thereby dramatically reducing the accuracy of the location position. In contrast, an anchor node with a confidence index in the range $0 < CI < 1$ has suspicious behavior, that is, its contribution is more or less prejudicious for the localization process. In conclusion, the higher confidence index is assigned to an anchor node, the less error impact on the location computing.

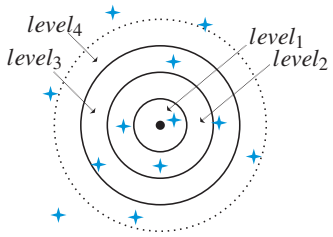


Fig. 2: Confidence index levels

For a given sensor node, anchor nodes are divided into four levels, which are described in Figure 2. The first level is composed of the set of *one-hop* away anchors. Each anchor in this level is assigned a confidence index CI_{l_1} in the range $[0.8,1]$. The second level is composed of the set of *two-hop* away anchors. A confidence index CI_{l_2} in the range $[0.6,0.8[$ is attributed to each anchor in this level. The third level is composed of the set of *three-hop* away anchors. Each anchor in this level is assigned a confidence index CI_{l_3} in the range $[0.4,0.6[$. Finally, the fourth level contains all the anchor nodes that are *four-hop* away or *beyond*. The reason behind our choice to restrict ourselves to only four levels stems from the fact that the error induced by the participation of four-hop anchors and beyond is generally prohibitive in distance-based multihop localization algorithms.

Note that here we focus only on the localization process in order to reduce the number of required anchors compared with the k+3 condition. We will not introduce messages cryptography nor authentications in the algorithms.

B. SecAT-Dist Description

Based on the previous trust model, SecAT-Dist mechanism aims at reducing the number of malicious anchors from taking part in the localization process. The idea is that by introducing the confidence index, SecAT-Dist operates in such a way that it excludes non confident anchors that could *bias* the estimate toward an inaccurate location while selecting confident anchors that could contribute more to accuracy. In this way, SecAT-Dist is expected to use a lower number of anchors compared to the "$k+3$" *condition*. Based on an iterative process, SecAT-Dist works as follows. As beacons are being received, a given

sensor node starts the process by summing up confidence indexes starting by CI_{l_1}, then CI_{l_2}, CI_{l_3} and finally CI_{l_4} for the rest of anchors until obtaining a satisfactory condition that is the calculated average number of confident anchors is greater or equal to the required minimum number of anchors given by the "$k+3$" *condition*. However, the latter condition has to be tuned by subtracting the contribution of confident anchors from the whole number of required anchor nodes, that is $k+3$. Formally, if the iteration process stops after n_{stop} iterations in the first level, (n_{stop} stands also for the number of all received beacons until the stop of the process), then the probability that a received beacon (or anchor) be confident is $P_{conf} = \sum_{1 \le l_1 \le n_{stop}} CI_{l_1}$ divided by n_{stop}. Thus, the average of confident beacons among the k received anchors is $k \times P_{conf}$. Therefore, the stop condition can be expressed as

$$\sum_{1 \le l_1 \le n_{stop}} CI_{l_1} \ge k+3-\frac{k}{n_{stop}} \times \sum_{1 \le l_1 \le n_{stop}} CI_{l_1}. \qquad (1)$$

The SecAT-Dist process is described in details by the two following algorithms. Note that here we focus only on the localization process in order to reduce the number of required anchors compared with the "$k+3$" *condition*. We will not introduce neither messages encryption nor authentications in the algorithms. SecAT-Dist (Algorithm 1) is initially executed. According to the stop condition explained above, function stop is called (Algorithm 2) as many times as it is necessary.

Algorithm 1 SecAT-Dist Algorithm

```
sum ← 0; stop ← false
{A: is a vector of CI_l1};{B: is a vector of CI_l2}
{C: is a vector of CI_l3};{D: is a vector of CI_l4}
Stop(n1,A,sum)
if !stop then
   Stop(n2,B,sum)
else
   Stop(n3,C,sum)
   if !stop then
      Stop(n4,D,sum)
   end if
end if
```

Algorithm 2 Stop(n,X,sum)

```
i ← 1; sumI ← 0
while n ≥ i do
   average ← sumI/i
   if (sum + sumI) ≥ (k + 3 − k × average) then
      stop ← true{stop algorithm}
   else
      sumI ← sumI + x_i
      i ← i + 1
   end if
end while
sum ← sumI + sum
```

V. Performance Evaluation

We investigate the efficiency and the accuracy of SecAT-Dist algorithm while considering the number of required anchors participating in the localization process, then transmission range, the distance error introduced by a malicious node, and the induced estimated location error. This includes also comparisons with the unsecured version of AT-Dist and the "$k+3$" *condition*.

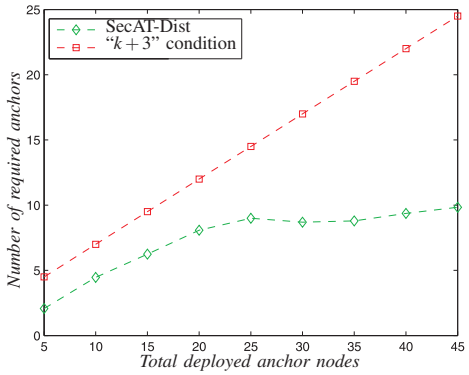


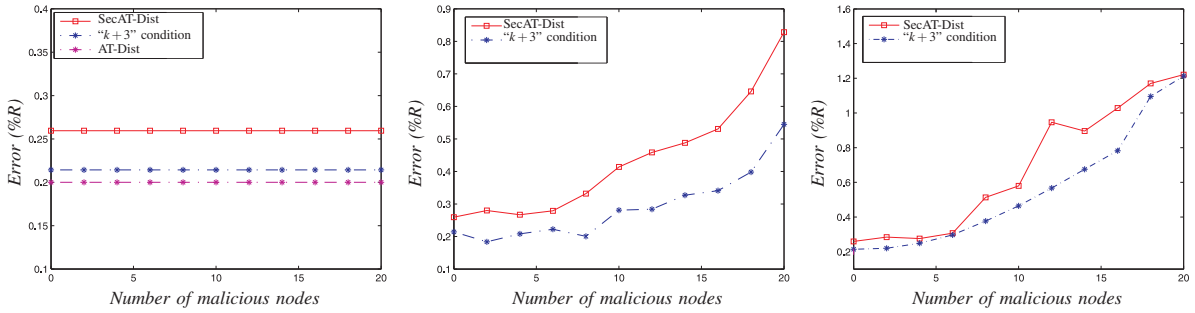
Fig. 3: Number of required node anchors as a function of the total deployed anchor nodes.

A. Simulation setup

We use the network simulator OMNET++. Simulation area consists of a 100 m × 100 m two dimensional zone. We consider a total number of 100 sensor nodes and 43 anchor nodes. Nodes are scattered uniformly over the simulation area. The sensor node that wants to estimate its location is also uniformly selected. The transmission range of each node is fixed to 15 m so that we can apply a multihop protocol. We choose ZigBee as a wireless technology. This choice can be explained by the fact that it is the most used for indoor environments and also because a ZigBee device is an ultra low power device. The propagation model is a vital parameter for a wireless sensor network simulation to determine whether our results take into consideration the workspace characteristics or not. In this simulation, we use the Log Normal Shadowing analogue model that can be used in an indoor environment.

B. Simulation results

1) Number of required anchors : First, we are interested in the efficiency of the SecAT-Dist algorithm in terms of required number of node anchors compared to the one obtained by the "$k+3$" *condition*. To this end, we plot in Figure 3 the required number of node anchors as a function of the total deployed anchor nodes for both algorithms. If we look at the graph, we will see that SecAT-Dist algorithm readily outperforms the "$k+3$" *condition*. This is an expected result because the SecAT-Dist algorithm takes benefits from the trust model by trying to eliminate as much as possible undesired anchor nodes. We can observe also that the curve of SecAT-Dist algorithm increases initially with a high rate similarly to the one of the "$k+3$" *condition* which has a linear growth. As we can see in the plot, there is a crossover in this behavior. Beyond the middle region (around the value 25), the SecAT-Dist algorithm plot increases but with a low slope.



(a) $\varepsilon = 0$ (b) $\varepsilon = 2$ (c) $\varepsilon = 4$

Fig. 4: Impact of the number of malicious anchor nodes on the localization error for different values of parameter ε.

2) Accuracy : We evaluate now the accuracy of the SecAT-Dist algorithm. To implement the malicious behavior of some anchor nodes, we consider that the distance measurement error induced by such a node is uniformly distributed between $[-\varepsilon, \varepsilon]$, where ε stands for the maximum distance measurement error introduced by a malicious anchor node. We intend here to study the impact of the number of malicious anchor nodes on the localization error for different values of the maximum distance measurement error ε. As illustrated in Figure 4, we observe this impact for three values of parameter ε, namely $\varepsilon = 0$ m, $\varepsilon = 2$ m and $\varepsilon = 4$ m and we plot the induced localization error normalized to the transmission range R for SecAT-Dist, the "$k+3$" *condition* and AT-Dist.

As the total number of anchor nodes is set to 43, the maximum number of malicious anchor nodes tolerable by the "$k+3$" *condition* is then $\frac{43-3}{2} = 20$. Therefore, we run our simulations under varying the number of malicious nodes up to the value 20. In Figure 4(a) that corresponds to $\varepsilon = 0$ m, we remark that the localization error remains constant as the number of malicious nodes increases. This is consistent with the intuition since $\varepsilon = 0$ m is equivalent to say that all anchor nodes are honest. Remark also that AT-Dist outperforms its secure extension SecAT-Dist in terms or localization accuracy. This observation is not surprising since that in AT-Dist all anchor nodes actively participate in the localization process, which is not the case for SecAT-Dist which reduces as much as possible the number of anchor nodes. However, the good accuracy of AT-Dist is achieved at the cost of additional state information at sensor nodes, which is costly in terms of complexity and energy.

As regards to Figures 4(b) and 4(c), some general remarks can be drawn. First, we can observe that the localization error increases as ε increases for both SecAT-Dist and the "$k+3$" *condition*. This is also consistent with the intuition that more malicious anchors decrease the localization precision. Second, at fixed values of ε, the localization error of SecAT-Dist increases very slowly as the number of malicious nodes increases until a given value (around 10). Moreover, at lower values of the number of malicious nodes, the SecAT-Dist scheme has similar accuracy not only as the "$k+3$" *condition* but also as the AT-Dist algorithm (Error around 0.2%R). However, at higher values of the number of malicious nodes, the localization error slightly increases but remains acceptable.

VI. Conclusion

We have proposed in this paper a general framework for securing AT-Dist. The proposed secure scheme was built by following two techniques: (1) A prevention-oriented technique based on encryption and authentication operations. (2) The second technique is based on mechanisms that are robust enough to tolerate the effect of malicious anchors by introducing a trust model. Such a model tends to favor confident anchors while preventing malicious anchors to take part in the localization process. To assess the efficiency of our solution, extensive simulations were conducted. The obtained results showed that our security scheme achieves acceptable accuracy while reducing the number of anchor nodes. As a future research, we plan to extend our trust model and give directions on how to implement it.

References

[1] Murtuza Jadliwala, Sheng Zhong, Shambhu Upadhyaya, Chunming Qiao, Senior Member, and Jean pierre Hubaux. Secure distance-based localization in the presence of cheating beacon nodes. *IEEE Transactions on Mobile Computing*, 9(6):810–823, 2010.

[2] Loukas Lazos and Radha Poovendran. Serloc: secure range-independent localization for wireless sensor networks. In *Proceedings of the 3rd ACM workshop on Wireless security*, WiSe '04, pages 21–30, New York, NY, USA, 2004. ACM.

[3] Loukas Lazos and Radha Poovendran. Hirloc: high-resolution robust localization for wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, 24(2):233–246, 2006.

[4] Satyajayant Misra, Guoliang Xue, and Sarvesh Bhardwaj. Secure and robust localization in a wireless ad hoc environment. *IEEE Transactions on Vehicular Technology*, 58(3):1480–1489, 2009.

[5] Clément Saad, Abderrahim Benslimane, and Jean-Claude König. AT-Dist: A Distributed Method for Localization with High Accuracy in Sensor Networks. *Stud. Inform. Univ.*, 6(1):14–39, 2008.

[6] Kuo-Feng Ssu, Wei-Tong Wang, and Wen-Chung Chang. Detecting sybil attacks in wireless sensor networks using neighboring information. *Comput. Netw.*, 53:3042–3056, December 2009.

[7] Yingpei Zeng, Jiannong Cao, Jue Hong, and Li Xie. Secure localization and location verification in wireless sensor networks. In *MASS*, pages 864–869, 2009.

[8] Chang N. Zhang, Qian Yu, Xun Huang, and Cungang Yang. An rc4-based lightweight security protocol for resource-constrained communications. In *Proceedings of the 2008 11th IEEE International Conference on Computational Science and Engineering - Workshops*, pages 133–140, Washington, DC, USA, 2008. IEEE Computer Society.