EURASIP Journal on Information Security
a SpringerOpen Journal

RESEARCH Open Access

ADLU: a novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks

Eirini Karapistoli* and Anastasios A Economides

Abstract

Wireless sensor networks (WSNs) are gaining more and more interest in the research community due to their unique characteristics. Besides energy consumption considerations, security has emerged as an equally important aspect in their network design. This is because WSNs are vulnerable to various types of attacks and to node compromises, and as such, they require security mechanisms to defend against them. An intrusion detection system (IDS) is one such solution to the problem. While several signature-based and anomaly-based detection algorithms have been proposed to date for WSNs, none of them is specifically designed for the ultra-wideband (UWB) radio technology. UWB is a key solution for wireless connectivity among inexpensive devices characterized by ultra-low power consumption and high precision ranging. Based on these principles, in this paper, we propose a novel anomaly-based detection and location-attribution algorithm for cluster-based UWB WSNs. The proposed algorithm, abbreviated as ADLU, has dedicated procedures for secure cluster formation, periodic re-clustering, and efficient cluster member monitoring. The performance of ADLU in identifying and localizing intrusions using a rule-based anomaly detection scheme is studied via simulations.

Keywords: Wireless sensor networks; UWB radio technology; Security in UWB WSNs; Anomaly-based detection; Attack attribution; Ranging attacks

1 Introduction

A wireless sensor network is a network of cheap and simple processing autonomous devices (called sensor nodes) that are spatially distributed in an area of interest in order to cooperatively monitor physical or environmental phenomena. Mostly based on non-renewable resources, such as batteries, wireless sensor networks (WSNs) call for robust and energy-efficient solutions both at the software and hardware levels. Undoubtedly, the IEEE 802.15.4-2011 standard [1] for low-rate wireless personal area networks (LR-WPANs) is a valuable candidate for the energy-constrained WSNs. The standard defines the physical (PHY) and medium access control (MAC) layers. Among the available PHY options, the impulse radio ultra-wideband (IR-UWB) PHY (formerly defined in the IEEE 802.15.4a-2007 standard) has several advanced properties, such as built-in ranging capabilities, low duty cycle, low probability of detection, and robustness against interference, appointing it an ideal information carrier for communication among the sensor network devices [2].

From an application's point of view, the driving force behind research in WSNs is to develop systems that can operate unattended for large periods. Besides energy consumption considerations, the unattended nature of the deployed WSNs raises administration problems and appoints the security as an additional critical element in the network design [3]. As identified in [4-6], WSNs are susceptible to various types of attacks or to node compromises that exploit known and unknown vulnerabilities of protocols, software, and hardware, and threaten the security, integrity, authenticity, and availability of data that reside in these networked systems.

UWB transmissions offer a potentially robust physical layer security for WSNs as a consequence of their large bandwidth. Indeed, WSNs that rely on UWB radio signals are somewhat inherently more secure, because

*Correspondence: ikarapis@uom.gr
Interdepartmental Programme of Postgraduate Studies in Information Systems, University of Macedonia, Egnatias 156, Thessaloniki 54006, Greece

the low output power and short pulses of these signals make their transmissions to appear as white noise from a distance. Nevertheless, UWB signals could potentially be sniffed by a determined attacker who is located close to the transmitter, enabling the latter to launch an attack against the WSN [7,8]. Therefore, even this class of WSNs requires that security mechanisms are implemented at every layer of the sensor network protocol stack.

Currently, research on providing security solutions for WSNs has mainly focused on key management [9], authentication, and secure routing [10], as well as secure services including secure localization [11] and secure aggregation [12]. A few secure ranging and localization protocols were specifically designed for protecting the integrity of ranging and for addressing location-related attacks in UWB WSNs [13-16]. Signaling schemes have also been proposed to improve physical layer security of UWB systems [8]. Finally, a number of routing and clustering protocols attempt to address networking issues in UWB WSNs [17], lacking however advanced security features in their design.

In general, most of the security protocols mentioned above can cope with weak, external attackers. However, strong, internal attackers, which managed to penetrate the first perimeter of defense (for instance through tampering sensor nodes [18]), can only be dealt with using intrusion detection systems (IDSs). Various signature-based and anomaly-based IDS architectures have been proposed for flat and hierarchical WSNs [19]. However, the energy constraints and scalability issues in WSNs dictate the use of an hierarchical anomaly-based detection model for IDS [20]. In this grouping technique, the essential operation is to select a set of cluster heads (CHs) among the nodes in the network and to cluster the rest of the nodes with them. Cluster heads are responsible for coordination among the nodes inside their clusters (intra-cluster data gathering) and for forwarding the collected data to the sink node, usually after efficiently aggregating them. With regard to anomaly detection, cluster heads are also tasked with intrusion detection functions, such as collecting intrusion alarms from their cluster members (CMs). Additionally, the cluster head nodes may also detect attacks against other cluster head nodes of the network, since they constitute the backbone of the routing infrastructure.

While a number of anomaly-based detection systems (ADSs) have been proposed for hierarchical, cluster-based WSNs [19-21], to the best of our knowledge, none of them is specifically designed for the emerging UWB transmission technology. The ultra-wideband nature of this PHY and its high precision ranging capability (1-m accuracy and better [22]) enable the ADS not only to detect a malicious behavior, but also to localize the anomaly by relying on internal tools, namely on accurate time-of-arrival (TOA)-based UWB distance measurements.

Accordingly, the present work contributes to the area of wireless sensor network security by proposing a novel anomaly-based detection and location-attribution algorithm for cluster-based UWB WSNs, named ADLU. The proposed algorithm has dedicated procedures for secure cluster formation, periodic re-clustering, and efficient cluster member monitoring. Furthermore, it exploits the peculiar characteristics of the UWB PHY defined in the IEEE 802.15.4 standard [1] in order to facilitate the anomaly detection and location attribution processes. To help address the security challenges, ADLU offers the following contributions:

- It defines a novel, trust-aware leader election metric that makes the leader election process of clustering immune to ranging attacks.
- It introduces a monitoring mechanism for both the cluster members and the cluster heads.
- It specifies a rule-based detection engine that accurately analyzes data packets to detect signs of sensor network anomalies.
- It encapsulates a UWB time-of-arrival triangulation of ranges technique that adds location-attribution capabilities to the algorithm.

ADLU is different from existing works in several other ways. Firstly, it does not rely on a special type of hardware, i.e., global positioning system (GPS) devices, to perform the localization task. Moreover, it does not require heavy communication among the nodes, since the decision making and node revocation processes follow the low overhead hierarchical network model.

The remainder of the paper is organized as follows. In Section 2, existing anomaly detection algorithms developed for cluster-based WSNs are outlined. A detailed description of the ADLU algorithm is provided in Section 3. Section 4 illustrates the obtained simulation results, followed by detailed reports. Finally, conclusions are given in Section 5.

2 Related work

The issue of anomaly detection in hierarchical, cluster-based WSNs has been addressed by several scientific works. According to a recent study [20], the developed ADSs can be categorized based upon the incorporated anomaly detection pattern. The detection pattern is basically linked to who takes charge of carrying out the data processing procedure of anomaly detection. There are basically three available options, which are highlighted in Figure 1. First, the cluster head is responsible for the processing and decision making alone [23]. Second, the cluster head and cluster members cooperate to accomplish

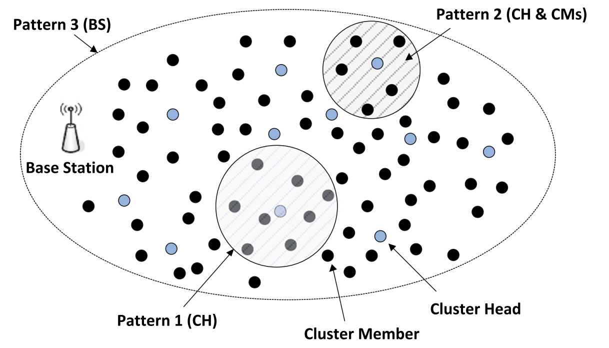

Figure 1 Anomaly detection patterns in hierarchical WSNs [20].

this [24-27]. Third, this procedure is carried out by a central authority, namely, the base station (BS) [28,29].

More specifically, in the protocol of the first detection pattern [23], the cluster head depends on the alarms or data received from the cluster members to determine whether a node is malicious. Thus, the cluster members, except collecting the input data sets, neither participate in the data processing procedure nor contribute to the procedure of analysis and decision. However, this clearly leads to the overuse of energy in the cluster heads. Moreover, the decision making procedure depends on the validity of the incoming data. If this data is falsified by a compromised node, the cluster head will not take the right decision [30].

The second and third detection patterns seem to balance the nodes' energy dissipation more reasonably. For instance, in [26] and [25], the cluster head is taking care of its cluster members, whereas a part of the cluster members are activated for monitoring the cluster head. By letting the cluster head be attended, one increases the security, as he or she meets the 'trust-no-node' requirement [31]. In [26], the authors by employing the self-organizing map (SOM) neural network algorithm and the K-means clustering algorithm at the same time, they raise massive computation burdens. Similarly in [25], the kernel density estimator, on which this detection scheme relies, requires massive information exchange between the sensor nodes, or equivalently, smart strategies to reduce the communication cost.

To reduce the energy overheads, the genetic algorithm (GA)-based scheme presented in [28] benefits from the hierarchical structure of the network arranging the primary computing tasks to the base station (recall that the base station has much softer limitations for power and computation). While this scheme is not directly concerned with detection, however, it could assist detection schemes in advancing their performance and efficiency by optimizing, for instance, the placement of the monitoring nodes. The limitation of this scheme is that GA suffers from exponential time increase if the network's scale grows.

From the above analysis, it becomes apparent that extensive work has been done in the area of anomaly-based detection for cluster-based WSNs. However, none of the proposed network-based ADS architectures can be directly applied to IEEE 802.15.4-compliant WSNs operating under the UWB PHY since they do not take into account the UWB technology strengths and limitations. Therefore, in this paper, we move towards that direction by proposing a modular, robust, and lightweight ADS architecture specifically designed for this class of wireless sensor networks.

3 Anomaly detection and localization in UWB wireless sensor networks

3.1 Basic concept and model assumptions

As already revealed, the energy constraints in WSNs dictate the use of a hierarchical model for anomaly detection. In order to partition the network into clusters and determine the cluster heads, a cluster formation protocol is executed first. Towards securing the leader election mechanism of this protocol, a new trust-aware leader election metric is defined. After the clusters are formed and a specific number of rounds is reached, called *repetition period* (RP), ADLU redistributes the role of the CH. One round is assumed to be completed when all cluster members (at maximum N_u) have exchanged a packet with their CH. Since each cluster may have a different number of cluster members, a total number of N_u exchanges is assumed so that all clusters begin and end their rounds in exactly the same time. ADLU adopts the concept of cluster member limitation, i.e., a maximum number of N_u nodes is set that can be members of a CH, so as to avoid high-energy transmissions and to bound the induced interference.

3.1.1 Exploiting the ranging capability of the 802.15.4 standard

Towards providing anomaly detection and localization functionalities, ADLU exploits the peculiar characteristics of the IEEE 802.15.4 UWB PHY and most importantly its capability at providing high precision ranging [1]. This feature is an enabler for our anomaly detection and location-attribution algorithm. Ranging in IEEE 802.15.4 standard is an optional capability achieved through support of a number of specific PHY capabilities as well as defined MAC behaviors and protocols. The mandatory ranging protocol is the two-way ranging (TWR) depicted in Figure 2, which allows for ranging measurements based on the round trip delay between two stations, without the need for a common time reference [22]. In this scheme, the ranging-capable device (RDEV) A begins the session by sending a range request packet[a] to node B. Then, node B waits a time τ, known to both devices, to send a request

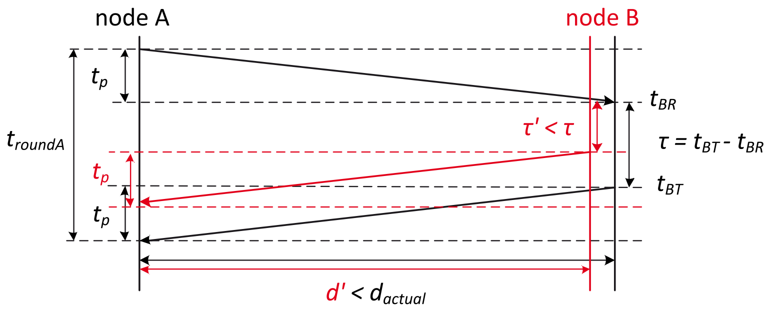

Figure 2 Attacking the two-way ranging protocol of the IEEE 802.15.4 standard. A distance-decreasing attack is shown.

back to node A. Based on that packet, node A can measure the round-trip time, $t_{\text{roundA}} = t_p + \tau$, and extract the one-way time-of-flight, t_p, with respect to its own reference time.

3.1.2 Vulnerability of the two-way ranging protocol

In localizing anomalies, trustworthy distance measurements are necessary. According to a recent study [32], however, the two-way ranging protocol of the UWB PHY is vulnerable to ranging attacks. A compromised node B may tamper its processing time as τ' in order to manipulate the distance measurement and cheat node A about its distance (see Figure 2 for an explanation). Hence, in making the UWB distance measurements immune to ranging attacks, even in the presence of an adversary interfering with the ranging process, ADLU adopts the PHY hacks proposed in [32], which include an energy detection (ED) countermeasure and convolutional plus time-hopping code patches.

Next, we describe the ADLU algorithm in detail. Within our model, we assume that no node can be fully trusted since no pre-existing distributed trust model exists. Moreover, we assume that a number of legitimate nodes are tampered with and reprogrammed for an adversary's purpose, i.e., in order to launch an attack against the clustering protocol. While an adversary can completely take over the nodes, we assume that such an adversary cannot outnumber legitimate nodes by replicating captured ones or introducing new ones in sufficiently many parts of the network.

3.2 Detailed protocol description

The ADLU algorithm uses a round-based approach towards cluster formation and anomaly detection. At the end of each round (RP), the network is re-clustered and new cluster heads are assigned. A monitoring mechanism is introduced to assist the analysis and decision making process of anomaly detection. Finally, anomalies are localized using a geometric, *trilateration* technique. The different phases of the ADLU algorithm are analyzed below.

3.2.1 Phase 1: secure leader election and cluster formation

In order to establish the clusters, a modified version of the *energy-aware self-organizing clustering* (EASOC) algorithm [33] is used. This protocol is a *leader-first* clustering protocol developed for UWB wireless sensor networks. This means that the cluster heads are elected first, based on an *energy-aware interference factor* (EAIF) shown in Equation (1) and then other nodes join these cluster heads forming a multi-cluster network.

$$\text{EAIF}_i = \frac{\frac{1}{N_i}\sum_{k=1}^{N_i} D_{ik}^{\alpha}}{E_i^{\text{res}}}. \qquad (1)$$

This protocol, however, does not offer the security we need when electing the cluster heads, because internal attackers that do not follow the protocol semantics can lie about their distance or their residual energy to make themselves elected as cluster heads, thus giving them the chance to launch severe attacks. This vulnerability is dealt with by modifying the leader election protocol (LEP). In securing the LEP protocol, a new leader election metric is introduced: the *secure leader election indicator* (SLEI). For a node i with N_i neighbors, its SLEI$_i$ is computed as follows:

$$\text{SLEI}_i = \text{EAIF}_i \cdot W_i = \frac{\frac{1}{N_i}\sum_{k=1}^{N_i} D_{ik}^{\alpha}}{E_i^{\text{res}}} \cdot \frac{1}{N_i}\sum_{k=1}^{N_i} \theta_{ki}, \qquad (2)$$

where D_{ik} is the distance between node i and its kth neighbor, α is the path loss exponent, E_i^{res} is the residual energy of node i, W_i is a weight ranging from 0 to 1, and $\theta_{ki} \in [0, 1]$ is a trust value assigned to node i by its peers. The rationale behind this definition is that when all nodes have the same EAIF$_i$, we should select the nodes with the highest weighted trust, W_i. Nodes that have lower weighted trusts are avoided from becoming cluster heads, even though they may have higher EAIF$_i$ (note that the EAIF indicator is upper bounded).

Basically, the clustering algorithm in [33] follows four steps towards dividing the network into clusters and defining the cluster heads. The *first step* consists of the exchange of ranging-enabled beacons between the neighbor nodes and the computation of the EAIF_i indicator. In the *second step*, each node floods the network with a table containing its closest N_u neighbors, and its locally computed EAIF_i, which maybe falsified if node i is malicious.

Hence, within ADLU, we modify this. Each node floods the network with a table containing its EAIF_i value and the trust values θ_{ik} this node assigns to its closest N_u neighbors. The trust metric is initialized to 1 and is updated every time a node enters the 'monitoring and trust update' phase. Trust updates are based on the trustworthiness of a node. We classify the trustworthiness into three grades: *trust*, *distrust*, and *uncertain*, valued as 1, 0, and 0.5, respectively. Hence, if node i behaves maliciously, the trust values assigned to this node by its monitoring neighbors, θ_{ki}, will be decreased using a *two-step strategy*: from 1 to 0.5 and then to 0. Accordingly, W_i and SLEI_i will be decreased. At the end of this step, every node constructs a table of N entries, one for every node in the network. Hence, all nodes have exactly the same global knowledge of the network status.

In the *third step*, ADLU's secure LEP protocol begins. The node with the maximum SLEI_i is marked as cluster head, and all its neighbors, N_u at maximum, are removed from the table. This procedure continues until there is no node left to be examined that is not a cluster head. After the cluster heads have been marked, every other node selects the closest one and joins its cluster. In the *fourth step*, the cluster heads and their cluster members exchange data. The cluster heads then forward the collected data to the BS. When a predefined number of data exchanges is reached, namely RP, the entire procedure starts from the beginning. In each RP, the cluster heads will probably be different from the previous ones, and in this way, the energy-consuming role of the cluster head is reassigned among the nodes of the network, resulting in a more uniform energy consumption. We do not oversee the cases where a malicious node is elected as cluster head, especially during the network setup when no prior knowledge exists. This is the reason why we introduce a mechanism to monitor the activity of the cluster heads as well.

3.2.2 Phase 2: monitoring and trust update

The next problem we must deal with is the determination of the nodes that will run the ADS, i.e., how many and which nodes should be on duty to detect misbehaviors. In monitoring the cluster members, the intrusion detection function is activated on the cluster heads. If after an interval equal to a *monitoring period* (MP) (measured in rounds) a cluster member is judged to be abnormal by its cluster head, it is revoked. In doing so, the trust value of the malicious node as seen by its cluster head is updated (reduced) and is broadcasted as an alarm message to all cluster member nodes.

Cluster heads on the other hand are monitored by their cluster members. Cluster head monitoring is necessary to assure that even in the case the LEP protocol fails, malicious cluster heads that went undetected do not retain this role for long. A part of the cluster members, three in total, are activated for monitoring and jointly making final decisions on the maliciousness of their CH. In each MP, the cluster member nodes with the second, third, and fourth in succession biggest SLEI_i values compose the monitoring team of the CH (recall that the CH has the highest SLEI_i value within its cluster). If after the MP interval half of these nodes indicate that the cluster head is malicious (majority vote rule), then the cluster head is revoked by the monitoring team. In revoking a malicious cluster head, each member of the monitoring team broadcasts an alarm message containing the reduced trust value of the malicious cluster head, as well as its new EAIF_i value (recall that a change in the EAIF_i value is reflected on the SLEI_i value; hence, this information would allow different cluster member nodes to probably monitor the cluster head in the next MP intervals). Following the identification and revocation of the malicious CH, another cluster head, among the cluster members, is elected. In this re-clustering process, the node with the new highest SLEI_i value in the attacked cluster becomes its cluster head. This node may retain the role of the CH until the next RP round, unless it is marked as malicious by its cluster members.

With a majority rule being applied when monitoring the activity of a cluster head, if a node from the monitoring team is compromised and issues a false alarm trying to revoke a legitimate cluster head, it would have no effect because the majority would prevail. However, since the majority-vote rule represents a cooperative anomaly-detection scheme, there might be the case that multiple malicious nodes with high SLEI_i values obtain the role of the monitoring team inside a cluster, enabling them to deceive the majority-vote rule and to revoke a legitimate CH. This situation is identified by the simulation results depicted in Section 4.2 and is indicated with a drop in the detection accuracy of the ADLU algorithm when 40% or more of the nodes behave maliciously. However, this is a highly hostile condition and cannot be dealt effectively by any cooperative anomaly-detection scheme.

3.2.3 Phase 3: anomaly detection and localization

Our network-based ADS detects anomalies based on the packets that it monitors. Each node running the ADS stores a data structure for each collected packet. Then, each data structure is evaluated according to the sequence of rules defined in Table 1 (please note that jamming attacks are not considered in our study). This means that within ADLU, we employ a rule-based approach to anomaly detection. Rule-based detection appears to be

Table 1 Rule definition

Rule description	Detection metric	Attack detected
When a packet is not forwarded as it should, increase a counter. When this counter reaches a threshold *t* after MP rounds, raise an alarm.	Packet drop rate	Selective forwarding and black hole attacks [34]
When a packet does not originate from a node with a distance no longer than the radio range of a single hop, raise an alarm.	Packet origin address	Hello flood and sinkhole attacks [35]
When the distance measurements between multiple, at least two, distinct nodes match, raise an alarm.	Distance matching criterion	Sybil [36] attacks

very attractive in the context of WSNs in the essence that the detection speed and complexity certainly benefits from the absence of an explicit training procedure required, for example, in data mining approaches [20]. In rule-based detection, the anomaly detector uses predefined rules to classify data points as anomalies or normalities. While monitoring the network, these rules are selected appropriately and applied to the monitored data packets. A data packet is discarded after being tested against all rules without violating any of them. On the contrary, if a violation of any of these rules occurs or equivalently if the rules defining an anomaly are satisfied, an anomaly is declared and an alarm will be raised. An alarm generated by a cluster head indicates that a cluster member is an intruder and needs to be revoked. Similarly, if the independent alarms raised by the monitor nodes of a cluster head satisfy the majority-vote rule, then this cluster head is revoked and a new cluster head, among the cluster members, is elected.

Each time an untrustworthy node is revoked (the revocation is indicated by a broadcast alarm message), an UWB ranging-based localization algorithm is executed to identify the location of the attacker. The location-finding algorithm is composed of two steps: *ranging* and *localization* [37]. The ranging process is the action of estimating the distance between two devices. Localization is the mechanism of finding the exact location of a given node by utilizing three or more range estimates. As already analyzed, among the available ranging techniques defined by the IEEE 802.15.4 standard [1], within ADLU, the range estimates are obtained using the two-way time-of-arrival technique depicted in Figure 2. Regarding the localization process, ADLU adopts the time-of-arrival triangulation of ranges technique defined by the standard. This technique applies to the general network lacking synchronization between devices and/or *a priori* organization, and assumes that three ranges $d_1 = c \times t_1$, $d_2 = c \times t_2$, and $d_3 = c \times t_3$ are gathered from three 'anchor devices' $i = 1, 2, 3$ with locations (x_i, y_i) (see Figure 3 for a geometry of this technique). The role of the three anchor nodes is assigned to those cluster member nodes that within the given MP interval have been elected to monitor the CH.

Following the assignment of the anchor nodes, the coordinates of the target node in the 2D space are computed by solving a linear least-squares (LLS) problem, which translates to finding the intersection of three circles. As soon as the x, y coordinates of the malicious node are determined, the anchor nodes are then responsible for forwarding this information to the BS to enable the system administrators and the security professionals to take countermeasures. In doing so, they first transmit the location information to the CH. Then, the CH forwards this information to the BS either directly (if the BS is within range) or via multiple hops (inter-cluster routing). Since, there might be the case that the CH is the malicious node the anchor nodes were monitoring and for which they initiated the localization process, then in this case, the anchor nodes will have to wait for the new CH to be elected before transmitting this critical data to the legitimate one. The three phases of the ADLU algorithm are summarized in algorithmic form within Algorithm 1.

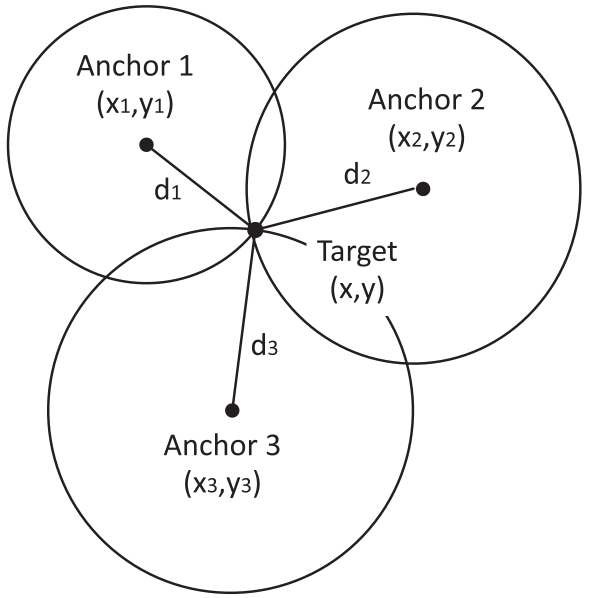

Figure 3 Time-of-arrival triangulation of ranges to determine location (Adapted from [1]).

Algorithm 1 The ADLU algorithm

```
{ Phase 1: Secure Leader Election and Cluster Formation}
for each node $i$ in the network do
    Step 1: exchange a ranging-enabled beacon with all its neighbors (closest $N_u$)
    Step 1: calculate its EAIF$_i$ indicator
    Step 2: flood the network with the table {node_ID $i$, EAIF$_i$, $\theta_{ik} = 1, \forall$ neighbors $k$}
end for
Step 2: construct a table from the received messages
for each node $i$ in the table run the LEP protocol do
    if nodes are left in the table then
        Step 3: mark node with the maximum SLEI$_i$ as cluster head (CH)
        Step 3: delete the neighbors of this CH from table ($N_u$ at most)
    end if
end for
for each node left in the table do
    Step 4: node $i$ joins the closest CH
end for
Step 4: cluster members (CMs) exchange data with their CH

if Rounds > repetition period, RP then
    start from the beginning (Step 1)
end if
{ Phase 2: Monitoring & Trust Update }
for each node $i$ in the network do
    if node $i$ is the CH then
        start monitoring your CMs
        if Rounds > monitoring period, MP then
            collect data, update, if necessary, the trust values, $\theta_{ik}$, and execute Phase 3
        end if
    else
        select the cluster member nodes with the $2^{nd}$, $3^{rd}$, and $4^{th}$ in succession biggest SLEI$_i$ values, and start to monitor the CH
        if Rounds > MP then
            collect data, update, if necessary, the trust value $\theta_{ki}$ of the CH, and execute Phase 3
            update, if necessary, the members of the CH's monitoring team based on the updated EAIF$_i$ values of current monitoring nodes
        end if
    end if
end for
{ Phase 3: Anomaly Detection and Localization }
Apply rules on the collected data packets
if Rules are satisfied then
    Step 1: Declare the anomaly and start node revocation
    Step 2: Execute the time-of-arrival triangulation of ranges algorithm to localize the malicious node
else
    Discard the packet and continue operation
end if
```

4 Performance evaluation

We used a custom-developed simulation tool implemented in C++ to evaluate the performance of the ADLU algorithm. As stated earlier, comparison of our algorithm with classical, cluster-based ADSs would not be appropriate, as they do not take into account the UWB technology limitations and strengths. We only compare the ADLU algorithm with its ancestor, the EASOC algorithm [33], in an attempt to evaluate the energy and communication overhead it incurs to a clustering algorithm that does not implement the detection and location-attribution engines of the ADLU algorithm.

With regard to the network topology, 100 nodes were randomly placed inside a square area of 100 × 100 m^2 (the BS was placed at the center). The cluster member-limitation parameter, N_u, was set to 10[b]. Cluster member nodes where generating packets with an interarrival time equal to two packets per second. We chose to vary the monitoring period and the repetition period as follows: MP $= \{1, 2, 3\}$ rounds and RP $= \{80, 140\}$ rounds. The UWB PHY parameters are summarized in Table 2. All the presented results were averaged over 20 simulation runs.

We simulated a security-oriented application supporting sink-based reporting, that is to say, traffic flowing from the leaf nodes to the BS (typical case of a sensor network). Randomly selected intelligent adversaries include themselves in the network by replicating legitimate (captured) nodes and start launching an attack, as reflected in Table 1. In case of selective forwarding attacks, a malicious node selectively drops packets with a probability p_d. When $p_d = 1.0$, the attacker is executing a black hole attack.

Three metrics were used to evaluate the efficiency of the ADLU algorithm. These are as follows:

1. The *communication overhead*, defined as the ratio of the total communication overhead in a system that incorporates our detection algorithm against a system that does not
2. The *percentage reduction in network lifetime*, resulting from the incorporation of our detection algorithm
3. The *detection accuracy*, defined as the ratio of the detected attacks to the total number of detected and undetected attacks
4. *False negative rate*, defined as the rate at which events are not flagged intrusive by the detector, although the attack exists.

4.1 Energy and communication overhead

We begin by analyzing the communication overhead of two systems, one incorporating the ADLU algorithm and its anomaly detection and location-attribution engines, and one that does not, namely the EASOC algorithm.

Table 2 UWB PHY parameters

Property	Value
PHY option	IEEE 802.15.4 UWB PHY
Frequency band	Channel {0} with $f_c = 499.2$ MHz and BW = 499.2 MHz
Data rate	0.85 Mbs (mandatory data rate)
Rate-dependent and Timing-related parameters	mean PRF = 15.60 MHz, $T_{d\mathrm{sym}} = 1{,}025.64$ ns, $T_{p\mathrm{sym}} = 993.6$ ns, $N_{\mathrm{sync}} = 64$ symbols, $N_{sfd} = 8$ symbols
Power	36.5 μW (FCC limit for ≈ 0.5-GHz bandwidth)
Communication range	20 m
DATA packet length	1,038 symbols (+ 64 symbols for SYNC trailer)
Ranging support	TW-TOA (mandatory ranging)
Channel access	UWB preamble sense based on the SHR of a frame (clear channel assessment - CCA Mode 5)

Their ratio is denoted as the relative communication overhead. To simulate this scenario, we chose at random a number of network nodes, and we programmed them to selectively launch one of the attacks depicted in Table 1. With regard to selective forwarding attacks (launched only by cluster heads), the attacker was dropping packets with a probability $p_d = 30\%$. When $p_d = 100\%$, the attacker was executing a black hole attack. We set the threshold value for the percentage of packets being dropped over an interval MP to be $t = 20\%$. Above this threshold, an alarm was generated and node revocation was initiated. Packets dropped at a lower rate were attributed to other factors, such as collisions or node failures and did not produce an intrusion alert. For all other types of attack, distance-related rules are responsible for raising an alarm.

In Figure 4a, the curves show that the relative communication overhead increases smoothly as the percentage of malicious nodes increases. This is because more packet exchanges occur following the introduction, identification, and revocation of an increasing number of adversaries. In all cases, however, the communication overhead is kept at very low ratios, as low as 0.050 and 0.042 for RP = 80 and 140 rounds, respectively. A smaller RP value causes a slightly higher increase to the relative communication overhead, notably because of the slightly higher number of packets being broadcasted as a result of the shorter network re-clustering phase. As expected, the communication overhead is extremely low when the network contains no malicious nodes. No curves are shown with regard to the changing value of the monitoring period, MP. This is because the MP interval by relating to the decision making window of the monitoring phase mostly affects the detection accuracy of the ADLU algorithm.

Figure 4b illustrates the percentage reduction in network lifetime when common sensor nodes run our anomaly detection and location attribution algorithm. Once again, the results illustrate that as the percentage of malicious nodes inside the network increases, the reduction in the network lifetime increases. As the curves highlight, the reduction is slightly higher when RP is equal to 80. As mentioned earlier, smaller RP values cause a slightly higher increase to the relative communication overhead, which also translates to an increase in the

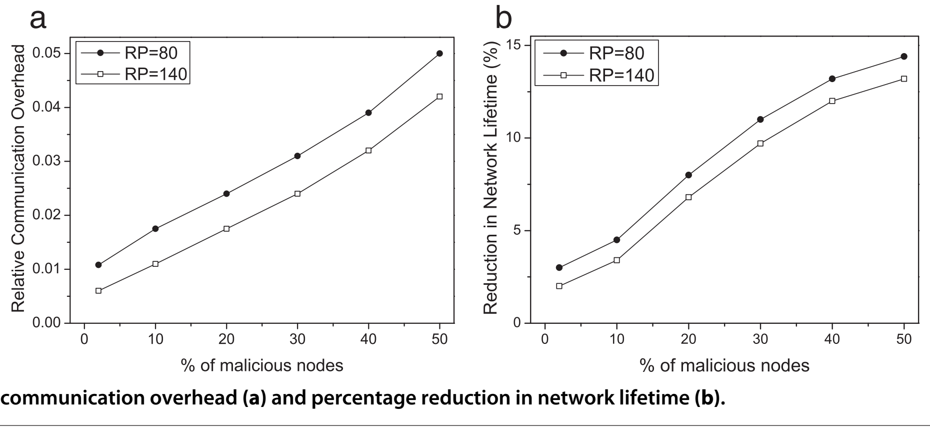

Figure 4 Relative communication overhead (a) and percentage reduction in network lifetime (b).

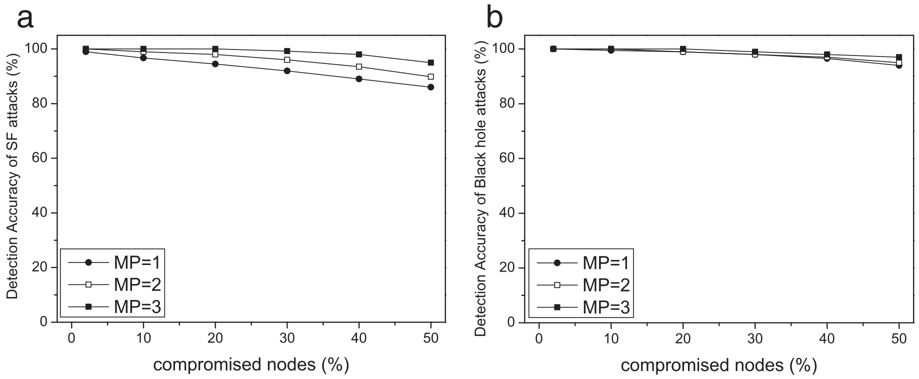

Figure 5 Detection accuracy of (a) selective forwarding attacks and (b) black hole attacks.

energy dissipation of the nodes. Overall, the network lifetime decreases by as high as 14.4% when RP = 80 rounds, and by 13.2% when RP = 140 rounds. The relatively small reduction observed in both cases is due to the fact that within ADLU, the nodes rotate the energy-consuming roles of the CH and that of the monitoring team, and as such, the energy dissipation is uniformly distributed among the network nodes. Since the network lifetime is in comparative levels when compared to a system that does not incorporate our anomaly detection algorithm, this fact can justify the installation of our ADS on the sensor nodes.

4.2 Detection accuracy and false-negative rate

The rest of the figures evaluate the detection accuracy of the ADLU algorithm against the attacks of Table 1 and the false-negative rates that it achieved. In the subsequent simulations, and more specifically in each attack scenario presented next, there was always one single type of attacker, which was varied in each simulation.

As an overall observation, we can say that the variation of MP solely affects the detection accuracy of the selective forwarding and black hole attacks illustrated in Figure 5a,b. This happens because these attacks are assessed over a time window, and therefore, their detection accuracy is affected by the monitoring interval, MP. Recall that the interval MP relates to the time window that a monitor node has in order to gather packets and analyze them for signs of intrusion. Since less packets are being collected as a result of the smaller MP interval and given that packets are dropped probabilistically, there might be the case that during a monitoring interval, the dropped packets are less than $t = 20\%$, and hence, no alarm is produced, generating false negatives (see Figure 6a). This is less probable to happen when the value of MP gets bigger or when nodes launch black hole attacks, i.e., $p_d = 100\%$. In the latter case depicted in Figure 5b, the probability that the dropped packets during an MP interval are less than t, which results in a false negative, is close to zero, and hence, the accuracy in detecting this attack is close to 100% (this is also shown in Figure 6b).

Figure 7a illustrates the detection accuracy of hello flood attacks (similar curves are obtained when the attacker launches a sinkhole attack). In examining these attacks, we chose to vary the accuracy in the UWB

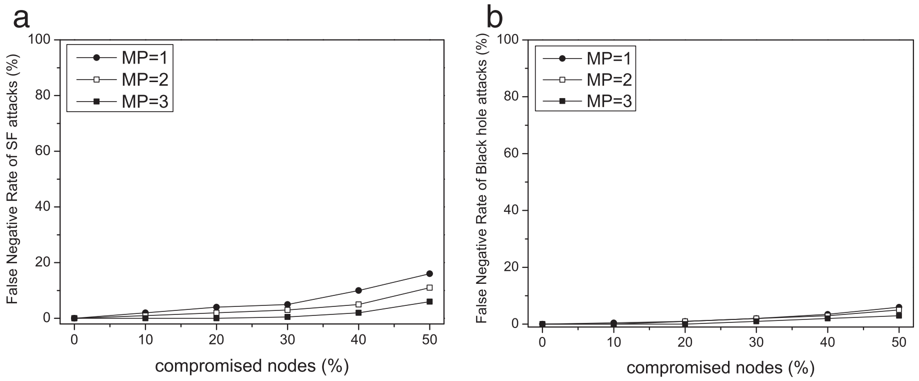

Figure 6 False-negative rate when detecting (a) selective forwarding attacks and (b) black hole attacks.

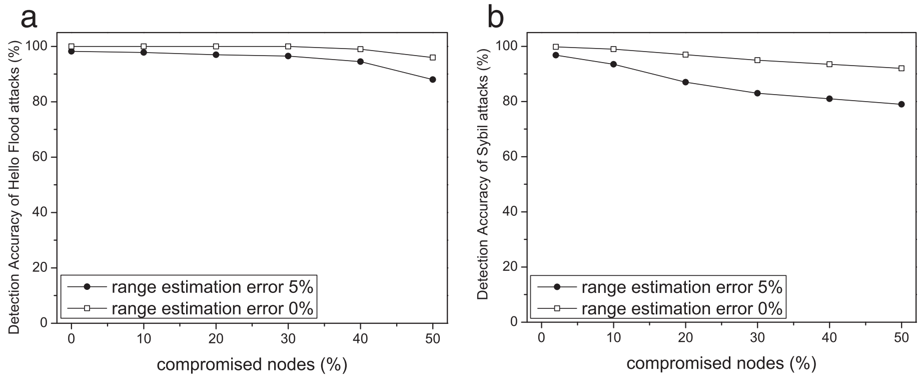

Figure 7 Detection accuracy of (a) hello flood attacks and (b) Sybil attacks.

distance measurements resembling ranging attacks that went undetected. When the range estimation error ϵ_r is equal to 0%, the detection was always close to 100%, notably because of the rule being applied to detect this kind of attack. Another factor that keeps the detection levels high in this case is that these attacks are not mistaken with occasional network or communication failures, as the previous attack category, and as such, fewer false negatives are generated as shown in Figure 8a. However, an increase in the number of misdetections is obtained in two cases. Firstly, when half or more of the network nodes behave maliciously. In this case, the majority-vote rule being applied fails to prevail. Secondly, when inaccuracies are introduced in the UWB range estimates, namely, when ϵ_r is up to 5%. Recall that in these attacks, the rule being applied depends on the distance measurements. Hence, when range estimation errors exist, the detection effectiveness of the ADLU algorithm drops.

Similar to the previous attack scenario, the accuracy in detecting Sybil attacks depends on the accuracy of the UWB distance measurements. As shown in Figure 7b, the detection accuracy of Sybil attacks ranges between 99% and 78.8%. The drop in the detection accuracy is higher when compared to the previous attack scenario. This is actually an indication of the higher dependence between the rule being applied to detect this kind of attack and the distance estimation error, ϵ_r. Apparently, the distance-matching criterion could not be satisfied when inaccuracies in the range estimates, ϵ_r, are introduced. Following this observation, we then relaxed the matching criterion and adjusted the rule, taking into account errors in the distance estimation in the order of 2%. By doing this, we slightly reduced the number of generated false negatives (see Figure 8b).

5 Conclusions

In this paper, we presented an anomaly detection and localization algorithm specifically designed for hierarchical, cluster-based UWB wireless sensor networks. A novel, trust-aware leader election metric was defined to secure the algorithm's cluster formation protocol. The simulation results showed that the proposed algorithm achieves high detection accuracy and low false-negative rates while maintaining the communication overhead at low levels.

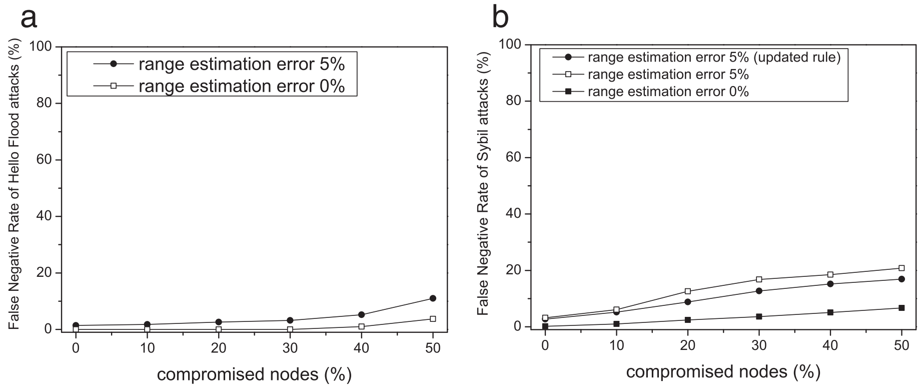

Figure 8 False-negative rate when detecting (a) hello flood attacks and (b) Sybil attacks.

In the future, we intend to examine the effectiveness of the ADLU algorithm in detail by considering larger networks as well as the presence of malicious nodes heavily interfering with the UWB ranging process.

Endnotes

[a]The packets used for ranging estimation are standard packets, with the only difference being the value of a specific bit in the PHY header (PHR) called the 'ranging bit', which is set by the transmitting PHY for frames intended for ranging. A UWB frame with the ranging bit set to 1 is called a ranging frame (RFRAME). There is nothing else, beyond the ranging bit, that makes an RFRAME unique. RFRAMEs can carry data or can even be acknowledgments.

[b]Note that the choice of the N_u parameter may affect the operation of ADLU. As such, we have run multiple simulation tests to fine-tune this metric prior to selecting its final value.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

This work was performed within the framework of the Action 'Supporting Postdoctoral Researchers' of the Operational Programme 'Education and Lifelong Learning' (Actions Beneficiary: General Secretariat for Research and Technology, GSRT), and is co-financed by the European Social Fund (ESF) and the Greek State.

Received: 25 July 2013 Accepted: 27 December 2013
Published: 17 January 2014

References

1. IEEE, *IEEE 802.15.4™-2011*: IEEE Standard for Local and Metropolitan Area Networks–Part 15. 4: Low-Rate Wireless Personal Area Networks (LR-WPANs). (IEEE, Piscataway, 2011)
2. E Karapistoli, FN Pavlidou, I Gragopoulos, I Tsetsinas, An overview of the IEEE 802.15.4a Standard. Commun. Mag. IEEE. **48**(1), 47–53 (2010)
3. N Sastry, D Wagner, Security considerations for IEEE 802.15.4 networks. Paper presented at the 3rd ACM workshop on wireless security (WiSe), Philadelphia, PA, USA, 1 Oct 2004, pp. 32–42
4. C Karlof, D Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures. Paper presented at the first IEEE international workshop on sensor network protocols and applications, Anchorage, AK, USA 11 May 2003, pp. 113–127
5. D Martins, H Guyennet, Wireless sensor network attacks and security mechanisms—A short survey. Paper presented at 13th international conference on network-based information systems (NBiS), Takayama, Japan, 14–16 Sept 2010, 313–320
6. K Xing, S Srinivasan, M Rivera, J Li, X Cheng, ed. by SCH Huang, D MacCallum, and D-Z Du, Attacks and countermeasures in sensor networks: A survey, in *Network Security* (Springer, New York, 2010), pp. 251–272
7. S Ghose, R Bose, Physical layer security in UWB networks. Paper presented at the IEEE international conference on microwaves, communications, antennas and electronics systems (COMCAS), Tel Aviv, 7–9 Nov 2011, pp. 1–5
8. M Ko, D Goeckel, Wireless physical-layer security performance of UWB systems. Paper presented at the military communications conference (MILCOM), San Jose, CA, USA 31 Oct–3 Nov 3 2010, pp. 2143–2148
9. SA Camtepe, B Yener, Key distribution mechanisms for wireless sensor networks: A survey. Technical report, Rensselaer Polytechnic Institute, 2005
10. E Shi, A Perrig, Designing secure sensor networks. IEEE Wireless Commun. Mag. **11**(6), 38–43 (2004)
11. L Lazos, R Poovendran, SeRLoc: Robust localization for wireless sensor networks. ACM Trans. Sensor Netw. (TOSN). **1**, 73–100 (2005)
12. S Roy, M Conti, S Setia, S Jajodia, Secure data aggregation in wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **7**(3), 1040–1052 (2012)
13. M Flury, M Poturalski, P Papadimitratos, JP Hubaux, JY Le Boudec, Effectiveness of distance-decreasing attacks against impulse radio ranging. Paper presented at the third ACM conference on wireless network security (WiSec). Hoboken, NJ, USA, 22–24 March 2010, pp. 117–128
14. N Tippenhauer, S Capkun, ID-based secure distance bounding and localization. ESORICS. **5789**, 621–636 (2010)
15. Y Wang, X Ma, G Leus, An UWB ranging-based localization strategy with internal attack immunity. ICUWB. **2**, 1–4 (2010)
16. Y Zhang, W Liu, Y Fang, D Wu, Secure localization and authentication in ultra-wideband sensor networks. IEEE J. Select. Areas Commun. **24**(4), 829–835 (2006)
17. YH Jazyah, M Hope, ed. by D Taniar, O Gervasi, B Murgante, E Pardede, and BO Apduhan, A review of routing protocols for UWB MANETs, in *Proceedings of the 2010 International Conference on Computational Science and Its Applications, Part III* (Springer, Berlin, 2010), pp. 228–245
18. A Becher, Z Benenson, M Dornseif, ed. by J Clark, R Paige, Polack F, and P Brooke, Tampering with motes: Real-world physical attacks on wireless sensor networks, in *Security in Pervasive Computing, Lecture Notes in Computer Science, vol. 3934* (Springer, Berlin, 2006), pp. 104–118
19. A Farooqi, F Khan, ed. by Slezak D, T Kim, AC Chang, T Vasilakos, M Li, and Sakurai Kouichi, Intrusion detection systems for wireless sensor networks: A survey, in *Communication and Networking, vol. 56* (Springer, Berlin, 2009), pp. 234–241
20. M Xie, S Han, B Tian, S Parvin, Anomaly detection in wireless sensor networks: A survey. J Netw. Comput. Appl. **34**(4), 1302–1325 (2011)
21. V Chandola, A Banerjee, V Kumar, Anomaly detection: A survey. ACM Comput. Surv. **41**(3), 15:1–15:58 (2009)
22. Z Sahinoglu, S Gezici, Ranging in the IEEE 802.15.4a Standard. Paper presented at the IEEE annual conference on wireless and microwave technology (WAMICON), Clearwater Beach, FL, USA, 4–5 Dec 2006, pp. 1–5
23. CC Su, KM Chang, YH Kuo, MF Horng, The new intrusion prevention and detection approaches for clustering-based sensor networks. WCNC. **4**, 1927–193 (2005)
24. S Rajasegarar, C Leckie, M Palaniswami, J Bezdek, Distributed anomaly detection in wireless sensor networks. Paper presented at the 10th IEEE international conference on communication systems (ICCS), Singapore, 30 Oct–2 Nov 2006, pp. 1–5
25. S Subramaniam, T Palpanas, D Papadopoulos, V Kalogeraki, D Gunopulos, Online outlier detection in sensor data using non-parametric models. Paper presented at the 32nd international conference on very large data bases (VLDB), Seoul, South Korea, 12–15 Sept 2006, pp. 187–198
26. H Wang, Z Yuan, C Wang, Intrusion detection for wireless sensor networks based on multi-agent and refined clustering. CMC. **3**, 450–454 (2009)
27. YY Zhang, W-C Yang, K-B Kim, M-S Park, Inside attacker detection in hierarchical wireless sensor network. Paper presented at the 3rd international conference on innovative computing information and control (ICICIC). Dalian, Liaoning, 18–20 June 2008, pp. 594–594
28. K Rahul, H Liu, HH Chen, Reduced complexity intrusion detection in sensor networks using genetic algorithm. Paper presented at the IEEE international conference on communications, Dresden, Germany, 14–18 June 2009, pp 1–5
29. S Rajasegarar, C Leckie, M Palaniswami, J Bezdek, Quarter sphere based distributed anomaly detection in wireless sensor networks. Paper presented at the IEEE international conference on communications, Glasgow, 24–28 June 2007, pp. 3864–3869
30. IM Atakli, H Hu, Y Chen, WS Ku, Z Su, Malicious node detection in wireless sensor networks using weighted trust evaluation. Paper presented at the spring simulation multiconference (SpringSim), Ottawa, Canada, 14–17 Apr 2008, pp 836–843
31. I Krontiris, T Dimitriou, FC Freiling, Towards intrusion detection in wireless sensor networks. Paper presented at the 13th European wireless conference, Paris, France, 1–4 Apr 2007
32. M Poturalski, M Flury, P Papadimitratos, JP Hubaux, JY Le Boudec, Distance bounding with IEEE 802.15.4a: Attacks and countermeasures. IEEE Trans. Wireless Commun. **10**(4), 1334–1344 (2011)

33. G Koltsidas, E Karapistoli, FN Pavlidou, An energy-aware self-organizing clustering algorithm for UWB wireless sensor networks. Paper presented at the IEEE 19th international symposium on personal, indoor and mobile radio communications (PIMRC). Cannes, 15–18 Sept 2008, pp. 1–5
34. L Bysani, A Turuk, A survey on selective forwarding attack in wireless sensor networks. Paper presented at the international conference on devices and communications (ICDeCom), Mesra, Algeria, 24–25 Feb 2011, pp. 1–5
35. I Krontiris, T Giannetsos, T Dimitriou, Launching a sinkhole attack in wireless sensor networks: The intruder side. Paper presented at the IEEE international conference on wireless and mobile computing, networking and communication, Avignon, France, 12–14 Oct 2008, pp. 526–531
36. J Newsome, E Shi, D Song, A Perrig, The Sybil attack in sensor networks: Analysis defenses. Paper presented at the third international symposium on information processing in sensor networks. Berkeley, California, USA, 26–27 Apr 2004, pp. 259–268
37. S Gezici, Z Tian, G Giannakis, H Kobayashi, A Molisch, H Poor, Z Sahinoglu, Localization via ultra-wideband radios: A look at positioning aspects for future sensor networks. Signal Process Mag. IEEE. **22**(4), 70–84 (2005)

doi:10.1186/1687-417X-2014-3
Cite this article as: Karapistoli and Economides: **ADLU: a novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks.** *EURASIP Journal on Information Security* 2014 **2014**:3.