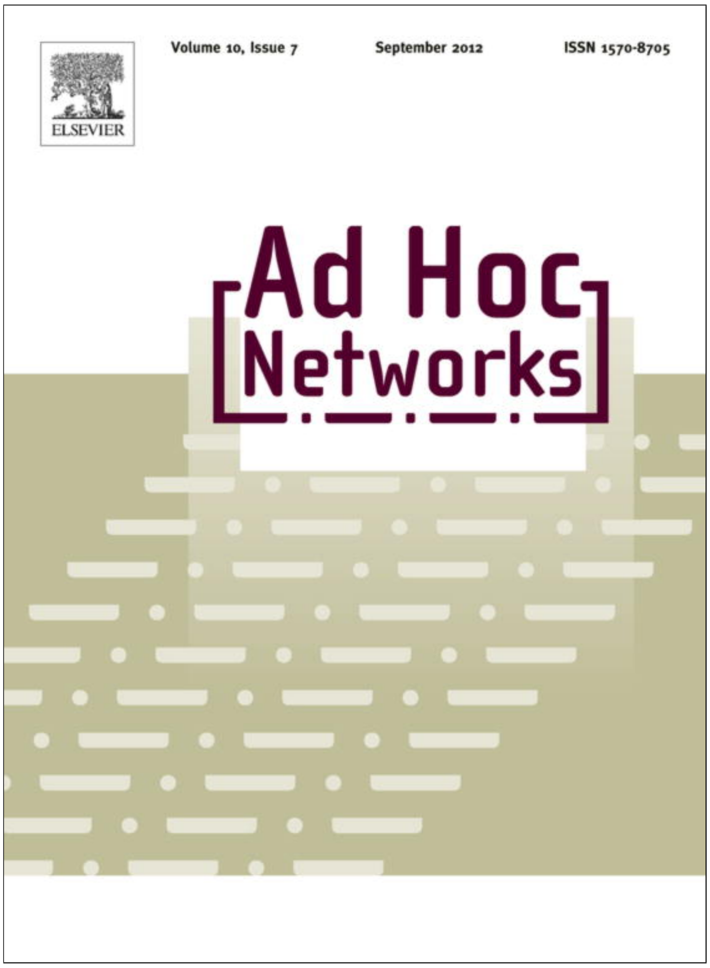

Volume 10, Issue 7
September 2012
ISSN 1570-8705
ELSEVIER
Ad Hoc Networks

Ad Hoc Networks 10 (2012) 1267–1277

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Node localization through physical layer network coding: Bootstrap, security, and accuracy

Zhiwei Li, Weichao Wang *

Department of SIS, UNC Charlotte, Charlotte, NC 28223, United States

ARTICLE INFO

Article history:
Received 12 August 2011
Received in revised form 23 March 2012
Accepted 5 April 2012
Available online 16 April 2012

Keywords:
Physical layer network coding
Node localization
Wireless networks

ABSTRACT

Previous research on physical layer network coding (PNC) focuses on the improvements in bandwidth usage efficiency. Its capability to assist wireless nodes in localization was first discussed in [1]. In that paper, however, the authors discussed only the basic idea to detect and separate the interfered signals for calculating the node positions. Many important issues to turn the idea into a practical approach are not extensively studied. In this paper, we plan to investigate these problems. Specifically, our research focuses on the bootstrap procedures, security, and localization accuracy of the PNC based mechanism. We first study the required node density to bootstrap the localization procedure in both infrastructure-based and self-organized networks. With this question answered, researchers can recognize the network scenarios to which PNC based localization can be applied. We design mechanisms to protect integrity of the exchanged information and defend against node impersonation attacks so that the localization procedures will be robust against malicious activities. For localization accuracy, we study the negative impacts of the position errors of the anchor nodes. We design two mechanisms to reduce the localization inaccuracy for both individual nodes and cumulative procedures through excluding the anchor nodes with positioning errors and introducing multiple bootstrap areas. Both simulation and theoretical analysis are used to support our investigation. This research shows that PNC based node localization can satisfy the security and accuracy requirements of different types of wireless networks and it can be widely deployed.

1. Introduction

With the proliferation of wireless networks and applications, the localization problem attracts a lot of research efforts. Locating the absolute (or relative) positions of the wireless nodes can improve the performance and safety of the networks. For example, the positions of nodes can be used to authenticate the senders [2], enforce access control [3], and detect Sybil attacks [4]. The position information can also enable the deployment of new location-based services [5–7].

Restricted by the application environments or hardware cost, sometimes we cannot equip every wireless node with the positioning devices such as GPS. Under these conditions, localization algorithms will be adopted. Various range-based and range-free localization algorithms have been designed [8–10]. The adopted techniques include Angle of Arrival [11], Received Signal Strength Indicator [12], Time of Arrival [13,14], Time Difference of Arrival [8,15,16], and Hop-based Reconstruction [17]. Many of these approaches depend on some special hardware to estimate the positions of the nodes. The examples include directional antennas [11], synchronized clocks [18], multiple signal sources [19], power level measurement devices [20], and frequency shift detectors [21]. Although the unit price of the hardware can be very low, the extra cost can still restrict the wide adoption of these methods.

Using the physical layer network coding (PNC) technique to achieve node localization was first studied by Li et al. [1].

* Corresponding author.
E-mail address: weichaowang@uncc.edu (W. Wang).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2012.04.001

PNC uses the additive nature of electromagnetic waves to serve as the coding procedure and improve the network efficiency [22–24]. In [1], the proposed approach determines the position of a wireless node by letting the radio signals from two anchor nodes interfere with each other. The wireless node and another anchor node will capture the interfered sequences. The mechanism will then calculate a hyperbola on which the wireless node resides by comparing the starting points of collisions at the two nodes. When multiple hyperbolas are determined, the wireless node will be positioned at the intersection of these lines.

In their paper [1], Li et al. introduce only the basic idea to detect and recover the interfered signals and calculate the time differences. Many important issues for the practicability and wide adoption of the mechanism, however, are left untouched. For example, since we need multiple independent hyperbolas to determine the position of a wireless node, the density and distribution of anchor nodes will directly impact the number of wireless devices that can be positioned. As another example, the properties that can impact the localization accuracy are not investigated. In this paper, we plan to study these problems. Specifically, our research will focus on the bootstrap procedures, security, and localization accuracy of the PNC based mechanism. We plan to study the required node density for the localization procedures in both infrastructure-based and self-organized networks so that most nodes in the network can be positioned. With this question answered, researchers can recognize the network scenarios to which PNC based localization can be applied. We will design mechanisms to protect integrity of the exchanged packets and defend against node impersonation attacks. For localization accuracy, we will study the impacts of the position errors of the anchor nodes on subsequent operations. The security and localization accuracy results will help end users to determine whether or not this approach will satisfy their requirements. Both simulation and theoretical analysis will be used to support our investigation results.

The contributions of the paper can be summarized as follows: First and most importantly, we conduct a comprehensive study of the practicability of PNC based localization from multiple aspects. The required node density to bootstrap the mechanism and the localization accuracy that can be delivered will help end users to determine whether or not it can be adopted by their applications. Second, while previous research on PNC focuses on its capability to improve bandwidth usage efficiency, the localization mechanism will provide a new incentive for further investigation and wide deployment of this technique. Last but not least, although in this paper we present the bootstrap, security, and accuracy schemes as independent methods, they can be smoothly integrated into a system to improve the overall localization results.

The remainder of the paper is organized as follows: In Section 2 we revisit the basic idea of PNC based node localization. The required anchor node density to bootstrap the localization procedures under different network setups is investigated in Section 3. In Section 4, we study the safety of the approach under different attacks. The localization accuracy is studied in Section 5. Finally, Section 6 concludes the paper.

2. Revisit of PNC based localization

2.1. Introduction to PNC

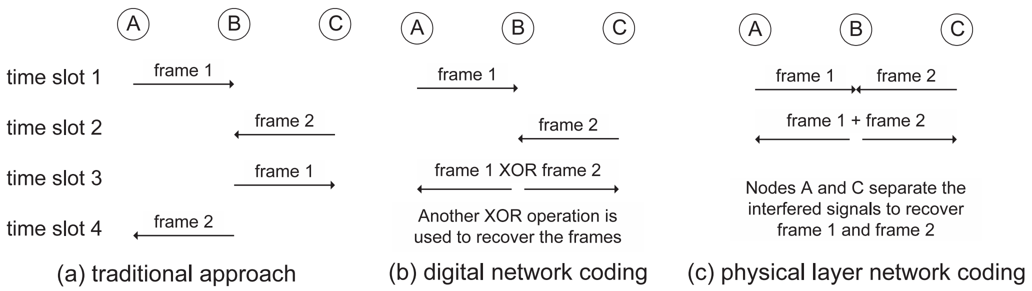
In this part, we introduce the background of physical layer network coding technique. Fig. 1 illustrates the differences among the traditional approach, network layer network coding, and physical layer network coding. In the topology, *A* and *C* depend on *B* to forward the frames between them. In the traditional approach, *A* and *C* need four time slots to exchange a pair of packets. In network layer network coding schemes, node *B* will conduct an XOR operation (or other operations) to combine *frame*1 and *frame*2. Therefore, three time slots are needed for the operations. In the PNC approach, *A* and *C* will send out their packets and *B* will receive the interference results of the two frames. It will rebroadcast the received signals to both *A* and *C* so that they can leverage their knowledge about *frame*1 and *frame*2, respectively to separate the signals and recover the data. From this example, we can see that PNC has the potential to achieve higher bandwidth usage efficiency than network layer network coding. PNC based mechanism does not require the frames to reach the receiver simultaneously since it can accurately locate the starting point of signal collisions [23]. Data transmission using PNC in more complicated network topologies can be found in [23,24].

Since the concept of PNC was proposed in [24], multiple research groups have implemented the approach upon software defined radio (SDR) platforms. In [23], the researchers used the Universal Software Radio Peripheral (USRP) [25] and GNURadio [26] to implement strategic signal-level interference and achieved 500 kb/s bandwidth in the 802.11 frequency range. In [27], the authors implemented multi-relay cooperative communication so that multiple signal sequences from different senders could arrive at the receiver simultaneously. Frequency domain oriented PNC upon the SDR platform was implemented in [28] and significant performance improvements over traditional scheduling and straightforward network coding were achieved. DARPA's Wireless Network after Next (WNaN) program [29] has set a unit cost goal of $500 for a multi-channel SDR device. With the fast development of wireless communication and FPGA techniques, the unit price of the hardware platforms for PNC will become cheaper in the near future.

The PNC technique can co-exist with the traditional wireless communication technique in the same network. It will be transparent to terminals not equipped with corresponding hardware since the devices can identify those interfered sequences through the properties of the received signals. For example, if phase-based modulation is adopted, wireless devices can distinguish among the states of no signal, one signal, and two interfered signals through the perceived power level and its variance [23]. State separation under other signal modulation techniques can be found in [28].

2.2. PNC based node localization

In this part, we introduce the basic idea of using PNC to calculate the position of a wireless node. We use d_{MN} to


A
B
C
time slot 1
time slot 2
time slot 3
time slot 4
frame 1
frame 2
frame 1
frame 2
frame 1 XOR frame 2
Another XOR operation is used to recover the frames
frame 1
frame 2
frame 1 + frame 2
Nodes A and C separate the interfered signals to recover frame 1 and frame 2

(a) traditional approach (b) digital network coding (c) physical layer network coding

Fig. 1. Traditional approach, network layer network coding, and PNC.

represent the distance between two nodes M and N. We use T to represent a specific moment and t to represent a time duration. If radio waves propagate at the speed s, the transmission delay between M and N will be $\frac{d_{MN}}{s}$. In our analysis, we measure the difference between the arriving time of two sequences based on the starting point of signal collisions. We must clarify that we are not using the system clocks in wireless nodes to directly measure the actual time. On the contrary, we can locate the symbol in the sequence from which the collision starts. Then we can translate this information into a time difference based on the frequency of the radio signals.

Fig. 2 illustrates an example of radio signals colliding at wireless receivers. We assume that four nodes A, C, D, and E can receive the signals from each other. We also assume that nodes C,D, and E are anchor nodes and they know their positions. Node A wants to determine its position based on the signal interference results. Two anchor nodes C and D send out signal sequences that will collide at both A and E. Without losing generality, we assume that C starts sending at $T_C = 0$ and D starts sending at $T_D \geqslant 0$.

Therefore, A will receive the sequence from C at $\frac{d_{AC}}{s}$, and the sequence from D at $\left(T_D + \frac{d_{AD}}{s}\right)$. The difference between the arriving time of two sequences is $t_{diffA} = \left(T_D + \frac{d_{AD} - d_{AC}}{s}\right)$. In other words, A will first receive the sequence from C for t_{diffA} seconds, then the two sequences will collide at the node. If $t_{diffA} < 0$, the sequence from D will arrive at A first. Similarly, we can calculate the difference between the arriving time at node E as $t_{diffE} = \left(T_D + \frac{d_{ED} - d_{EC}}{s}\right)$. Now let us look at the difference between t_{diffA} and t_{diffE}:

$$t_{diffE} - t_{diffA} = \left(T_D + \frac{d_{ED} - d_{EC}}{s}\right) - \left(T_D + \frac{d_{AD} - d_{AC}}{s}\right)$$

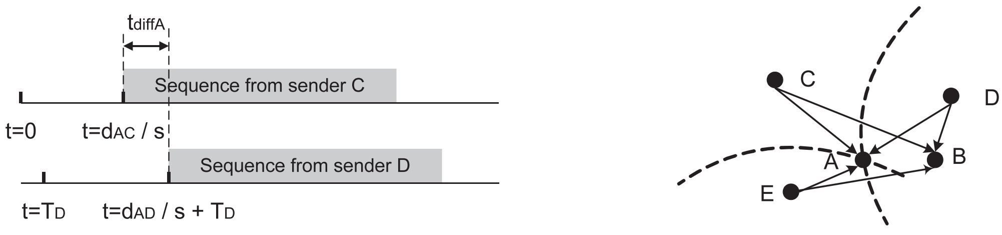
We simplify this equation and will get:

$$d_{AD} - d_{AC} = (d_{ED} - d_{EC}) + s \times (t_{diffA} - t_{diffE}) \quad (1)$$

Since nodes C, D, and E know their positions, they can calculate $d_{ED} - d_{EC}$. Nodes A and E can count the number of symbols between the first sequence arrives and the collision starts. They can translate the number of symbols into a time duration based on the frequency of the carrier signals. Therefore, we can use these values to calculate $d_{AD} - d_{AC}$. Since nodes C and D know their positions, node A will reside on one wing of the hyperbola that is jointly determined by the positions of C and D and the value of $d_{AD} - d_{AC}$. Obviously, we need more hyperbolas to determine the position of node A. We can choose other pairs of anchor nodes to send out signals and determine more hyperbolas. Node A will be positioned at the intersection point (or zone) of these hyperbolas, as shown in Fig. 2.

In real application environments, the information for localization can be delivered to wireless devices through different schemes. For example, the positions of the anchor nodes can be distributed to the devices before the localization procedures. Similar schemes have been adopted by other anchor-based localization approaches [8,15,16]. With this information, the nodes can independently calculate the distances between the anchors such as $d_{ED} - d_{EC}$. At the same time, we can distribute the value of t_{diff} with only a few bytes. Our previous analysis in [1] shows that if the average number of neighbors in an ad hoc network is 10, every node needs to transmit less than 9 KBytes to help its neighbors to determine their positions. This communication overhead can be easily handled by a laptop or a PDA.

Please note that this approach is different from existing localization mechanisms such as time-of-arrival (TOA)



Left: t_{diffA}: difference b/w the arriving time of two sequences at node A. Right: Node A is at the intersection of two hyperbolas.

Fig. 2. Node localization through physical layer network coding.

[13,14] and time-difference-of-arrival (TDOA) [8,15,16] since wireless nodes are not using their system clocks or GPS devices to directly measure the signal propagation time. On the contrary, physical layer signal interference results are used to calculate the time differences. Since the value of T_D has been canceled out in Eq. (1), the two senders do not need to synchronize their transmission operations as long as the sequences will interfere at the receivers.

While the basic idea is straightforward, several issues in the physical and network layers must be carefully addressed to turn it into a practical solution. For example, the receiver needs to distinguish among three states of the system: no signal, one incoming sequence, and two colliding sequences. As another example, the receiver needs to separate the interfered signals to recover the original sequences so that it can verify their authenticity and determine the time differences. These questions have been studied in [1,23,24] and we refer readers to these papers for more details.

PNC based localization has several highly desirable properties for its wide adoption in wireless networks. First, since the mechanism uses only starting points of collisions to determine hyperbolas and calculate positions of wireless nodes, we do not need wireless nodes to synchronize their transmission operations. This also enables multiple nodes to use the same pair of interfered sequences for their localization procedures. Second, the proposed mechanism does not require wireless nodes to be equipped with any special hardware (e.g. directional antennas, GPS devices) which will result in a lower node cost. Third, the proposed approach works in a distributed manner and does not require a centralized controller. With these properties, the approach has the potential to be adopted by various types of wireless networks.

3. Bootstrapping localization in different network environments

As we describe in Section 2, the PNC based localization mechanism needs multiple hyperbolas to determine the position of a wireless node. One factor that may restrict the wide adoption of the approach is the required number and distribution of anchor nodes. If a wireless node and q anchor nodes can receive signals from each other, we can determine $(q - 1)$ independent hyperbolas. Under most conditions, we need two to three hyperbolas to uniquely position a wireless node [30]. Based on this observation, we will study the bootstrap conditions of the localization procedures in two types of networks.

3.1. Localization in infrastructure-based networks

We first consider wireless networks with pre-established infrastructures such as wireless LANs, mesh networks, and cellular networks. These networks often contain a group of special nodes such as the access points, cellular phone towers, or the nodes with high speed Internet access. Under many conditions, these nodes are trusted by other devices in the network [31–33]. At the same time, it is reasonable to assume that these special nodes know their positions [34,35]. Since they are powered by wall sockets, these special nodes do not have to worry about their power consumption. Traditional topology design of wireless networks requires neighboring cells to use different frequency channels. In real worlds, however, inter-cell interference is a frequently seen scenario in unplanned wireless networks. For example, in a densely deployed wireless LAN up to 40% of the access points can be in communication range and share the same channel [36,37]. Similar conditions also exist in WiMAX networks [38]. Although inter-cell interference may impact the network performance, it provides an excellent opportunity for the adoption of the proposed localization mechanism.

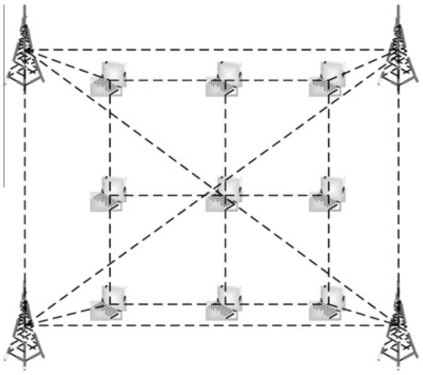


Fig. 3. Localization in infrastructure-based networks.

To apply the proposed localization mechanism to wireless networks with infrastructures, we can deploy the special nodes so that: (1) they can directly communicate with each other, and (2) most wireless devices will be covered by multiple special nodes. We can then choose different pairs of special nodes to serve as senders. Other special nodes will share the interference results that they receive with other devices. The wireless nodes can combine the information with their own interference results to calculate their positions. This mechanism is highly scalable since the same signal interference results can be used by many wireless nodes. As an example, Fig. 3 shows four cellular phone towers and the wireless nodes covered by them.

There are several reasons to believe that the proposed localization mechanism has a limited impact on the performance of wireless networks with pre-established infrastructures. First, since a wireless node needs only two to three hyperbolas to determine its position, the number of interfered access points (or cellular phone towers) can be restricted to three to four.[1] Previous research [36,37] shows that under this condition the network throughput will experience a degradation by a factor of 2–3 when network coding is not adopted. Second, based on the theoretical analysis and simulation results in [40–42], the capacity improvement brought by the PNC technique can compensate the degradation caused by the increased density of access points. Last but not least, we can schedule the channel assignment

[1] It has been formally proven in [39] that for distance-difference based localization, two hyperbolas having a common focus may have at most two intersections. Therefore, sometimes we need the third hyperbola to identify the correct position of the node.

algorithm for the access points so that inter-cell interference will last for only a short period of time during the localization procedures.

3.2. Localization in infrastructure-less networks

In self-organized wireless networks such as ad hoc or sensor networks, most nodes have the same transmission range. At the same time, most nodes can establish the trust relationship with only their direct neighbors through interactions. Therefore, we cannot locate a group of special nodes that can serve as senders to cover the whole network. Fortunately, the self-organization property allows the wireless nodes to help each other: the nodes already learning their positions can serve as anchor nodes for other devices. Under this condition, we need to investigate the required density and distribution of the initial anchor nodes and wireless devices so that the localization procedure can propagate throughout the network. We will use both theoretical analysis and simulation to study this problem.

An example scenario is shown in Fig. 4. We assume that all nodes in the self-organized network have the same transmission range. To initialize the localization procedure, we deploy a small group of anchor nodes that also have the same transmission range in the network. We expect that the direct neighbors of the anchor nodes will be able to determine their positions based on the proposed approach. These nodes, after learning their positions, will become new anchors and help other nodes to determine their positions. The localization procedure will propagate as a growing circle until all nodes successfully calculate their positions.

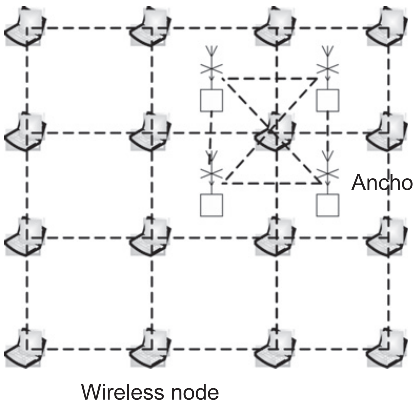


Fig. 4. Localization in infrastructure-less networks.

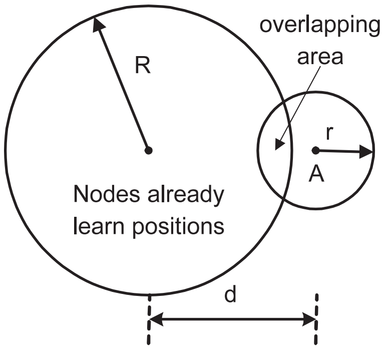


Fig. 5. Required anchor node density for localization.

This self-organization approach poses special requirements on the anchor node density: if a wireless node does not have enough number of anchor nodes as its direct neighbors, the localization procedure will stop. The theoretical analysis can be conducted as follows: We assume that the communication range of the wireless nodes is r. Without losing generality, we assume that all nodes in a circle area with the radius R have determined their positions and they are willing to serve as anchor nodes. Therefore, in circle R the density of the anchor nodes equals to that of the wireless devices. As shown in Fig. 5, node A will use the anchor nodes in the overlapping area between its communication range and the circle R to determine its position. If the distance between the centers of the two circles is d (to guarantee overlapping, we must have $R < d < R + r$), the size of the overlapping area is:

$$S_{overlap} = r^2 \cos^{-1}\left(\frac{d^2 + r^2 - R^2}{2dr}\right) + R^2 \times \cos^{-1}\left(\frac{d^2 + R^2 - r^2}{2dR}\right) - \frac{1}{2} \times \sqrt{(-d + r + R)(d + r - R)(d - r + R)(d + r + R)} \tag{2}$$

Given R and r, the expected value of $S_{overlap}$ will be:

$$\mathrm{E}(S_{overlap}) = \frac{\int_R^{r+R} S_{overlap} \times 2\pi x dx}{\pi(R + r)^2 - \pi R^2} \tag{3}$$

Let us consider two extreme cases. When $R = r$, we assume that all anchor nodes are deployed in the communication range of one wireless device. We substitute the parameters into Eq. (3) and will get $\mathrm{E}(S_{overlap}) = \frac{\sqrt{3}}{4} r^2$. In the second case, when $R = \infty$, the arc of the large circle can be viewed as a segment of a straight line. We substitute the parameters into Eq. (3) and will get $\mathrm{E}(S_{overlap}) = \frac{2}{3} r^2$. To determine the position of node A, we need to have at least three anchor nodes in the overlapping area to determine two different hyperbolas. Since in circle R the density of the anchor nodes equals to that of the wireless devices, we can use the expected size of the overlapping area to estimate the node density in the network. Based on this analysis, the average number of neighbors of the wireless devices should fall into the range between $\left(3/\frac{2}{3} r^2 \times \pi r^2 = 14\right)$ and $\left(3/\frac{\sqrt{3}}{4} r^2 \times \pi r^2 = 22\right)$ so that the self-organized localization procedure can propagate throughout the network. As a specific example, if the communication range $r = 250$ m, we need to deploy 71–112 nodes in a 1 km^2 area to reach this degree of connectivity.

Please note this is a very conservative estimation of the required node density for the proposed localization mechanism. In real networks, a lower node density would be required since anchor nodes outside of the circle R can also assist wireless devices in their localization procedures. For example, we need only two anchor nodes in the overlapping area to serve as the senders. Another anchor node can be at any position as long as it can receive the interfered sequences. Node A can then exchange information with the third anchor node through a multi-hop path. This relaxed requirement will allow the proposed approach to be adopted by more networks.

We have conducted extensive simulation in static wireless networks to validate our analysis. In our simulation setup, we assume that wireless nodes are randomly and uniformly distributed in a 2000 m × 2000 m square area. The communication range of the wireless devices is $r = 100$ m. In the bootstrap procedure, a group of anchor nodes are deployed in the network to help wireless devices to determine their positions. Then these devices will serve as anchor nodes for other devices. We want to investigate the relationship among the parameters such as the density of the wireless nodes and the size, distribution and position of the bootstrap areas. The results are shown in Figs. 6 and 7. Each point in the figures is the average value of 25 experiments with different network setups.

Fig. 6 illustrates the impacts of node density and size of the bootstrap area on the proposed localization mechanism. On the *X*-axis of the figure, we use the average number of neighbors of the wireless devices to represent node density. The bootstrap area is a circle with the radius *R* and it is deployed in a corner of the network. We change the ratio between *R* and the communication range *r* to investigate the impacts of the size of the bootstrap area. From this figure, we can find out two facts about the proposed approach. First, when the average degree of connectivity reaches about 12, majority of the nodes in the wireless network will be able to determine their positions. The simulation results and our analysis results match with each other.

Second, there is an interesting relationship between the size of the bootstrap area and the fraction of nodes whose positions can be determined. As shown in Fig. 6, when the node density is high (e.g. $\geqslant 12$), almost all nodes can determine their positions. Therefore, the size of the bootstrap area does not matter too much and the four lines stay very close to each other. On the other side, when the node density is low (e.g. ≈ 9), only the nodes in the bootstrap area can be positioned. Therefore, the fraction roughly equals to the ratio between the size of the bootstrap area and the whole network. Between the two extreme cases, the size of the bootstrap area will impact the localization procedures from two aspects. (a) As the analysis shows, when *R* becomes larger, the expected overlapping area between the bootstrap circle and the communication range of a wireless node will also become larger. Therefore, the node has a higher probability to be the direct neighbor of multiple anchor nodes so that its position can be determined. (b) A large bootstrap area may cover some of the sparse node zones so that the nodes in these zones can also determine their positions. The impacts can be seen clearly from the line for '$R = 4r$'.

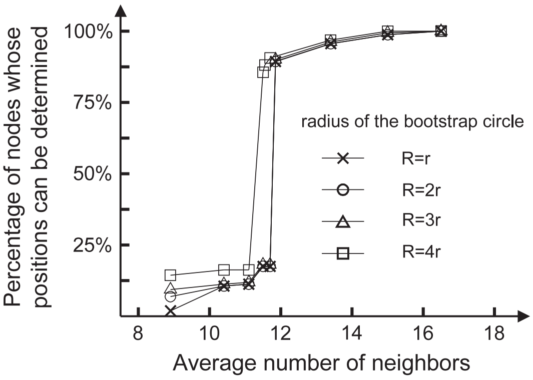


Fig. 6. Impacts of node density and size of bootstrap area.

In the second group of experiments, we investigate the impacts of the distribution and position of the bootstrap areas on the proposed approach. Based on the experiment results in Fig. 6, we set the ratio between *R* and *r* to be 3 so the total size of the bootstrap area is $9\pi r^2$. In Fig. 7a, we deploy the bootstrap area at different positions in the network: a corner, the center, and a random place. We then study the percentage of nodes that can determine their positions under different node densities. From Fig. 7a, we find that: (a) in sparse networks, deploying the bootstrap area in the center of the network will help more nodes to determine their positions since the average path length between a wireless node and the initial anchors is shorter; and (b) when the node density is large enough, the position of the bootstrap area does not matter too much since most nodes can find enough anchor nodes in their direct neighbors.

In Fig. 7b, we keep the total size of the bootstrap area unchanged but divide it into smaller pieces. For example, we may deploy two bootstrap areas each with the radius of $\frac{3}{\sqrt{2}}r$ or four areas each with the radius of 1.5*r* into the network. The results show that in sparse networks, it is actually beneficial to use multiple small bootstrap areas to replace one large area. We believe that the advantages come from two aspects: (a) multiple small bootstrap areas can cover sparse node zones at different places so that the nodes in these zones can also determine their positions; and (b) we can reduce the average path length between a wireless device and the initial anchors.

4. Safety of the approach

4.1. Assumptions

In this part we plan to investigate the security of the proposed approach. Specifically, we focus on the integrity and authenticity of the exchanged information among the anchor nodes and wireless devices. Since the proposed approach consists of multiple steps, malicious attackers can distribute false information at different stages to reduce or even abolish the localization accuracy. For example, attackers can impersonate a legitimate node to send out false sequences or interference results to mislead the calculation of hyperbolas and the final positions.

To defend against such attacks, the wireless nodes must be able to verify the authenticity of the received information. This is usually achieved with the help of shared secrets among wireless nodes. For the networks with pre-deployed infrastructures, if the wireless nodes can handle asymmetric encryption, the anchor nodes can deploy public keys into the devices when they join the network. Digital signatures can then be attached to the packets to protect their authenticity. This scheme is especially suitable for the scenarios in Fig. 3 since the public

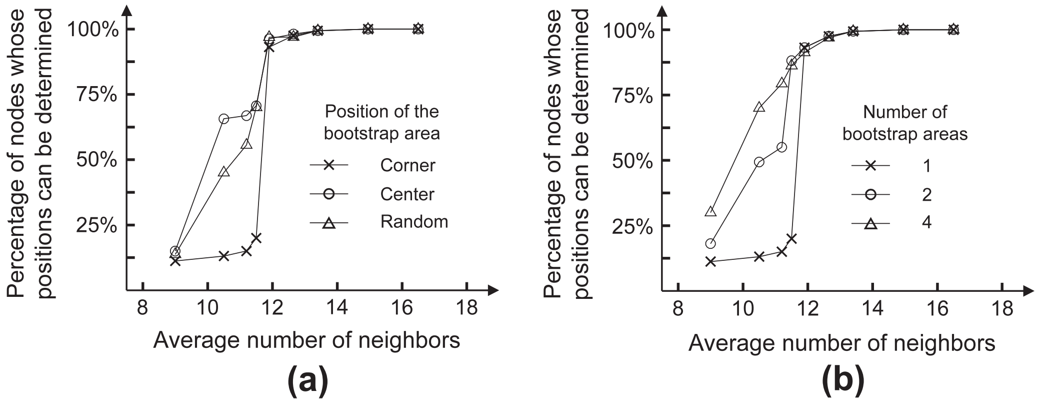


Fig. 7. Impacts of the distribution and position of the bootstrap areas.

keys of the cellular carriers can be pre-installed into the cellular phones. If the wireless nodes cannot handle asymmetric encryption, pair-wise keys [43,44] or group based encryption [45–47] can be adopted to protect the information. Special mechanisms will be designed in Section 4.3 to reduce the communication overhead when we have a large number of receivers and different keys have to be used for integrity verification.

In addition to the shared secrets, we also assume that the wireless devices share some light weight functions such as pseudo random number generators [48,49] and secure hash functions. Previous research has shown that these functions will not introduce significant computation and storage overhead at the devices. The wireless nodes can use these functions to generate nonces so that the freshness of the information can be verified.

4.2. Defending against stealth attacks

The properties of wireless communication enable the malicious nodes to conduct stealth attacks on the proposed approach. In these attacks, the malicious nodes do not directly change the contents of the packets from the anchors and wireless devices. Therefore, we cannot mitigate them through traditional mechanisms such as encryption. As an example, the attackers can send out noises in parallel with the anchor nodes to cause three-party interference at the receivers. Since the receivers cannot correctly recover the original sequences, the localization procedure will fail. As another example, the attackers can conduct wormhole attacks [50] by recording and re-broadcasting the sequences from an anchor node at a different place. This will also lead wireless devices to generate fake hyperbolas during localization. New mechanisms must be designed to mitigate these attacks.

The malicious nodes can send out jamming signals to impair the localization procedures. Different from many anti-jamming scenarios, we cannot directly adopt the frequency hopping technique since the senders and the receivers do not have synchronized clocks and they cannot guarantee that the interfered signals always have the same carrier frequency. To avoid jamming, the senders and receivers can determine the carrier frequency of the signals through a secure communication channel among them before the localization procedures. There are such transceivers on the market that allow the wireless nodes to adjust the carrier frequency within the range of 150 MHz. The change at this scale will have a good chance to avoid the external jammers. For internal jammers, we can divide wireless nodes into multiple groups with overlapping members. If whenever a certain node *X* is included in the current group the localization procedures will be impacted by jamming attacks, we can label it as suspicious and avoid it in the future.

Sybil attacks [51] and wormhole attacks [52] are two representations of stealth attacks on wireless networks. In a Sybil attack, the same physical device can illegitimately act with multiple identities in the network. In a wormhole attack, the malicious nodes can eavesdrop on the packets, tunnel them to another location in the network, and retransmit them. These attacks pose severe threats to both routing protocols [53] and misbehavior detection mechanisms [54] in wireless networks. For example, the devices may depend on the neighbor discovery procedures to construct local network topology. If the neighbor discovery beacons are tunneled through wormholes, the good nodes will get false information about their neighbors and choose a non-existent route.

To defend against these stealth attacks, we plan to adopt the approaches also based on physical layer network coding [55,56] so that the same group of assumptions are made. In both [55] and [56] the wireless devices measure the arriving time of the interfered sequences to detect the anomalies. Since this information is also used by our localization mechanism, no additional overhead will be introduced by the attack detection schemes.

4.3. Protecting integrity and authenticity of interfered sequences

Depending on the number of intended receivers of the interfered sequences, we design different schemes to protect the integrity of the packets in infrastructure based and infrastructure-less networks. For the scenarios shown in Fig. 3, the packets from the anchor nodes will be received by a large number of wireless devices. If the wireless nodes can handle asymmetric encryption, the anchor nodes will attach digital signatures to the packets to protect their authenticity.

The scenarios are more complicated when the wireless devices can support only symmetric encryption. Since it is not efficient to attach a separate message authentication code (MAC) of the packet for every intended receiver, a group of receivers must be randomly determined to verify the information integrity. Here we propose a solution based on hash chains to select the nodes. When an anchor node wants to send out a message *msg* for localization, it will generate an *x*-entry hash chain for every receiver by repeatedly hashing the concatenation of the message and the node's identity: $hash^1(msg, node\ ID)$, $hash^2(msg, node\ ID) = hash(hash(msg, node\ ID)), \ldots, hash^x(msg, node\ ID)$. If in any of these hash results the last *l* bits are all '0', this node will be chosen as a verifier. For each selected verifier, the anchor will attach a message authentication code (MAC) based on the packet contents and its shared key with the device. Since we assume that all wireless nodes in the network share this secure and random hash function, they can easily check the identities of the selected verifiers. The selected nodes can use their pair-wise keys with the anchors to verify the integrity of the packet. If there are more than a threshold number of nodes sending alarms to report integrity violations, the packet will be discarded.

We can adjust the values of the parameters *x* and *l* to achieve a trade-off between the safety and efficiency of the integrity verification scheme. For a well-designed hash function, the probability that the last *l* bits of the hash result of a random message are all '0' is $1/2^l$. For an *x*-entry hash chain, the probability that at least one of them satisfies this requirement is $p = 1 - \left(1 - \frac{1}{2^l}\right)^x$. If we assume that *n* nodes are intended receivers of the packet, on average $n \times p$ nodes will be selected to verify the integrity of the information. The extra communication overhead mainly comes from the attached MAC codes for the selected verifiers.

A concrete example can be calculated as follows: If we construct a hash chain with the length $x = 10$ for every receiver and examine the last $l = 9$ bits of the hash results, the probability $p = 1 - \left(1 - \frac{1}{2^9}\right)^{10} = 1.94\%$. If there are 1000 receivers in the network, about 19 nodes will be selected to verify the integrity of the packet. To determine the verifiers, the anchor node needs to calculate $10 \times 1000 = 10{,}000$ hash functions, which can be accomplished by most modern computers within 1 ms. Since 80-bits MAC values can satisfy the security requirements of most applications in wireless networks [57], this approach will introduce $19 \times 10 = 190$ bytes communication overhead for each localization packet from the anchor.

For the scenarios shown in Fig. 4, the anchor nodes need to consider only their direct neighbors. In this way, a separate message authentication code (MAC) for each of the intended receivers can be attached to the packet. Combining this result with the overhead analysis in [1], we find that PNC based node localization will introduce very limited computation and communication overhead into the networks.

5. Improving localization accuracy

There are two groups of factors that can impact the localization accuracy of the PNC based mechanism. The first group contain the errors that are introduced during the execution of the localization procedures. These errors can usually be reduced or mitigated through an improved algorithm design. For example, as shown in Eq. (1), the wireless nodes depend on the detection of the starting points of signal interference to calculate t_{diff}. Considering the high propagation speed of the radio waves, if the detected collision is offset by several symbols, the introduced error can be large. Some mechanisms must be designed to reduce the impacts.

We plan to adopt the mechanism described in [1,23] to solve this problem. Specifically, we will embed a pilot bit sequence with known contents at both the beginning and end of each packet. With this information, even when the detected collision has an offset of several symbols, the wireless devices can still determine the correct starting point. Since previous research [23] shows that a 64-bit pilot sequence will be long enough to distinguish the packet from any random noise, this scheme will not introduce much communication overhead into our approach.

Another factor that could impact the localization accuracy is the frequency jitter of the carrier signals. In real wireless networks the carrier frequency is a time-varying variable and its jitter can impact the localization accuracy from two aspects. First, it will cause an increase in the bit error rate (BER) at the receivers, which will harm the sequence separation procedure. Our previous research [56] shows that the increased BER can be compensated by introducing redundancy into the data packets. Second, the frequency jitter will impact the accuracy of distance estimation. For example, if the receivers assume that the frequency of the signals is *f* while a jitter of Δf exists, the estimated distance will have an error proportional to the value of $\Delta f / f$. Fortunately, research in [58,59] shows that the impacts of clock jitter is usually very small in physical layer network coding systems.

The second group of factors that can impact the localization accuracy are not directly related to the design or implementation of our algorithms. For example, many localization schemes assume that the anchor nodes learn their positions through GPS devices. There are implicit inaccuracies in the GPS readings [60,61]. Most civilian GPS devices can provide positioning results with an average error of 5 m horizontally. Such errors will be carried into the proposed approach and impact the positioning procedures of other nodes. As the example shown in Fig. 8, the errors in GPS readings move node *B* from its real

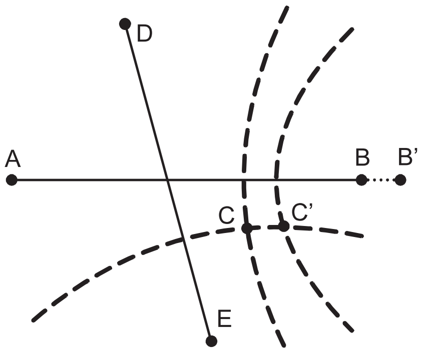


Fig. 8. Localization inaccuracies caused by GPS errors.

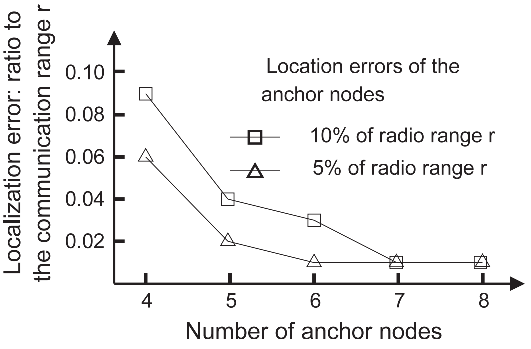


Fig. 9. Using uncertainty area to reduce localization errors.

position to the fake position *B*′. As a result, the intersection of two hyperbolas is moved from *C* to *C*′. If node *C* uses this result to help other nodes to determine their positions, the errors will be carried over and amplified in subsequent operations. The accumulated errors are especially harmful in multi-hop localization procedures.

We have developed two mechanisms to reduce the negative impacts of these errors. The first scheme tries to identify the hyperbolas that are determined by the anchor nodes with positioning errors and exclude their intersections. In this way, it can improve the localization accuracy of individual nodes. The basic idea is as follows: If we model the positioning errors of the anchor nodes with a zero-mean Gaussian random variable [62], the distribution of the intersection points will demonstrate the following property. The intersections determined by the accurate positions are concentrated near the true node location, while those determined by the anchors with positioning errors are distributed all over the network. We can use the intersection distribution function (*DF*) to quantify their density:

$$DF(x,y) = \sum_{i=1}^{M} exp\left(-\frac{((x-x_i)^2+(y-y_i)^2)}{\epsilon^2}\right) \tag{4}$$

Here *M* is the total number of intersection points and (x_i, y_i) are their coordinates. The parameter ϵ^2 is used to adjust the contribution of an intersection to the final *DF*, thus will directly determine the size of the uncertainty area. Previous research [30,63] shows that ϵ should be chosen as 1–2 times the standard deviation of the receiver noise. Based on this result, the position uncertainty area will be a circle centered at the calculated intersection with the radius 0.7–1.5 times the positioning errors of the anchor nodes. In real applications, we will use the uncertainty area to cover the zone with the largest intersection density. The covered intersection points will then be used to calculate the position of the wireless device.

To evaluate the effectiveness of the mechanism, we use simulation to study the relationship between the localization accuracy and the number of intersection points. Based on [30], *m* anchor nodes can determine $\binom{m}{3} + 3 \times \binom{m}{4}$ intersections of the hyperbolas. We test two cases in which

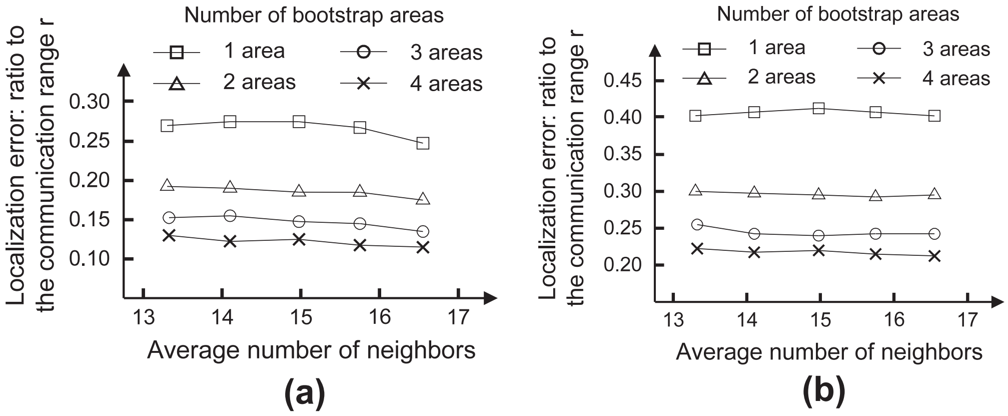


Fig. 10. Relationship between localization accuracy and the number of bootstrap areas. Positioning errors of the anchor nodes: (a) 5%*r* and (b) 10%*r*.

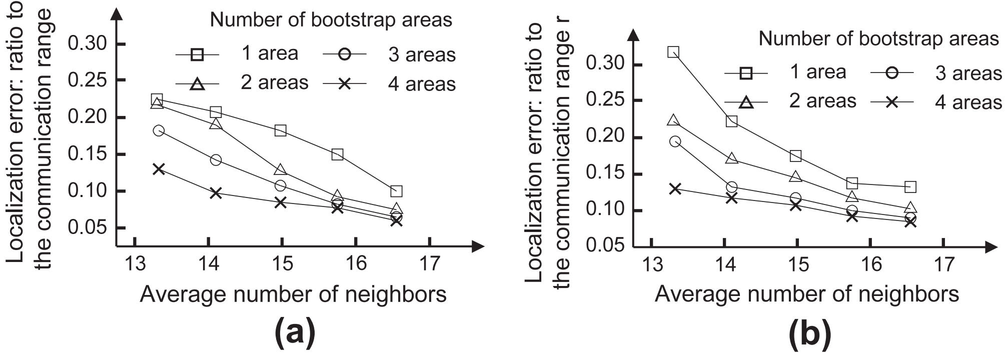


Fig. 11. Localization accuracy with both mechanisms enabled. Positioning errors of the anchor nodes: (a) 5%*r* and (b) 10%*r*.

the initial positioning errors of the anchor nodes follow a zero mean Gaussian distribution with the standard deviation equal to 5% and 10% of the communication range respectively. From Fig. 9, we find that as the number of anchor nodes (thus, intersection points) increases, the localization errors decrease very quickly.

The second mechanism that we propose will reduce the cumulative errors in multi-hop localization procedures. Specifically, we plan to deploy multiple groups of anchor nodes at different places in the network [64] to bootstrap the localization procedures. This mechanism has at least two advantages. First, by introducing multiple bootstrap areas, we can reduce the shortest distance between a node and the anchors. In this way, the localization errors will be carried over through fewer hops. Second, the localization procedure will be conducted through multiple independent growing circles. The wireless nodes can cross-examine the localization results from multiple sources to improve the accuracy.

We use simulation to study the relationship between the localization accuracy and the number of bootstrap areas. In our simulation, a group of wireless nodes are randomly and uniformly distributed in a $2000\,\mathrm{m} \times 2000\,\mathrm{m}$ square area. The wireless communication range is $r = 100$ m. We position multiple bootstrap areas in different corners of the network. Each bootstrap area is a circle with the radius $R = 100$ m. We model the positioning errors of anchor nodes with a zero mean Gaussian distribution with the standard deviation equal to 5% and 10% of the communication range respectively. The simulation results are shown in Fig. 10. Each point in the figure is the average value of 25 experiments with different network setups.

From Fig. 10, we find that increasing the node density cannot effectively reduce the cumulative localization errors through multi-hop paths. On the contrary, by introducing more bootstrap areas, we can reduce the localization errors to about a half of the worst cases. The study shows that it will be more beneficial to introduce multiple small bootstrap areas at different places in the network than one large bootstrap area.

The two mechanisms that we propose can work together to improve the localization accuracy. We use the same simulation setup as above and Fig. 11 illustrates the results when both mechanisms are adopted.

6. Conclusion

In this paper we study different properties of the physical layer network coding based localization mechanism. We investigate the required node density for the execution of the proposed approach in self-organized wireless networks through both theoretical analysis and simulation. Mechanisms using message authentication code (MAC) and hash chains are designed to protect the integrity of the packets. We also study the localization inaccuracies caused by the positioning errors of anchor nodes and design mechanisms to reduce their impacts. The research results allow us to deeply understand the PNC based localization mechanism. They will also help end users to determine whether or not this approach can be applied to their networks.

Immediate extensions to our approach consist of the following aspects. First, we plan to implement the proposed approach on a software defined radio platform so that we can test it in real network environments. Second, we will explore mechanisms to improve the efficiency of the proposed approach so that it can be applied to mobile networks. Finally, we will investigate using physical layer network coding to accomplish other tasks such as sender authentication in wireless networks. This research is supported in part by NSF under award number 1143602.

References

[1] Z. Li, D. Pu, W. Wang, A. Wyglinski, Node localization in wireless networks through physical layer network coding, in: Proceedings of IEEE Globol Communications Conference (GLOBECOM), 2010.

[2] D.B. Faria, D.R. Cheriton, Detecting identity-based attacks in wireless networks using signalprints, in: Proceedings of ACM WiSe, 2006, pp. 43–52.

[3] C.A. Ardagna, M. Cremonini, S.D.C. d. Vimercati, P. Samarati, Managing privacy in location-based access control systems, in: L.T. Yang, A.B. Waluyo, J. Ma, L. Tan, B. Srinivasan (Eds.), Mobile Intelligence, John Wiley & Sons, Inc., 2010.

[4] L. Lazos, R. Poovendran, Serloc: Robust localization for wireless sensor networks, ACM Trans. Sen. Netw. 1 (1) (2005) 73–100.

[5] P. Bellavista, A. Kupper, S. Helal, Location-based services: back to the future, IEEE Perv. Comput. 7 (2) (2008) 85–89.

[6] S. Dhar, U. Varshney, Challenges and business models for mobile location-based services and advertising, Commun. ACM 54 (5) (2011) 121–128.

[7] I.A. Junglas, R.T. Watson, Location-based services, Commun. ACM 51 (3) (2008) 65–69.

[8] A. Srinivasan, J. Wu, A survey on secure localization in wireless sensor networks, in: B. Furht (Ed.), Encyclopedia of Wireless and Mobile Communications, CRC Press, Taylor and Francis Group, 2008.

[9] I. Guvenc, C.C. Chong, A survey on toa based wireless localization and nlos mitigation techniques, IEEE Commun. Surv. Tutor. 11 (3) (2009) 107–124.

[10] J. Wang, R.K. Ghosh, S.K. Das, A survey on sensor localization, J. Contr. Theory Appl. 8 (1) (2010) 2–11.

[11] D. Kumar, S. Varma, An efficient localization based on directional antenna for wireless sensor networks, Int. J. Comput. Electr. Eng. 1 (5) (2009) 542–549.

[12] K. Whitehouse, C. Karlof, D. Culler, A practical evaluation of radio signal strength for ranging-based localization, SIGMOBILE Mob. Comput. Commun. Rev. 11 (2007) 41–52.

[13] Y. Chan, W. Tsui, H. So, P. Ching, Time-of-arrival based localization under nlos conditions, IEEE Trans. Veh. Technol. 55 (1) (2006) 17–24.

[14] U. Klee, T. Gehrig, J. McDonough, Kalman filters for time delay of arrival-based source localization, EURASIP J. Appl. Signal Process. (2006) 167–181.

[15] I. Amundson, X.D. Koutsoukos, A survey on localization for mobile wireless sensor networks, in: Mobile Entity Localization and Tracking in GPS-less Environnments, 2009, pp. 235–254.

[16] G. Mao, B. Fidan, B.D.O. Anderson, Wireless sensor network localization techniques, Comput. Netw. 51 (10) (2007) 2529–2553.

[17] S. Lederer, Y. Wang, J. Gao, Connectivity-based localization of large-scale sensor networks with complex shape, ACM Trans. Sen. Netw. 5 (31) (2009) 1–31.

[18] W. Qiu, E. Skafidas, Distributed source localization based on toa measurements in wireless sensor networks, Res. Let. Signal Proc. 8 (2009) 1–5.

[19] A. Bishop, B. Fidan, K. Doğançay, B. Anderson, P. Pathirana, Exploiting geometry for improved hybrid aoa/tdoa-based localization, Signal Process. 88 (7) (2008) 1775–1791.

[20] R. Chen, J. Park, J. Reed, Defense against primary user emulation attacks in cognitive radio networks, IEEE JSAC 26 (1) (2008) 25–37.

[21] B. Kusy, A. Ledeczi, X. Koutsoukos, Tracking mobile nodes using rf doppler shifts, in: Proceedings of ACM SenSys, 2007, pp. 29–42.

[22] M. Hay, B. Saeed, C.-H. Lung, A. Srinivasan, Co-located physical-layer network coding to mitigate passive eavesdropping, in: Eighth Annual International Conference on Privacy Security and Trust (PST), 2010.

[23] S. Katti, S. Gollakota, D. Katabi, Embracing wireless interference: analog network coding, in: ACM SigComm, 2007, pp. 397–408.

[24] S. Zhang, S. Liew, P. Lam, Physical-layer network coding, in: ACM MobiCom, 2006, pp. 358–365.

[25] Ettus Research, Universal software radio peripheral <http://www.ettus.com>.

[26] G. SFS, Gnu radio – gnu fsf project <http://www.gnu.org/software/gnuradio>.

[27] J. Zhang, J. Jia, Q. Zhang, E. Lo, Implementation and evaluation of cooperative communication schemes in software-defined radio testbed, in: INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1–9.

[28] L. Lu, T. Wang, S.C. Liew, S. Zhang, Implementation of physical-layer network coding, *Phys. Commun.*, 2012.

[29] P. Marshall, Darpa progress in spectrally adaptive radio development (2006).

[30] C. Ma, R. Klukas, G. Lachapelle, A nonline-of-sight error-mitigation method for toa measurements, IEEE Trans. Veh. Technol. 56 (2) (2007) 641–651.

[31] Y. Matsunaga, A.S. Merino, T. Suzuki, R.H. Katz, Secure authentication system for public wlan roaming, in: Proceedings of ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, 2003, pp. 113–121.

[32] J. Sun, C. Zhang, Y. Fang, A security architecture achieving anonymity and traceability in wireless mesh networks, in: IEEE INFOCOM, 2008, pp. 1687–1695.

[33] Y. Zhang, Y. Fang, Arsa: An attack-resilient security architecture for multihop wireless mesh networks, IEEE J. Select. Areas Commun. 24 (10) (2006) 1916–1928.

[34] U. Ahmad, A. Gavrilov, S. Lee, Y.-K. Lee, Modular multilayer perceptron for wlan based localization, in: International Joint Conference on Neural Networks, 2006, pp. 3465–3471.

[35] Y.-C. Cheng, Y. Chawathe, A. LaMarca, J. Krumm, Accuracy characterization for metropolitan-scale wi-fi localization, in: Proceedings of Iinternational Conference on Mobile Systems, Applications, and Services, 2005, pp. 233–245.

[36] A. Akella, G. Judd, S. Seshan, P. Steenkiste, Self-management in chaotic wireless deployments, Wirel. Networks 13 (2007) 737–755.

[37] M.A. Ergin, K. Ramachandran, M. Gruteser, An experimental study of inter-cell interference effects on system performance in unplanned wireless lan deployments, Comput. Network 52 (2008) 2728–2744.

[38] J.-H. Yeom, Y.-H. Lee, Mitigation of Inter-Cell Interference in Mobile WiMAX, John Wiley & Sons, Ltd., 2008, Ch. Mobile WiMAX, pp. 31–47.

[39] X. Xu, S. Sahni, N. Rao, On basic properties of localization using distance-difference measurements, in: International Conference on Information Fusion, 2008.

[40] C. Chen, H. Xiang, The throughput order of ad hoc networks with physical-layer network coding and analog network coding, in: IEEE International Conference on Communications (ICCs), 2008, pp. 2146–2152.

[41] H. Gacanin, F. Adachi, The performance of network coding at the physical layer with imperfect self-information removal, *EURASIP J Wirel Comm*, 8 (2010) 1–8.

[42] K. Lu, S. Fu, Y. Qian, H.-H. Chen, On capacity of random wireless networks with physical-layer network coding, IEEE J. Sel. A. Commun. 27 (2009) 763–772.

[43] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, M. Galloway, A survey of key management schemes in wireless sensor networks, Comput. Commun. 30 (2007) 2314–2341.

[44] J. Zhang, V. Varadharajan, Wireless sensor network key management survey and taxonomy, J. Netw. Comput. Appl. 33 (2) (2010) 63–75.

[45] E. Klaoudatou, E. Konstantinou, G. Kambourakis, S. Gritzalis, A survey on cluster-based group key agreement protocols for wsns, IEEE Commun. Surv. Tutor. 13 (3) (2011) 429–442.

[46] K.M. Martin, M.B. Paterson, D.R. Stinson, Key predistribution for homogeneous wireless sensor networks with group deployment of nodes, ACM Trans. Sen. Netw. 7 (2010) 11:1–11:27.

[47] W. Zhang, S. Zhu, G. Cao, Predistribution and local collaboration-based group rekeying for wireless sensor networks, Ad Hoc Networks 7 (6) (2009) 1229–1242.

[48] R. Jenkins, Isaac, in: International Workshop on Fast Software Encryption, 1996, pp. 41–49.

[49] R. Latif, M. Hussain, Hardware-based random number generation in wireless sensor networks, in: International Conference on Advances in Information Security and Assurance, 2009, pp. 732–740.

[50] M. Khabbazian, H. Mercier, V. Bhargava, Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks, IEEE Trans. Wirel. Commun. 8 (2) (2009) 736–745.

[51] D. Mónica, Thwarting the sybil attack in wireless ad hoc networks, Master's thesis, Instituto Superior Técnico, Universidade Técnica de Lisboa (July 2009).

[52] Y. chun Hu, A. Perrig, D.B. Johnson, Wormhole attacks in wireless networks, IEEE J. Sel. Areas Commun. 24 (2006) 370–380.

[53] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks 1 (2–3) (2003) 293–315.

[54] J. Newsome, E. Shi, D. Song, A. Perrig, The sybil attack in sensor networks: analysis and defenses, in: Proceedings of IEEE IPSN, 2004, pp. 259–268.

[55] Z. Li, D. Pu, W. Wang, A. Wyglinski, Forced collision: detecting wormhole attacks with physical layer network coding, Elsevier Tsinghua Science and Technology, Wirel. Mobile Comput. Network. 16 (5) (2011) 505–519.

[56] W. Wang, D. Pu, A. Wyglinski, Detecting sybil nodes in wireless networks with physical layer network coding, in: IEEE/IFIP International Conference on Dependable Systems and Networks (DSNs), 2010, pp. 21–30.

[57] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, Hash functions and rfid tags: mind the gap, in: International Workshop on Cryptographic Hardware and Embedded Systems, 2008, pp. 283–299.

[58] S. Jagannathan, H. Aghajan, A. Goldsmith, the effect of time synchronization errors on the performance of cooperative miso systems, in: Proceedings of IEEE Globecom, 2004, pp. 102–107.

[59] S. Zhang, S.-C. Liew, P. Lam, On the synchronization of physical-layer network coding, in: IEEE Information Theory Workshop, 2006, pp. 404–408.

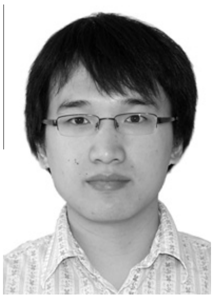
[60] R. Navon, Y. Shpatnisky, Field experiments in automated monitoring of road construction, J. Construct. Eng. Manag. 131 (4) (2005) 487–493.

[61] J. Paek, J. Kim, R. Govindan, Energy-efficient rate-adaptive gps-based positioning for smartphones, in: Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys), 2010, pp. 299–314.

[62] L. Harcke, R. Ueberschaer, J. Sinko, J. Strus, Gps/imu error analysis for airborne sar remote sensing, in: Proceedings of the International Technical Meeting of the Satellite Division of The Institute of Navigation, 2007, pp. 1631–1635.

[63] C. Ma, R. Klukas, G. Lachapelle, An efficient nlos error mitigation method for wireless location, in: Proceedings of TRLab Wireless Conference, 2002, pp. 160–167.

[64] S. Yamada, J.-y. Takayama, S. Ohyama, Wireless sensor nodes localization based on multiple range data fusion, in: International Conference on Networked Sensing Systems, 2008.



Zhiwei Li is a PhD student at the Department of Software and Information Systems, University of North Carolina at Charlotte, USA. His research interest focuses on network and information security, especially the analysis and verification of security protocols.

Weichao Wang received his PhD in Computer Science from the Purdue University in 2005. He is currently an Assistant Professor at the Department of Software and Information Systems, University of North Carolina at Charlotte, USA. His research interests are in designing protocols and mechanisms to secure pervasive systems, especially the resource-restraint networks. He is a Member of ACM.