R. Rios, and J. Lopez, "Exploiting Context-Awareness to Enhance Source-Location Privacy in Wireless Sensor Networks", *The Computer Journal*, vol. 54, pp. 1603-1615, 2011.
http://doi.org/10.1093/comjnl/bxr055
NICS Lab. Publications: https://www.nics.uma.es/publications

Exploiting Context-Awareness to Enhance Source-Location Privacy in Wireless Sensor Networks

Ruben Rios and Javier Lopez

Computer Science Department, University of Malaga, Spain
Email: ruben@lcc.uma.es

The source-location privacy problem in Wireless Sensor Networks has been traditionally tackled by the creation of random routes for every packet transmitted from the source nodes to the base station. These schemes provide a considerable protection level at a high cost in terms of message delivery time and energy consumption. This overhead is due to the fact that the data routing process is done in a blind way, without knowledge about the location of the attacker. In this work we propose the Context-Aware Location Privacy (CALP) approach, which takes advantage of the ability of sensor nodes to perceive the presence of a mobile adversary in their vicinity in order to transmit data packets in a more energy-efficient and privacy-preserving manner. In particular we apply the concepts of CALP to the development of a shortest-path CALP routing algorithm. A permissive and a strict version of the protocol are studied for different adversarial models and the proposed schemes are evaluated through simulation experiments in terms of privacy protection and energy consumption. Finally, we conclude the paper and present possible extensions of this work.

Keywords: Context-Awareness; Location Privacy; Wireless Sensor Networks

Received 00 January 2009; revised 00 Month 2009

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are comprised of a large number of small, costless devices (sensor nodes or motes) which are able to monitor the physical phenomena taking place in their vicinity and to wirelessly communicate these data to a high-capacity device (base station or sink) with the ability to process and analyse all the collected information. In this way, WSNs might resemble living organisms since they are capable of getting stimuli from their surroundings and processing that information in order to eventually perform some action. Under this metaphoric view of WSNs, sensor nodes represent the senses, the communication channels can be regarded as the nerves, and the base station depicts the brain.

The various types of sensors that might be coupled to a sensor node are extensive, such as temperature, humidity, pressure, acoustic, and radiation sensors [1, 2]. This makes WSNs a rather versatile technology capable of performing many diverse tasks which, together with the low cost and size of the devices, becomes the ideal technology for monitoring diverse environments and assets. Precisely, this reason makes WSNs suitable for many different areas, namely air quality monitoring and environmental data collection, efficient crops management, detection and prevention of forest fires, homeland security, healthcare, and industrial processes monitoring, among many other.

The imminent widespread of WSNs is drawing the attention of the privacy community due to their exceptional ability to collect large amounts of information about individuals without them even noticing it. However, there are also network privacy considerations that might leak information about the network itself [3]. In particular, the location of the events being monitored (i.e. the source location) is an extremely valuable information that must be kept safe from potential adversaries, which in possession of such knowledge become very powerful. To exemplify the criticality of this problem consider a WSN deployed in a nuclear plant to monitor the levels of radiation and thus keep control of possible leaks. An attacker might benefit from the already deployed infrastructure to determine the location of radioactive materials.

This is a challenging problem because even in the presence of message confidentiality mechanisms, an adversary is capable of obtaining sensitive information. In addition, the extreme resource limitation of the sensor nodes further complicates the problem. Consequently, most of the works dealing with source-

location privacy in WSNs have focused on randomly sending every packet on a different route in order to minimize the chances of an attacker finding the source of the messages. However, sending packets on randomly chosen paths does not always reduce the likelihood of the attacker reaching the source of events since truly random paths are difficult to achieve [4]. Thus, the protection level provided by these solutions could be unleashed if we consider that sensor nodes have the ability to feel their environment.

The main contribution of this work is the CALP (Context-Aware Location Privacy) approach. CALP takes advantage of sensor nodes' context-awareness in order to detect the presence of a mobile adversary in their surroundings so that packets are routed in a more efficient and privacy preserving manner. The solution aims to anticipate the movements of the attacker in order to minimize the number of packets he is able to capture and analyse, hence reducing the likelihood of the attacker finding the source. Moreover, the protection mechanism will be in operation only when the attacker is moving in the field. Since the network is expected to be free from threats most of the time, the use of CALP translates into a significant reduction of the incurred overhead compared to previous source-location privacy solutions.

Therefore, the CALP approach is suitable for application scenarios where the detection of moving objects in the field is among the various tasks of the sensors nodes. Many of such scenarios exist such as country perimeter control, battlefield surveillance, and endangered animal monitoring. Moreover, it is also necessary to discriminate between adversaries and authorised users or other moving objects. A straightforward solution to the discrimination problem is to launch a challenge-response authentication mechanism [5, 6] once a moving object has been detected. A target in the field unable to authenticate itself to the network, either because it carries no transmitter or because it ignores a shared secret, is considered an intruder. Consequently, the privacy preservation mechanism is activated.

The remainder of this paper is organized as follows. Sec. 2 gives an overview of the most relevant works in the area of source-location privacy in the presence of local adversaries. Next, we describe the network and threat model under consideration in Sec. 3. The main components of the CALP approach are described in detail in Sec. 4. Sec. 5 presents the implementation of the shortest-path CALP routing algorithm, which combines the CALP approach with an energy-efficient routing algorithm. Subsequently, the shortest-path CALP routing is evaluated through simulation experiments in Sec. 6. Finally, we conclude the paper and provide various possible extensions to this work in Sec. 7.

2. RELATED WORK

The source-location privacy problem in WSNs was first considered by Ozturk et al. [7]. They analysed several routing protocols widely used in WSNs and found out that they provide a poor protection level. To reduce this threat, they devised a set of two-phase protocols known as Phantom Routing [7, 8]. Firstly, every new packet travels h hops in either a random or directed walk to a phantom source. From the phantom source the packet is forwarded to the base station either by using a (baseline or probabilistic) flooding or a single-path routing.

Several solutions were devised to reduce some of the limitations in Phantom Routing. A two-way greedy random walk routing is proposed in [9] to reduce the problem of pure random walks staying close to the source. Additionally, increasing the length of the random walks does not necessarily improve the protection level because the phantom source might be placed close to the direct line from the base station to the source. To overcome this new problem, the authors in [4] prioritize the selection of the phantom sources with larger inclination angles.

Different new approaches to the source-location privacy problem were also presented. The Random Parallel routing [10] pre-assigns every sensor n parallel paths to the base station. These parallel paths are fixed and randomly chosen so that the attacker is forced to stay in one of them to trace back the source. Also, in [11] a set of traps in the form of network loops are created to keep the adversary away from the source. Additionally, Shao et al. [12] present a cross-layer approach, which takes advantage of beacon frames to covertly send data. After h hops the beacon reaches a pivot node from where the data is extracted and normally routed to the base station.

All the presented solutions provide an adequate level of protection to the source node against a local eavesdropper. However, they usually introduce a significant overhead to the network. Better results in terms of network efficiency (i.e. delivery time and energy consumption) and privacy protection level might be obtained if we take advantage of the ability of the network to detect the presence of the attacker in its surroundings.

3. PROBLEM STATEMENT

This section will present the main assumptions as well as the network model together with the features that define the type of attacker under consideration.

3.1. Network Model

We consider a fully-connected WSN comprised of n sensor nodes which are uniformly and randomly distributed in a field. Sensor nodes cover a large area so that the attacker has no visual information about

the network topology unless he is close enough to a node. Also, the nodes could be hidden to avoid visual recognition.

Every node in the network is assumed to have the ability to feel the physical phenomena occurring in its vicinity. This feature not only includes the collection of temperature, humidity and other environmental conditions but also considers the ability to detect the presence of moving objects in the field. This can be done by means of one or various types of sensors such as infrared, acoustic, thermal, and magnetic sensors. Also, as shown in [13] and [14], the location of transceiver-free moving objects can be estimated due to the interferences they cause in the radio signal strength at several network nodes.

Also, we assume that all exchanged messages must appear to be indistinguishable to an external observer. Moreover, the headers contain no information which might reveal the identity of the real sources of data. This can be achieved by using semantically secure encryption algorithms for the payload and pseudonyms schemes for the headers [15, 16].

3.2. Threat Model

The adversarial model considered in this work is a passive, external attacker with local eavesdropping capabilities. By passive we mean that the adversary does not interfere with the normal operation of the network. When referring to external we consider that the adversary is not able to compromise or control sensor nodes. Moreover, according to the eavesdropping capabilities, a local adversary has only a limited hearing range, similar to that of sensor nodes. This must not be regarded as a strong assumption since the network model under consideration is intended to cover large areas.

Also, contrarily to traditional attackers considered in [17, 18], the adversary is able to move in the direction of received packets. An attacker is able to determine the angle of arrival of a signal, for example by measuring the difference in received phase at each element of an antenna array [19], what finally allows him to find the source of a packet. Besides, we assume that the attacker is able to move at a reasonable speed but never exceeds the time it takes for a packet to reach a neighbouring node. Thus the speed of the attacker is not a critical factor, although it influences the response time of our scheme.

The attacker might start to monitor the communications either from an internal random position or, more naturally, from the edge of the network. Moreover, he might follow two different strategies, either to be patient or inquisitive. In the first case, he waits until he overhears a packet, while in the latter, he continuously moves at random until he finds a transmitting node, in which case he moves towards that direction and waits until he receives another packet. After a period of time without overhearing any packets, the inquisitive adversary starts to move again in search of new packets.

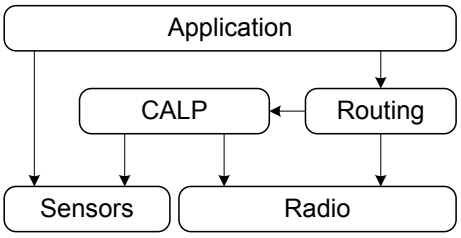


FIGURE 1. Components Interdependence

4. CONTEXT-AWARE LOCATION PRIVACY

This section provides the details of the Context-Aware Location Privacy scheme. The underlying idea of CALP is to anticipate to the movements of the attacker in order to decrease the number of packets he might capture and thus reduce the probability of the attacker finding the source node. To that end, it is necessary to take advantage of the ability of sensor nodes to perceive the existence of moving objects in their vicinity. Upon the detection of such an event, nodes react by broadcasting a route update message to its neighbouring nodes. This message might be forwarded several hops from the position of the attacker and thus it allows sensor nodes to modify their routing tables in order to circumvent the region under the control of the adversary.

4.1. Software Components

The Context-Aware Location Privacy scheme can be seen as a software component which integrates into the sensor nodes to provide the network with the privacy-aware functionality. In Figure 1 we show how this software component interacts with other components, where an outgoing arrow means that the component uses some of the functionality provided by the component receiving the arrow. Therefore, a simple monitoring Application could use the Sensors component to measure the physical conditions and a Routing component to send the information to the base station. Additionally, the Routing component uses the Radio component to send the data through the wireless interface and might use the CALP component to make decisions on the next hop of the communication, thus allowing the sensor nodes to adapt their routing strategy depending on the privacy needs. Finally, the CALP component could use either the Sensors component or the Radio Component, or both, to detect the presence of adversaries.

4.2. Adversary Recognition

Prior to the route update process it is necessary for the network to sound the area in case there is an adversary around. For this reason we consider the CALP approach to be suitable for application scenarios where among the tasks performed by the sensor nodes is the surveillance of moving objects in the field. The monitoring of endangered species, the surveillance of country borders, mineral deposits or oil and gas fields are typical scenarios where sensor nodes already incorporate the object tracking functionality. Most of these scenarios are highly sensitive to the presence of intruders and the authorised-personnel-only policy must be enforced. The use of traditional radio-based localisation methods [19], where the target object carries a transmitter or transceiver whose radio signals are analysed to determine its location, are not suitable for such critical scenarios because an intruder might not have such device or can simply drop it. Also, physical barriers has been a means of protection but in some cases, such as country perimeter surveillance, this might be highly costly or even infeasible. Given such circumstances, the use of WSNs capable of detecting and tracking objects crossing the area under study are of great interest [20, 21, 22, 23]. To that end, the nodes comprising the network can be equipped with motion sensors or they might measure the interferences in the signal strength of the radio signals.

The aforementioned techniques allow sensor nodes to determine the existence of mobile targets in their vicinity. However, these techniques on their own provide no means to discriminate between adversaries and authorised users or other moving objects. As a matter of fact, being able to distinguish adversaries from other mobile entities is not a trivial task. The only difference the sensor network might notice is between entities authorised to move around the field (e.g. those being monitored or network administrators) and other moving objects, which might be either adversaries or not. Therefore, the best strategy for the sensor network is to consider that any non-authorised moving object is an adversary although, ideally, the protection mechanism should be launched only in the presence of adversaries in order to reduce the extra overhead due to the performance of the privacy-aware routing mechanism.

Consider, for example, a sensor network which monitors the behaviour of an endangered animal species. Such network needs to be able to distinguish between different species so that it collects only relevant information concerning the protected species. This can be done in several different ways, for example, by tagging the animals with some sort of wireless device (e.g. an under-skin sensor node) being able to broadcast authenticated information regarding a specific animal. Also, biologists might carry their own personal devices in order to be recognized as authorised users. On the other hand, other animal species or adversaries willing to capture the protected animals would launch the protection mechanism since they are not in possession of an authenticated device.

A simple challenge-response protocol might allow the interaction of external authorised entities with the sensor network. After authentication, a temporal session key might be established between the sensor network and the external entity in such a way that this entity is able to securely transmit messages to the sensor network. Clearly, the session key must be occasionally updated. This process may require the use of public key (PK) operations. Several solutions to the user authentication problem have been devised [5, 24, 6, 25]. Also, similar solutions exist for unattended WSNs, where the sink visits the field sporadically to collect data from every single node [26]. Doubtlessly, the advances in Elliptic Curve Cryptography (ECC) will not only simplify the process but also reduce the overhead introduced by the use of authentication mechanisms.

4.3. Route Update Process

Upon the detection of an adversary in the proximities of the network, the privacy-preservation mechanism is triggered. The sensor or sensors nodes noticing the presence of an adversary inform their neighbouring nodes about this situation in order to prevent packets from traversing the area where the adversary is located. Moreover, as the adversary is capable of moving in any direction, it is necessary to anticipate his movements in order to minimize the number of packets he might be able to capture. Thus, the alerting mechanism needs to expand over several hops so that not only neighbours in a close range from the attacker are aware of the distance with respect to the adversary. Figure 2 depicts a sensor network comprised of $n \times n$ sensor nodes ($n = 50$) in which some of the nodes have detected the presence of adversaries and have informed about it to their neighbours. Clearly, the number of hops the alert must span depends on the ability of the attacker to monitor the communications. The more powerful the attacker is, the larger the radio of the area covered by the routing update message must encompass.

The power of the attacker can be measured by two not mutually exclusive means. First, the communications area the attacker is able to monitor. In this work, we focus on mote-class attackers, which are capable of eavesdropping and analysing the traffic on a region equivalent to that of any regular sensor node (r). This feature is also dependent on the size of the network since a large network is less vulnerable to an attacker with a hearing range of r than a network covering a small region. Also, the speed of the attacker influences the area covered by the update process. An attacker moving at an infinite speed has the ability to capture every packet in the network. Obviously, this type of attacker

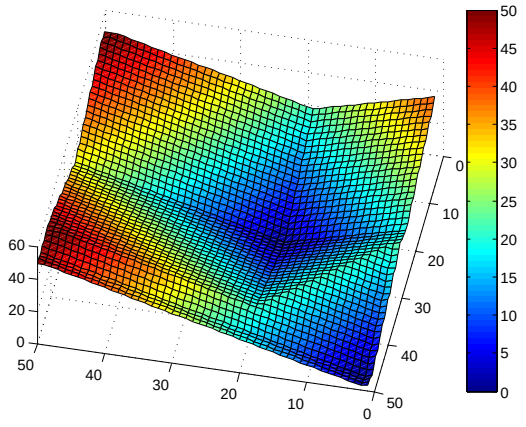


FIGURE 2. Distance of sensor nodes with respect to two adversaries

is out of the scope of our solution. We assume that the network is sufficiently agile to reconfigure the routing tables before the attacker reaches the next neighbouring node. In fact, this is not such a strong assumption since the time of flight of packets between contiguous nodes and the processing time of packets can be considered negligible.

Consequently, when a detector node sends a route update message to its neighbours, this message contains information regarding the distance at which the attacker is placed. In general, the number of hops is a good indicator of the distance if the sensor network is uniformly deployed, though more sophisticated devices might provide more accurate information about the location of the attacker. However, by using a hop-based distance estimation, the route update process is simplified because upon the reception of an update message, the receiving node merely increments the hop count before forwarding the packet and the routing table is modified in consequence without having to perform any further calculations to determine the distance between the node and the adversary.

Furthermore, the route update messages provide the adversary no information about the location of the source nodes because they are exchanged independently of the presence of events in the proximities of the network. In fact, these messages could be either sent periodically or just in the presence of adversaries. Consequently, in order to extend the lifetime of the network, it is recommended that alert messages are sent only upon the detection of an adversary. Also, since beacon frames are periodically broadcast for configuration purposes (regardless of the existence of events), we might take advantage of their ability to carry small amounts of data. Beacon frames involve no extra energy consumption to the network and they are able to convey the few bytes of data needed by route update messages to inform about the location of the adversary. Thus, using beacon frames instead of ordinary data packets further reduces energy consumption. However, in a similar way as described in [12], this approach presents some limitations in terms of the delay between two consecutive frames, which ranges from tens of milliseconds to hundreds of seconds. Therefore, there is a trade-off between the energy consumption and the routing update speed, which impacts on the privacy preservation of the source nodes in case of countering rapidly moving adversaries.

4.4. Data forwarding

The data forwarding process is dependent on the underlying routing algorithm used to transmit the event data from the source to the base station. In fact, CALP can be regarded as an add-in component that modifies the routing tables of sensor nodes in such a way that the subsequent nodes in the path are chosen taking into consideration the privacy of the source node. Thus, upon the reception of a data packet directed to the base station, the receptor decides in which direction to forward the message based on the routing algorithm and, additionally, the distance from its neighbours to the attacker.

At least two options exist when sending packets to neighbouring nodes in a close distance to the adversary. One might choose to prohibit sensor nodes to forward packets to those neighbours located at a distance less than a *minimum safety distance* from the adversary, that is, data packets must circumvent the region where the adversary is. Also, instead of simply blocking the arrival of event messages to sensor nodes in the proximities of the adversary, we might choose to further penalize the selection of these nodes with respect to other neighbours outside the established minimum safety distance. We call these two different options the strict and permissive security perimeter.

The use of a *strict* security perimeter has the advantage of ensuring that the attacker will not capture any packets unless he moves fast enough to cover areas at a distance greater than the predefined minimum safety distance because the routing tables have not been updated yet. As previously mentioned in Sec. 3.2, we do not consider such powerful adversaries. Besides, the use of a strict security perimeter presents some drawbacks that might negatively influence the operation of the network. In particular, the larger the minimum safety distance is, the larger the number of hops a packet will traverse in the presence of an adversary in the proximities of the predefined path. Consequently, the overall energy consumption of the network will be also increased. Furthermore, in the case of defending from an adversary placed in the proximities of the base station, a sufficiently large security perimeter might result in the non-reception of the data packets at the destination. The packets might travel among several hops continuously moving back and forth originating network loops. A possible countermeasure is to make senders temporarily store the received data packets

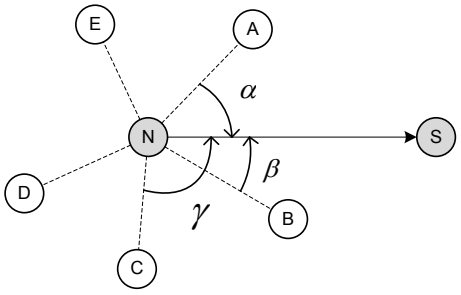


FIGURE 3. Locally optimal neighbour selection

while the adversary is nearby, but if the adversary being countered is patient, i.e. does not move until the reception a data packet, the delivery time would be significantly increased. Also, if the sensor nodes keep on receiving data packets they might run out of memory and this would result in the drop of some packets.

On the other hand, a *permissive* security perimeter avoids the problem of buffering data packets at intermediate sensor nodes in the vicinity of an adversary, thus saving memory and introducing no additional delays in the delivery process. Thus, a permissive minimum safety distance is advisable for non delay-tolerant applications. However, the adversary has better chances to reach the source node since the packets may be forwarded to nodes placed within the hearing range of the adversary.

5. SHORTEST-PATH CALP ROUTING

The CALP protection mechanism can be used in conjunction with different routing protocols to enhance the source-location privacy protection. In this paper we apply CALP to a shortest-path routing algorithm. These are energy-efficient protocols allowing a node to send data packets to a single neighbour, specifically to the node which is geographically closest to the base station. Several shortest- or single-path routing techniques can be found in the literature [27, 28, 29]. Usually, these techniques require that either the sensor nodes are equipped with additional hardware or that an initialization phase is performed.

In particular, the shortest-path routing technique considered in this section makes greedy forwarding decisions since it selects locally optimal neighbours. A neighbour is considered locally optimal when it minimally deviates from the straight line connecting the node and the destination. In Figure 3, N represents the node sending data in the direction to the base station (S) and A, B, C, D, E are the neighbours of N ($neighs(N)$). Also, $\alpha = \angle NAS$, $\beta = \angle NBS$, and $\gamma = \angle NCS$ are the angles formed between the line $\overline{NS}$, and $\overline{NA}$, $\overline{NB}$ and $\overline{NC}$ respectively. For the sake of simplicity only some of the angles have been represented. Thus, X is the locally optimal neighbour of N if $\forall X, Y \in neighs(N) \wedge X \neq Y, \angle NXS \leq \angle NYS$.

The main advantage of implementing a greedy shortest-path technique is that only a small amount of internal storage is required in the nodes to operate. In order to route data packets, a sensor nodes need information about its own neighbours and the location of the base station, but information about other intermediate nodes is not necessary. The main limitation of a greedy approach is that the path followed by the packets might not be globally optimal even though it is locally optimal, i.e. there might exist more efficient paths. Also, due to the limited network topology knowledge of sensor nodes, some packets might not reach their destination when traversing sparse network areas.

When combined with the CALP mechanism, the greedy shortest-path routing technique acquires the ability to anticipate the movements of the adversary in such a way that the number of packets he might be able to capture is significantly reduced. At the same time, the packets will be minimally deviated from the shortest path to the destination, thus the additional energy consumption incurred by the operation of the privacy preservation mechanism is reduced compared to other solutions. Moreover, the use of alternative paths instead of the most energy-efficient one only takes place when the adversary is located close to the shortest path. Figure 4 depicts an scenario where the network adapts the routing path in order to circumvent an adversary moving in the vicinity of the shortest path.

Two versions of the shortest-path CALP routing were devised. In the first version, a strict minimum safety distance is considered. Consequently, the route update messages are used to create an impassable security perimeter which data packets never traverse. Whenever the adversary is located at a distance from the shortest path no longer than the minimum safety distance, data packets will deviate from the original path to avoid crossing the security perimeter. However, in the permissive version, the packets do not necessarily change their itinerary in the case of an adversary placed in the shortest path. Packets are only deviated if the cost associated to performing such choice is greater than the cost of entering the adversary hearing range.

When the adversary is not present in the field, the proposed algorithm must behave as the original shortest-path routing. That is, the locally optimal forwarding neighbour is chosen so that it minimally deviates from the straight line connecting the node and the base station. Therefore, in order to successfully incorporate the CALP functionality, the original protocol operation must not be altered. To that end, the distance to the adversary is used as a penalty value in such a way that the closer the adversary is, the greater the penalty. In particular, we penalize the proximity of a neighbour to the adversary $\frac{\pi}{distance}$. Moreover, depending on whether the version in use is strict or permissive, an additional penalty is introduced when the distance to the adversary is less or equal than

FIGURE 4. Path adaptation depending on the presence of the adversary

Neighs	Angle	Distance
A	$\pi/4$	2
B	$\pi/5$	4
C	$5\pi/9$	5
D	$8\pi/9$	3
E	$11\pi/18$	4

TABLE 1. Routing table of node N

the predefined minimum safety distance. In the strict version, the penalty of sending a packet to a neighbour within the security perimeter is such that any other neighbouring node outside that region is chosen first.

Note that these simple calculations can be performed by any node at a very low cost in terms of additional storage and CPU operations. In particular, Table 1 shows the routing table of node N. The main difference with respect to the traditional approach is that every node requires an additional column in the routing table indicating the distance of a neighbouring node with respect to the adversary. The values in this column are updated upon the reception of the alert messages described in Sec. 4.3.

6. SIMULATION AND RESULTS

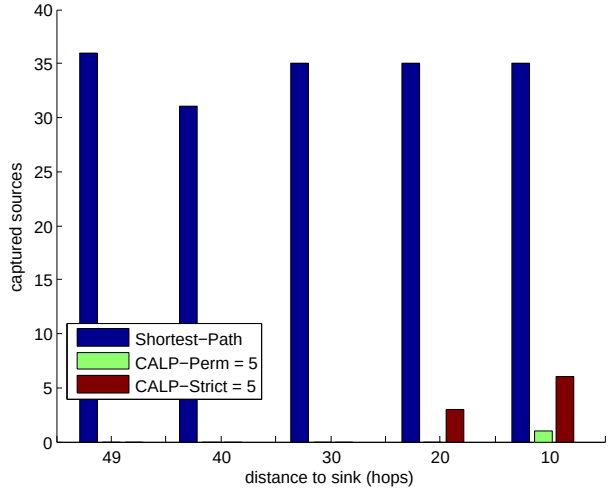
In this section we evaluate the performance and privacy protection level of the proposed shortest-path CALP routing mechanism. We conducted extensive simulations for a uniformly distributed network consisting of $n \times n$ nodes, where $n = 100$. This set up is similar to the ones commonly found in the literature [8, 12]. Every simulation instance is run 50 times and each of them consist of 500 simulation steps. For every simulation step a new message is generated by the source and forwarded by intermediate nodes in its way to the base station. Also, a beaconing phase is scheduled in such a way that the network is aware of the whereabouts of the adversary and thus packets are routed accordingly. Source nodes are placed at different distances from the base station but are static during each simulation. In the first simulation step the adversary is placed in the proximities of the base station, which is located at the centre of the network by default. The adversary under consideration is either inquisitive or patient. The inquisitive adversary moves randomly until he overhears a transmission in his vicinity, in which case he moves in the direction of the received message. If he follows a trace of packets and after a period of time no message arrives to his current position he starts to move randomly in the search of new packets. On the other hand, the patient adversary only moves in the presence of packets in his vicinity. Also, the adversary might move at different paces with respect to the simulation steps, however the adversary speed is considered to be constant within a single simulation. By default, we also consider that the network safety distance is equal to 5. Furthermore, the adversary has a hearing range equivalent to that of a sensor node. Only one adversary is considered to be present at a time in the field although the simulation environment allows for several adversaries. The simulation ends under two circumstances, either when the adversary reaches the source or when the adversary is unable to find the source and the last simulation step is reached.

Note that the simulations were conducted such that the adversary is considered to be in the field at all times. However, in real scenarios this is not the case, the adversary enters and leaves the network at will. Since the devised protection mechanism is only triggered in the presence of the adversary, contrarily to previously proposed schemes, the overall performance of the protocol in terms of energy consumption and delivery time might be significantly reduced.

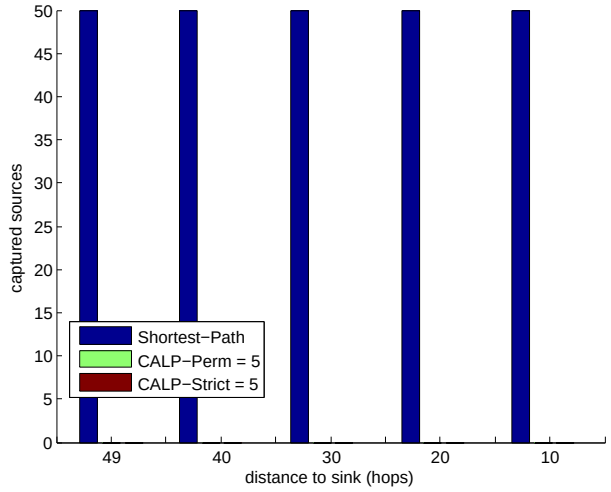
6.1. Privacy Protection

The permissive and strict versions of the shortest-path CALP routing scheme are evaluated in this section. The privacy protection level provided by the different schemes is measured by the number of source nodes the adversary is able to capture for every simulation instance. The two versions of the proposed mechanism are compared between each other and with respect to the traditional shortest-path routing scheme for various source-sink distances. Moreover, the simulations are conducted in the presence of both inquisitive and patient adversaries.

In the case of the shortest-path routing algorithm,



(a) Inquisitive Adversary



(b) Patient Adversary

FIGURE 5. Number of captured sources

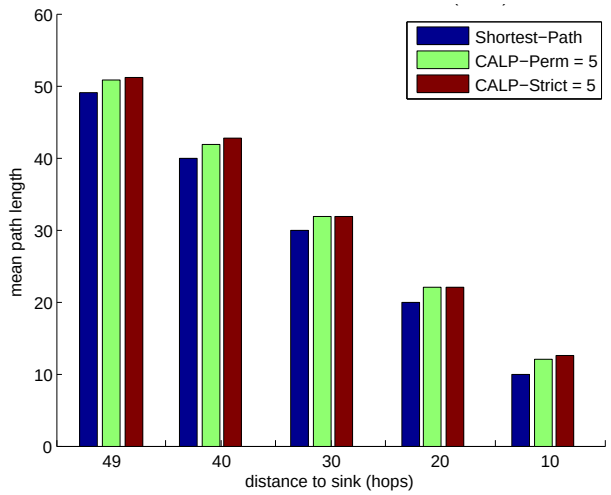
the distance of the source node with respect to the base station, represented in the x axis, has no clear impact. Independently of the distance, the source node is found in roughly the same number of cases. Besides, the patient adversary (see Figure 5b) is more likely to find the source node since he waits next to the base station until he first overhears a packet to follow and since all following packets follow the same path, the adversary easily finds the source node. The main drawback of inquisitive adversaries is that at the beginning of the simulation they might move away from the original location thus missing some of the packets arriving at base the station after several simulation steps, consequently missing the target for the given number of simulation steps.

On the other hand, the proposed scheme only reveals the location of the source node in the presence of an inquisitive adversary when the source-sink distance is rather short (see Figure 5a). Surprisingly, the permissive version of the shortest-path CALP routing provides a better protection level compared to the strict version. The reason is that in the strict version the movements of the adversary are never conditioned by the packets traversing the network since he is not able to overhear them given a sufficiently large safety distance. In particular, the safety distance in Figure 5 is equal to 5. In the permissive version, an inquisitive adversary is able to overhear some of the packets because under certain circumstances the nodes might choose a node within the security perimeter as the next hop. This makes the adversary to move in the direction of the received packet but since the path re-adapts to his movements, he might overhear packets coming from different neighbouring nodes what misleads him from the target. When facing a patient adversary both versions of our protocol never leak location information about the source node. Apparently the packets are able to circumvent the attacker without being detected. In the permissive version the packets might reach the base station by traversing the safety period and thus making the patient adversary move towards the packets and finally allowing the new paths to circumvent the area where he is located and reaching the base station. However, in the strict version, since the adversary is initially placed next to the base station and the packets never traverse the safety region, the packets are never deliver to their destination. This issue is reviewed in more detailed in the following sections.

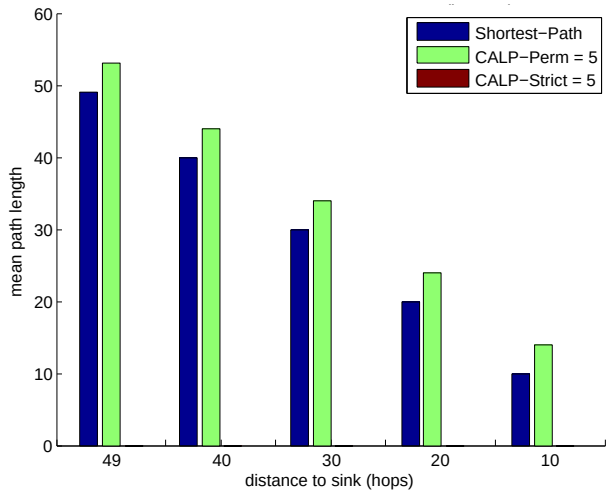
6.2. Protocol Performance

We evaluate the performance of the protocol by means of the length of the resulting routing paths. The length of the path not only determines the delivery time of the packets but also the overall energy consumption of the network. Longer paths result in more transmissions and consequently have a negative impact on the lifetime of the sensor nodes. In general, shortest-path routing algorithms are considered energy efficient algorithms since data packets are usually sent in the shortest path from the source node to the base station. However, shortest-path algorithms provide the lowest protection level since all the packets follow the same (shortest) path. Therefore, the proposed shortest-path CALP routing schemes trade off between performance and privacy protection level.

The results shown in Figure 6 represent the mean path length obtained in the simulations. In general, the mean path length is slightly higher to the minimum expected value, i.e. the value given by the shortest-path routing algorithm. As expected, in the presence of an inquisitive adversary (see Figure 6a), the permissive version of our scheme provides better results than the strict version. On the other hand, for a patient adversary (see Figure 6b), the permissive approach originates paths that are on average slightly longer than those facing an inquisitive adversary. The reason is that for a patient adversary the nodes need to deal



(a) Inquisitive Adversary



(b) Patient Adversary

FIGURE 6. Mean path length

with an adversary waiting in the vicinity of the base station. Moreover, the strict version is unable to create paths that circumvent the patient adversary and deliver the packets to the destination. Since the length of the packets is stored when they arrive at the base station, no data is shown for such scheme in Figure 6b. This problem is not due to the design of the CALP mechanism but to the underlying routing protocol. As mentioned in Sec. 5, due to the limited knowledge about the network topology, packets traversing sparse network areas might not reach their destination. In particular, dealing with a patient adversary in the vicinity of the base station is similar to the problem of reaching isolated nodes in shortest-path routing algorithms.

Although this problem is inherent to shortest-path algorithms, it could be lessen in several different ways depending on the requisites of the network. In a sensor network with no real-time requirements (i.e. tolerate moderate latencies), intermediate nodes could temporarily store the packets until the adversary decides to move away from the base station. However, if the adversary is patient enough, the highly constrained memory of the sensor nodes would require to drop some of the packets. In more time-critical scenarios, a mixed version of both approaches could be used depending on the location of the adversary. Therefore, the permissive version might be used while the adversary is in the vicinity of the base station, i.e. the safety distance prevents the delivery of packets, and when the adversary moves, the strict version might be triggered. Also, the problem could be overcome by dynamically re-adapting the safety distance depending on the whereabouts of the adversary.

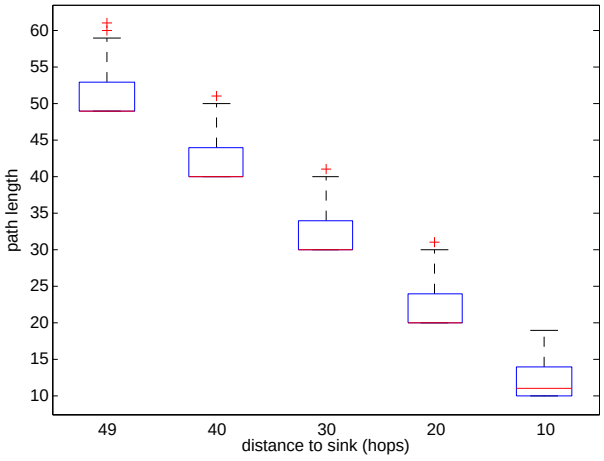
Despite the mean path length is close to the minimum value, some isolated packets traverse a large number of intermediate nodes before being delivered. Figure 7 gives a vivid illustration of the path length distribution due to the occurrence of an inquisitive adversary. This problem is particularly sensitive in the strict version of CALP where some isolated packets travel up to 134 hops before reaching the base station. The reason for such long paths is the creation of network loops due to the presence of the adversary in regions close to the sink. Packets are sent in the direction to the base station but nodes in the border of the safety region cannot send them forward and choose to relay them to other nodes which are in the same situation. Finally the packets are returned to any of the nodes which initially sent those packets. Keeping a list of already seen packets could help to avoid network loops, however, since the adversary is able to move, the next time a node receives the packet the situation might be different, i.e. the direction, which was previously occupied by the adversary, could be now safe.

Although the permissive version presents some isolated paths which are not representative of the distribution (i.e. outliers), these are very few and most of the paths are within the edges of the box, which are the 25^{th} and 75^{th} percentiles. As previously stated, the permissive approach is able to prevent the creation of large paths by allowing the packets to pass through the safety region. Therefore we can claim that the permissive version provides an adequate protection level without incurring an excessive overhead to the network.

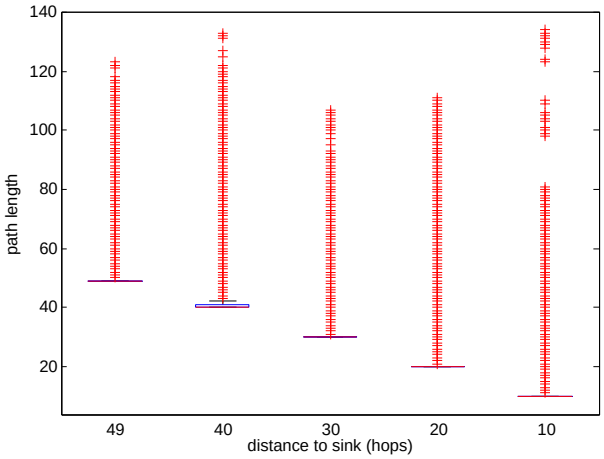
6.3. Safety Distance Impact

In this section we evaluate the impact of the security perimeter size on the privacy protection level and the mean path length. Also, we take into account the distance of the source node with respect to the base station. The adversary considered is an inquisitive adversary. Also, three different security perimeters have been defined, 2, 5, and 7.

As expected, the larger the security perimeter is, the less number of sources the inquisitive adversary is able to capture (see Figure 8). In general, both versions behave well for security perimeters longer than 2. More precisely, the adversary is only able to capture a few

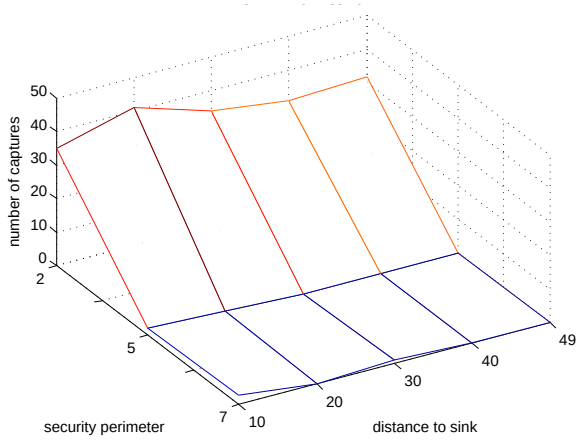


(a) Permissive CALP

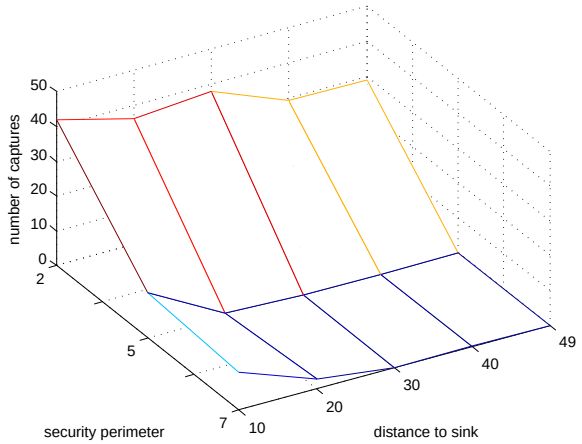


(b) Strict CALP

FIGURE 7. Path length distribution



(a) Permissive CALP



(b) Strict CALP

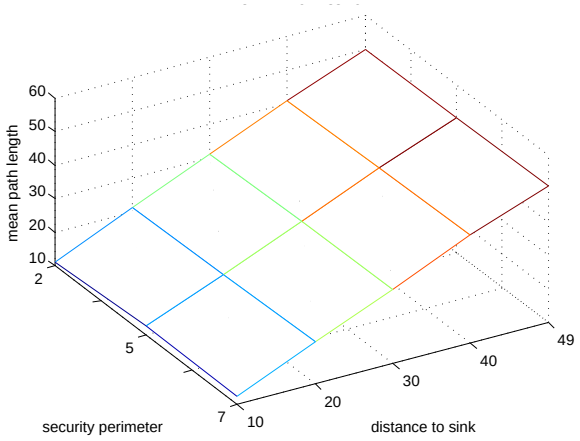
FIGURE 8. Impact on number of captures

packets in the permissive approach (see Figure 8a) when the distance to the base station is not sufficiently large. Also, from Figure 8b we observe that this problem is more pronounced in the strict approach. However, having a security perimeter too small, i.e. equal to 2, does not allow the network to properly readjust the routing paths and thus the adversary is very likely to capture packets, what leads him to the source node. Note that a security perimeter of 0 is equal to having a shortest-path routing algorithm.

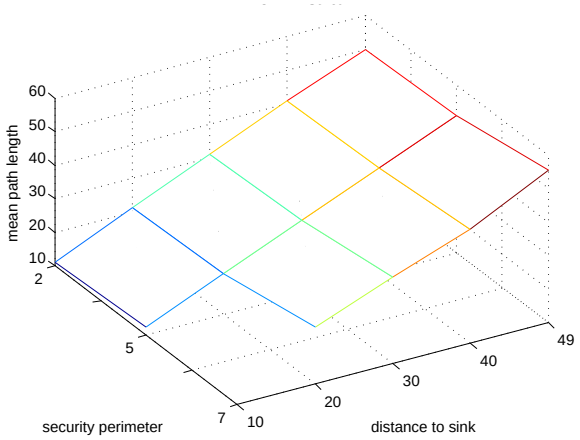
Besides, in Figure 9, we observe that the security perimeter has a small impact on the mean path length. However, there might be some packets traversing an undue number of nodes before reaching their destination, as noted in Sec. 6.2. The strict version is more sensitive to the size of the security perimeter. In particular, using larger security perimeters when the source node is close to base station might result in some executions with no packets reaching their destination. This particular case is depicted in Figure 9b for a security perimeter of 7 and a source node placed at a distance of 10 hops from the base station. To counter the problem of having some packets not reaching their destination, a source-sink distance dependent security perimeter might be used. That is, the security perimeter might be larger as the nodes are further away from the base station. Besides, as the security perimeter size increases, the mean path length increase is more pronounced in the strict version than in the permissive version.

7. CONCLUSIONS AND FUTURE WORK

In this work we present a new approach to source-location privacy in WSNs. Previous solutions were mostly based on the creation of random paths for every single packet transmitted by the source node. These solutions make routing decisions in a blind way in such a way that the paths are independent of the location of the adversary. We propose to take advantage of the inherent capacity of the network to feel what is happening in the field and thus detect the presence of the adversary. Knowing and disseminating information about the whereabouts of the adversary allows the creation of more efficient and privacy-preserving routing. We call this approach CALP, which



(a) Permissive CALP



(b) Strict CALP

FIGURE 9. Impact on mean path length

stands for Context-Aware Location Privacy.

As a matter of fact, CALP can be regarded as a software component to be used in conjunction with some existing routing protocols to enhance the privacy protection level of the events being monitored. In particular, we have developed the shortest-path CALP routing which combines a shortest-path protocol with CALP. More precisely, two versions of the protocol have been developed based on the way data packets are forwarded when an adversary is within a minimum safety distance of the sender. Extensive simulations were conducted for both the strict and permissive versions developed.Moreover, the simulations consider the existence of different types of adversaries, an inquisitive and a patient adversary. The results show that the shortest-path CALP routing scheme provides a solid privacy protection level for source nodes located at various distances from the base station. More precisely, the permissive version provides better results than the strict version when countering an inquisitive adversary. Besides, the average energy consumption is very close values provided by shortest-path routing algorithms. However, in the strict version there might appear some large paths, which implies increased energy consumption as well as increased delivery time. Finally, note that since the CALP protection mechanism is context-aware, the increase in power consumption because use of the protocol takes place only at certain times, i.e in the presence of an adversary. Therefore, the overhead of the presented results could be significantly reduced since the presence of adversaries in the field is unusual.

As future work we will investigate the robustness of the scheme against more skilled adversaries. We will consider an scenario were several external adversaries collude to reduce the privacy protection level of our approach. Also, we intend to extend this work to deal with compromised nodes in the network, which are controlled by an external adversary. Moreover, we will investigate the performance of a mixed version of the permissive and strict CALP routing as well as the dynamic adaptation of the minimum safety distance. Finally, we will study the benefits of a context-aware routing to the protection of receiver-location privacy.

ACKNOWLEDGEMENTS

This work was supported by the by the Ministry of Science and Innovation through the ARES [CSD2007-00004], SPRINT [TIN2009-09237] and IOT-SEC [ACI2009-0949] projects. The SPRINT project is co-financed by FEDER (European Regional Development Fund) and the IOT-SEC project is under the ACI-COLABORA programme.

REFERENCES

[1] Crossbow (2007). MTS/MDA Sensor Board Users Manual.

[2] Libelium (2009). Waspmote - Sensor boards. online.

[3] Pai, S., Bermudez, S., Wicker, S., Meingast, M., Roosta, T., Sastry, S., and Mulligan, D. (2008) Transactional Confidentiality in Sensor Networks. *IEEE Security & Privacy*, **6**, 28–35.

[4] Wei-Ping, W., Liang, C., and Jian-Xin, W. (2008) A source-location privacy protocol in WSN based on locational angle. *ICC '08. IEEE International Conference on Communications*, May, pp. 1630–1634.

[5] Wang, H. and Li, Q. (2006) Distributed user access control in sensor networks. In Gibbons, P., Abdelzaher, T., Aspnes, J., and Rao, R. (eds.), *Distributed Computing in Sensor Systems*, Lecture Notes in Computer Science, **4026**, pp. 305–320. Springer Berlin / Heidelberg.

[6] Vaidya, B., Chen, M., and Rodrigues, J. J. P. C. (2009) Improved robust user authentication scheme for wireless sensor networks. *Wireless Communication and Sensor Networks (WCSN), 2009 Fifth IEEE Conference on*, Allahabad, pp. 1 – 6.

[7] Ozturk, C., Zhang, Y., and Trappe, W. (2004) Source-Location Privacy in Energy-Constrained Sensor Network Routing. *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, New York, NY, USA, pp. 88–93. ACM.

[8] Kamat, P., Zhang, Y., Trappe, W., and Ozturk, C. (2005) Enhancing Source-Location Privacy in Sensor Network Routing. *ICDCS 2005. 25th IEEE International Conference on Distributed Computing Systems*, June, pp. 599–608.

[9] Xi, Y., Schwiebert, L., and Shi, W. (2006) Preserving Source Location Privacy in Monitoring-Based Wireless Sensor Networks. *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*, April 8 pp.

[10] Wang, H., Sheng, B., and Li, Q. (2009) Privacy-aware routing in sensor networks. *Comput. Netw.*, **53**, 1512–1529.

[11] Ouyang, Y., Le, Z., Chen, G., Ford, J., and Makedon, F. (2006) Entrapping Adversaries for Source Protection in Sensor Networks. *WOWMOM '06: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, Washington, DC, USA, pp. 23–34. IEEE Computer Society.

[12] Shao, M., Hu, W., Zhu, S., Cao, G., Krishnamurthy, S., and La Porta, T. (2009) Cross-layer enhanced source location privacy in sensor networks. *IEEE Conference on Sensor, Mesh, and Ad Hoc Communications and Networks (SECON '09)*, June, pp. 1–9. IEEE Communications Society.

[13] Zhang, D., Ma, J., Chen, Q., and Ni, L. M. (2007) An RF-Based System for Tracking Transceiver-free Objects. *Pervasive Computing and Communications, PerCom '07. Fifth Annual IEEE International Conference on*, pp. 135 –144.

[14] Wilson, J. and Patwari, N. (2010) Radio Tomographic Imaging with Wireless Networks. *Mobile Computing, IEEE Transactions on*, **9**, 621 –632.

[15] Misra, S. and Xue, G. (2006) Efficient anonymity schemes for clustered wireless sensor networks. *International Journal of Sensor Networks*, **1**, 50–63.

[16] Ouyang, Y., Le, Z., Xu, Y., Triandopoulos, N., Zhang, S., Ford, J., and Makedon, F. (2007) Providing Anonymity in Wireless Sensor Networks. *Pervasive Services, IEEE International Conference on*, July, pp. 145–148.

[17] Reiter, M. and Rubin, A. (1998) Crowds: Anonymity for Web Transactions. *ACM transactions on information and system security*, **1**, 66–92.

[18] Reed, M., Syverson, P., and Goldschlag, D. (1998) Anonymous Connections and Onion Routing. *Selected Areas in Communications, IEEE Journal on*, **16**, 482–494.

[19] Mao, G., Fidan, B., and Anderson, B. D. (2007) Wireless sensor network localization techniques. *Computer Networks*, **51**, 2529 – 2553.

[20] Aslam, J., Butler, Z., Constantin, F., Crespi, V., Cybenko, G., and Rus, D. (2003) Tracking a Moving Object with a Binary Sensor Network. *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*, New York, NY, USA, pp. 150–161. ACM.

[21] Dousse, O., Tavoularis, C., and Thiran, P. (2006) Delay of Intrusion Detection in Wireless Sensor Networks. *Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing*, New York, NY, USA MobiHoc '06, pp. 155–165. ACM.

[22] Liu, B., Dousse, O., Wang, J., and Saipulla, A. (2008) Strong Barrier Coverage of Wireless Sensor Networks. *Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing*, New York, NY, USA MobiHoc '08, pp. 411–420. ACM.

[23] Lazos, L., Poovendran, R., and Ritcey, J. A. (2009) Analytic Evaluation of Target Detection in Heterogeneous Wireless Sensor Networks. *ACM Trans. Sen. Netw.*, **5**, 1–38.

[24] Jiang, C., Li, B., and Xu, H. (2007) An efficient scheme for user authentication in wireless sensor networks. *Advanced Information Networking and Applications Workshops, International Conference on*, **1**, 438–442.

[25] Cheikhrouhou, O., Koubaa, A., Boujelben, M., and Abid, M. (2010) A lightweight user authentication scheme for wireless sensor networks. *Computer Systems and Applications, ACS/IEEE International Conference on*, **0**, 1–7.

[26] Di Pietro, R., Mancini, L., Soriente, C., Spognardi, A., and Tsudik, G. (2009) Data Security in Unattended Wireless Sensor Networks. *Computers, IEEE Transactions on*, **58**, 1500 –1511.

[27] Intanagonwiwat, C., Govindan, R., Estrin, D., Heidemann, J., and Silva, F. (2003) Directed Diffusion for Wireless Sensor Networking. *IEEE/ACM Trans. Netw.*, **11**, 2–16.

[28] Karp, B. and Kung, H. T. (2000) GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, New York, NY, USA, pp. 243–254. ACM.

[29] Niculescu, D. and Nath, B. (2003) Trajectory Based Forwarding and Its Applications. *MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking*, New York, NY, USA, pp. 260–272. ACM.