This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

Wormhole-Resilient Secure Neighbor Discovery in Underwater Acoustic Networks

Rui Zhang and Yanchao Zhang
Department of Electrical and Computer Engineering
New Jersey Institute of Technology
Email: {rz23,yczhang}@njit.edu

***Abstract*—Neighbor discovery is a fundamental requirement and need be done frequently in underwater acoustic networks (UANs) with floating node mobility. In hostile environments, neighbor discovery is vulnerable to the wormhole attack by which the adversary uses secret wormhole links to make distant nodes falsely accept each other as a neighbor. The wormhole attack may lead to many undesirable consequences and cannot be solved by cryptographic methods. Existing wormhole defenses for ground wireless networks cannot be directly applied to UANs where most of their assumptions no longer hold. This paper presents a suite of novel protocols to enable wormhole-resilient secure neighbor discovery in UANs. Our protocols are based on the Direction of Arrival (DoA) estimation of acoustic signals, a basic functionality readily available in current UANs. The proposed protocols can thwart the wormhole attack with overwhelming probability without conventional hard requirements on secure and accurate time synchronization and localization. Detailed theoretical analysis and simulation results confirm the high performance of the proposed protocols.**

I. Introduction

Underwater Acoustic Networks (UANs) [1]–[3] are an enabling paradigm for many scientific, commercial, and military scenarios. Typical applications include ocean sampling, environmental monitoring, undersea explorations, disaster prevention, tactical surveillance, underwater warfare, and so on [3]. A UAN often consists of heterogeneous nodes such as divers, submarines, Remotely Operated Vehicles (ROV), Unmanned Underwater Vehicles (UUV), and surface stations, and nearby nodes communicate via acoustic rather than radio signals.

Neighbor discovery is a crucial requirement in UANs as in ground wireless networks such as mobile ad-hoc networks (MANETs) and wireless sensor networks (WSNs). It is the process of each node discovering others in its transmission range. Without successful neighbor discovery, other network functionalities like multi-hop routing cannot be performed. In a UAN, neighbor discovery need be done frequently because nodes may move proactively or unpredictably due to underwater current, which is similar to neighbor discovery in MANETs where nodes constantly move.

Neighbor discovery is vulnerable to various attacks in UANs deployed in hostile environments. For example, in a military UAN, attackers may conduct neighbor discovery with legitimate nodes and thus become internal nodes to gather secret information and also disturb network operations; attackers in a commercial UAN may do the same thing to degrade the quality of service provided by the target UAN. This situation necessitates secure neighbor discovery in UANs as in ground networks [4].

Common solutions to secure neighbor discovery rely on cryptographic methods, in which each node with proper keys conduct authenticated neighbor discovery with other nodes via an appropriate three-way handshake protocol [5]. Attackers without correct keys thus cannot cheat legitimate nodes into believing that they are good nodes, so the aforementioned attack is successfully defeated. There are, however, some more subtle attacks to defend against, among which the *wormhole* attack [5]–[14] is one of the most challenging.

In a wormhole attack, two collaborating attackers create a wormhole link, essentially an out-of-band and low-latency channel, between two distant network locations. They then tunnel messages recorded at one end of the wormhole link to the other. The wormhole attack will severely disturb neighbor discovery and cannot be thwarted by cryptographic methods. In particular, two distant nodes will be able to execute a cryptographic authentication protocol via the wormhole link invisible to them. As a result, they will falsely consider each other a neighbor. Attackers can then use wormhole links to tunnel routing information to disturb routing operations, selectively drop packets, and even create routing loops to waste the limited energy of the network without the need to compromise any node. There are many elegant solutions to the wormhole attack in ground wireless networks, see [5]–[14] for example. These solutions, however, cannot be directly applied to UANs due to their unique features [15], [16]. Most notable are long propagation delays, severely impaired channels, very limited acoustic link capacity, floating node mobility, the 3-D nature, absence of GPS signaling, and so forth [3]. Thus we are motivated to design a new solution to wormhole-resilient secure neighbor discovery in UANs.

A. Related Work

Secure neighbor discovery in ground wireless networks is studied in [4], [17], [18]. It is shown in [17], [18] that a feasible solution should use both time and location information.

There is a rich literature on wormhole detection in ground wireless networks, for which we only give a brief survey due to the space limitations. Distance-bounding solutions [6], [7] are based on the principal that it is impossible for the attacker to relay a packet faster than the speed of light. They cannot be applied in UANs where the propagation speed of acoustic

978-1-4244-5837-0/10/$26.00 ©2010 IEEE

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

signals is five orders slower than that of light. Location-based solutions [5], [8], [9] require nodes to be location-aware. This assumption does not hold in a UAN because GPS signals are not available in underwater environments and secure localization in UANs is another very difficult problem without available solution. Using RF fingerprinting to detect wormhole links is introduced in [10], while the feasibility of applying such techniques to acoustic signals is unclear. A heuristic based on a connectivity graph is proposed in [11] to detect wormholes and reject false links and is recently improved in [12]. They both better work for networks with relatively high density which cannot be assumed in UANs. A solution using directional antennas is presented in [13], and recently Shokri *et al.* propose a novel neighbor verification protocol [14] under the assumption that two nodes can communicate using both RF and sound. They cannot be applied to UANs because light and RF signals severely attenuate in the water.

To the best of our knowledge, [15], [16] are the only two pieces of work on wormhole detection in UANs (more specifically, underwater sensor networks). In [15], Kong *et al.* demonstrate the damage caused by wormhole links and also the inapplicability of traditional defenses based on distance bounding and localization. In [16], Wang *et al.* present a solution called Dis-VoW, which detects potential wormhole link by analyzing the distortions in edge lengths and angles among neighboring nodes in the reconstructed local topology. Dis-VoW depends on secure distance estimation for which there is no existing solution in UANs, while our solution does not have such requirement.

B. Our Contribution

Our major contribution in this paper is a set of wormhole-resilient secure neighbor discovery protocols for UANs, which is the first work of its kind. Our solution is based on the key observation that wormhole attackers cannot manipulate acoustic signals' directions of arrival (DoAs) so easily as signal power and transmission time, as DoAs are solely dependent on the relative locations of signal transmitters and receivers. Since the DoA estimations of a pair of true neighboring transceivers should satisfy some geometric relationships, this motivates us to exploit this nice property to build wormhole-resilient neighbor discovery in UANs. In contrast to related work, our solution has no traditional requirements such as secure and accurate time synchronization and localization and/or high node density. Instead, it only assumes that each node can estimate the DoAs of incoming acoustic signals, which is not a hard requirement because DoA estimation is a fundamental functionality readily available in most sonar systems for many underwater applications. Our solution consists of four protocols. The first protocol B-NDP involves two nodes in each instance of neighbor discovery, while the second protocol DV-NDP requires three nodes. DV-NDP dramatically improves the wormhole resilience of B-NDP at the cost of decreasing the probability of two true neighbors successfully discovering each other. The third protocol SDV-NDP turns DV-NDP into a deterministic wormhole-resilient protocol with little modification. By the last protocol MA-NDP, we show how to accommodate floating node mobility in UANs during the execution of B-NDP, DV-NDP, or SDV-NDP. All of our schemes can provide strong resilience to the wormhole attack. Their extraordinary performance is confirmed by comprehensive theoretical and simulation results.

II. Direction-of-Arrival Estimation

DoA estimation of acoustic signals is widely used in both military and commercial underwater applications. For example, from a communication point of view, if the DoA of the desired signal is known, adaptive beamforming algorithms can be performed to minimize the power of the interfering signals, which will in turn maximize the power of the desired signal [19]. In addition, in underwater warfare an accurate DoA estimation can enable underwater vehicles such as Torpedo to determine the locations of targets [20]. Moreover, the DoA estimation is also adopted to measure the seabed information in an Underwater Geographical Information System [21].

DoA estimation generally requires an array of hydrophones, which is a microphone designed to record or listen to underwater sound and the building block of modern active or passive sonar systems. Alternatively, DoA estimation can be realized via an array of vector sensors [22] which are formed by connected hydrophones and sensitive to the magnitude and direction of the acoustic waves. When a plane acoustic wave approaches the array of hydrophones or vector sensors from an unknown direction, it exerts a force on each hydrophone which is converted by the electronic components. Then the DoA can be estimated through analyzing the phase differences among the signals received by different hydrophones.

III. Network and Attacker Models

A. Network Model

We assume a UAN consists N nodes randomly distributed in a $\mathbf{D}^3$ cubic area. The transmission range of each node is a ball with radius R. Nodes may move proactively or unpredictably due to underwater current. We do not assume that nodes are synchronized or know their respective locations. Instead, we assume each node is equipped with an array of hydrophone or vector sensors to enable DoA estimation which are readily available in most underwater applications. For simplicity, we also assume that all the nodes have the same X, Y, and Z axis orientations with negligible errors. We intend to release this assumption in our future work. In addition, we assume that the channel is bidirectional: if node A can hear node B, then B can also hear A.

Secure neighbor discovery requires nodes to have proper keys to perform mutual authentication. For simplicity, we assume a key distribution scheme such as [5] based on Identity-Based Cryptography (IBC) [23]. In particular, each node A has an ID ID_A as its public key and an ID-based private key K_A^{-1} issued by a trusted authority prior to network deployment, which removes the need to transmit potentially lengthy keying information such as public-key certificates in other public key distribution schemes. This is very desirable

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

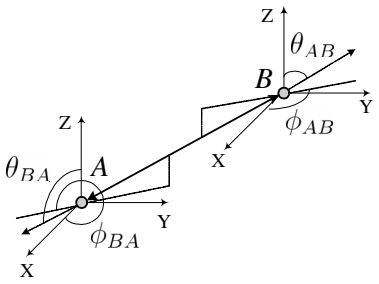


Fig. 1. The basic idea of wormhole detection with DoA estimation.

in UANs with limited link capacity. Our solution, however, does not preclude other key distribution schemes and the corresponding authentication methods.

B. Adversary Model

We focus on detecting wormhole attackers in this paper. Other important security issues in UANs are still open topics deserving investigation. The adversary aims to interrupt neighbor discovery and thus network operations by creating fake links between nodes which are actually outside each other's transmission range. To do so, the adversary places some wormhole links in the network. Each wormhole link is assumed to be bidirectional because unidirectional wormhole links do not affect neighbor discovery. To attack neighbor discovery, a wormhole attacker tunnels overheard related messages via the wormhole link to the other wormhole attacker which in turn rebroadcasts the messages to its neighborhood. Attackers may purposely introduce some random delays during this process, which nevertheless have no impact on our solution that does not rely on such timing information.

IV. Wormhole-Resilient Secure Neighbor Discovery

In this section, we present four wormhole-resilient secure neighbor discovery protocols (NDPs for short). The first scheme B-NDP involves two nodes, while the second scheme DV-NDP uses three with better wormhole resilience. The third scheme SDV-NDP further improves DV-NDP to realize deterministic detection of wormhole links. We finally present the last scheme MC-NDP to accommodate node mobility.

To ease the presentation, we will use the following terms and notations throughout the paper.

- *True neighbors*: Two nodes are called *true neighbors* if they are in each other's transmission range and both have authentic public/private keys issued by the authority.
- *Fake neighbors:* Two nodes are called *fake neighbors* if they are not true neighbors but can communicate via a wormhole link invisible to them.
- P_f: It is defined as the probability that a node establishes a neighboring relationship with a fake neighbor after a complete NDP execution.
- P_s: It is defined as the probability that two true neighbors can establish neighboring relationship.

We seek to maximize P_s while minimizing P_f.

A. B-NDP: A Basic Neighbor Discovery Protocol

This subsection presents a basic NDP (B-NDP for short). For clarity, we leave the discussion on the impact of node mobility during neighbor discovery to Section IV-D.

Protocol Description

We use nodes A and B as an example to illustrate B-NDP. Assume that A and B are true neighbors, as shown in Fig. 1. Let $\overrightarrow{AB}$ and $\overrightarrow{BA}$ denote the directions of signals from A to B and from B to A, respectively. It is easy to see that

$$\overrightarrow{AB} = -\overrightarrow{BA}\ . \tag{1}$$

Let θ_{UV} and ϕ_{UV} be the inclination and azimuth angles of an arbitrary direction $\overrightarrow{UV}$. We further have

$$\begin{cases} \theta_{AB} + \theta_{BA} = \pi\ , \\ \phi_{AB} - \phi_{BA} = \pm\pi\ . \end{cases} \tag{2}$$

Intuitively, A and B can verify that they are true neighbors by comparing their respective DoAs of incoming signals. The following authenticated NDP is based on this observation.

Assume that A wants to discover neighbors. It broadcasts the following request

$$A \rightarrow *:\ ID_A, n_A, \langle \text{prior-data} \rangle_{K_A^{-1}}\ ,$$

where n_A is a random nonce to thwart message replay attacks and $\langle\cdot\rangle_*$ denotes a digital signature operation with the private key at the subscript. After hearing the request, B estimates θ_{AB} and ϕ_{AB} as $\widehat{\theta_{AB}}$ and $\widehat{\phi_{AB}}$, respectively. Then it verifies $\langle \text{prior-data} \rangle_{K_A^{-1}}$ using ID_A as the public key [5]. If succeeds, B decides that A has authentic public/private keys and then unicasts the following message:

$$B \rightarrow A:\ ID_A, ID_B, \widehat{\theta_{AB}}, \widehat{\phi_{AB}}, n_B, \langle \text{prior-data} \rangle_{K_B^{-1}}\ ,$$

where n_B is a random nonce chosen by B. On receiving the reply, A estimates θ_{BA} and ϕ_{BA} as $\widehat{\theta_{BA}}$ and $\widehat{\phi_{BA}}$, respectively. Then it verifies $\langle \text{prior-data} \rangle_{K_B^{-1}}$ using ID_B as the public key to ascertain that $\widehat{\theta_{AB}}$ and $\widehat{\phi_{AB}}$ indeed come from B. If succeeds, A decides that B has authentic public/private keys. Finally, A checks if the following conditions hold:

$$\begin{cases} |\widehat{\theta_{AB}} + \widehat{\theta_{BA}} - \pi| \le 2\sigma_\theta\ , \\ |\widehat{\phi_{AB}} - \widehat{\phi_{BA}} \pm \pi| \le 2\sigma_\phi\ , \end{cases} \tag{3}$$

where σ_θ and σ_ϕ are system parameters and denote the predetermined maximum possible estimation errors of inclination and azimuth angles, respectively. If so, A accepts B as a true neighbor and sends the following reply:

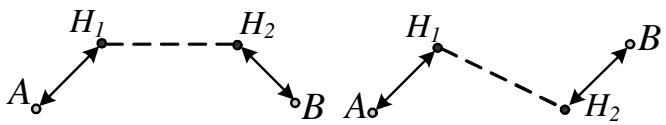
$$A \rightarrow B:\ ID_B, ID_A, \widehat{\theta_{BA}}, \widehat{\phi_{BA}}, \langle \text{prior-data} | n_A | n_B \rangle_{K_A^{-1}}\ .$$

On receiving the reply, B first verifies the digital signature. If it is valid, B further checks if the inequalities in Eq. (3) hold and accepts A as a true neighbor if so.

Performance Analysis

B-NDP can prevent attackers without authentic public/private keys from cheating good nodes into accepting them

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.



(a) An unsuccessful wormhole (b) A successful wormhole

Fig. 2. Wormhole attacks against B-NDP.

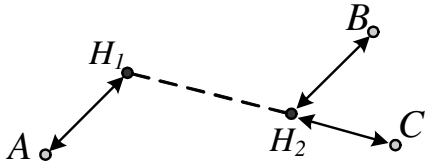


Fig. 3. Illustration of DV-NDP.

as a true neighbor. Since the DoA of a particular signal is solely dependent on the relative locations of the signal transmitter and receiver, B-NDP can defeat a randomly positioned wormhole link in most situations, e.g., Fig. 2(a), but may fail in some cases. Consider Fig. 2(b) as an example with a wormhole link H_1H_2. If $\overrightarrow{H_1A}$ is almost parallel to $\overrightarrow{BH_2}$, then the inequalities in Eq. (3) will hold with very high probability. Consequently, A and B will falsely accept each other as a true neighbor even though their authentication messages are tunneled via the wormhole link. Below we estimate the probability P_f of this situation occurring.

For simplicity, we subsequently assume that $\sigma_\theta = \sigma_\phi = \sigma < \pi/2$ and that the estimation errors of inclination and azimuth angles are two independent random variables both uniformly distributed between $[-\sigma, \sigma]$. If this assumption does hold, our following analysis can be modified with little effort. We then have the following theorem about P_f.

THEOREM *1: With B-NDP, each node will establish a neighboring relationship with a fake neighbor via a wormhole link with probability*

$$P_f = \frac{\sigma \sin(2\sigma)}{2}. \tag{4}$$

Proof: Consider the example in Fig. 2(b). The DoAs estimated by A and B are actually for $\overrightarrow{H_1A}$ and $\overrightarrow{H_2B}$, respectively. A and B will falsely accept each other as a true neighbor if the following inequalities hold.

$$\begin{cases} |\widehat{\theta_{H_2B}} + \widehat{\theta_{H_1A}} - \pi| \le 2\sigma \ , \\ |\widehat{\phi_{H_2B}} - \widehat{\phi_{H_1A}} \pm \pi| \le 2\sigma \ . \end{cases} \tag{5}$$

Denote by $\mathcal{C}_1$ and $\mathcal{C}_2$ the events that the first and second conditions in Eq. (5) hold, respectively. We first estimate the probability of $\mathcal{C}_1$ happening. Assume that A and B are randomly positioned within the transmission and reception ranges of the wormhole endpoints H_1 and H_2, respectively. Then θ_{H_2B} and θ_{H_1A} are two independent random variables with p.d.f.,

$$p(\theta = t) = \begin{cases} \frac{1}{2}\sin t, & \text{if} \quad 0 \le t \le \pi \ , \\ 0, & \text{otherwise} \ , \end{cases} \tag{6}$$

and so do $\widehat{\theta_{H_2B}}$ and $\widehat{\theta_{H_1A}}$ if we ignore the boundary situation. Then we have

$$\Pr(\mathcal{C}_1) = \int_0^{\pi} \int_{\pi-u-2\sigma}^{\pi-u+2\sigma} \frac{1}{4} \sin v \sin u \, dv \, du = \frac{\pi \sin(2\sigma)}{4} \ . \tag{7}$$

In contrast to θ_{H_2B} and θ_{H_1A}, ϕ_{H_2B} and ϕ_{H_1A} are two independent random variables uniformly distributed in the range $[0, 2\pi)$, and so do $\widehat{\phi_{H_2B}}$ and $\widehat{\phi_{H_1A}}$. Similarly, we can have $P(\mathcal{C}_2) = 2\sigma/\pi$ and finally compute

$$P_f = \Pr(\mathcal{C}_1)\Pr(\mathcal{C}_2) = \frac{\sigma \sin(2\sigma)}{2} \ .$$

■

In addition, since all pairs of true neighbors can successfully discover each other, we have $P_s = 1$ for B-NDP.

B. DV-NDP: A Double-Verification Neighbor Discovery Protocol

With B-NDP in mind, we now introduce a double-verification NDP (DV-NDP for short) to improve the wormhole resilience of B-NDP by requiring three nodes to establish mutual neighboring relationships at the same time.

Protocol Description

The basic idea of DV-NDP can be best illustrated with Fig. 3, in which A and B are fake neighbors. Assume that $\overrightarrow{H_1A}$ is almost parallel to $\overrightarrow{H_2B}$. Nodes A and B will falsely accept each other as a true neighbor under B-NDP. Now suppose that there is another node C which is also a fake neighbor of A and can be reached by H_2. DV-NDP requires A to accept either both B and C as true neighbors or neither of them. Therefore, A is affected by the wormhole link $\overrightarrow{H_1H_2}$ only when the angle formed by $\overrightarrow{H_2B}$ and $\overrightarrow{H_2C}$ is very small. DV-NDP thus can improve the resilience to wormhole attacks.

To be more specific, DV-NDP requires three nodes to engage in neighbor discovery. Consider nodes A, B, and C as an example. DV-NDP is a three-step process. In the *estimation* step, every node broadcasts a request of the same format in B-NDP, and here we assume a suitable MAC protocol to resolve possible collisions (e.g., using randomized broadcasting times). Every node thus will hear two requests and process them in the same way as in B-NDP, i.e., estimating the DoA and verifying the digital signature. After this step, A has ($\widehat{\theta_{BA}}$, $\widehat{\phi_{BA}}$) and ($\widehat{\theta_{CA}}$, $\widehat{\phi_{CA}}$); B has ($\widehat{\theta_{AB}}$, $\widehat{\phi_{AB}}$) and ($\widehat{\theta_{CB}}$, $\widehat{\phi_{CB}}$); C has ($\widehat{\theta_{AC}}$, $\widehat{\phi_{AC}}$) and ($\widehat{\theta_{BC}}$, $\widehat{\phi_{BC}}$). In the *exchange* step, every node broadcasts a reply containing all its DoA estimations. For example, A broadcasts the following message.

$$A \to *: ID_A, ID_B, \widehat{\theta_{BA}}, \widehat{\phi_{BA}}, ID_C, \widehat{\theta_{CA}}, \widehat{\phi_{CA}}, \\ \langle \text{prior-data} | n_A | n_B | n_C \rangle_{K_A^{-1}} \ ,$$

where n_A, n_B, and n_C are random nonces exchanged in the estimation step. In the final *decision* step, every node verifies the digital signatures in the received replies and then checks whether every pair of inclination and azimuth angles satisfy similar inequalities as in Eq. (3). If so, the DV-NDP

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

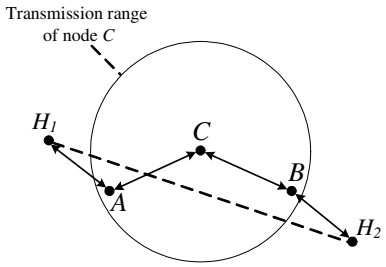


Fig. 4. An example of one pair of fake neighbors among three nodes.

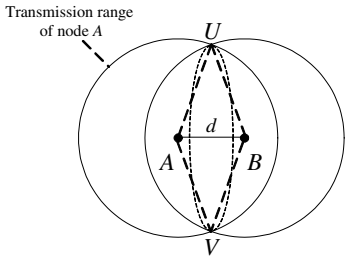


Fig. 5. The intersection of two balls.

instance is considered successful, and every node knows that they three have established pairwise neighboring relationships. Otherwise, the DV-NDP instance is deemed unsuccessful, and no new neighboring relationship should be established. Note that A, B, and C will reach a consensus since their decisions are based on the same broadcast information.

It is worth noticing that it is possible that two nodes among three may have already established neighboring relationship before the DV-NDP execution. In such cases, only two new neighboring relationships will be established.

Performance Analysis

Apparently, it is more difficult for the attacker to launch a successful wormhole attack under DV-NDP. Now we analyze its performance. We first have the following lemma.

LEMMA *1: Assuming that there are three nodes which can communicate either directly or via a wormhole link, there are at most two pairs of fake neighbors.*

Proof: Let m be the number of fake neighbor pairs among three nodes. The cases for $m = 1$ and $m = 2$ are shown in Fig. 4 and Fig. 3, respectively. We now show that $m \neq 3$.

Without loss of generality, we assume that (A, B) and (A, C) are two pairs of fake neighbors resulting from a wormhole link H_1H_2, that A is within the transmission range of H_1, and that B and C are within the transmission range of H_2. If B and C are true neighbors, then $m = 2$. Otherwise, they can communicate only if H_2 locally repeats what it receives from either of them. Let d_B be the distance between B and H_2 and d_C between C and H_2. Without loss of generality, we assume that $d_B \leq d_C$, which implies that if C hears H_2's transmission, so does B. Therefore, B will overhear its previous messages being repeated by H_2 to reach C and thus detect the attack. We thus have $m \neq 3$. ■

For $m = 1$ as in Fig. 4, the DV-NDP instance succeeds only when the inequalities in Eq. (3) hold. Due to the space limitation, we only briefly discuss the properties of such wormhole links and will ignore them in the rest of this paper.

- Since this wormhole link only decreases the path length between A and B by one hop, it has limited impact on the UAN operations.
- P_f in this case is lower than $\sigma \sin(2\sigma)/2$ in contrast to B-NDP, as H_1 and H_2 can no longer be positioned uniformly at random. In particular, they cannot reside in C's transmission range.

For $m = 2$ as in Fig. 3, we have the following theorem about P_f under DV-NDP.

THEOREM *2: With DV-NDP, a node with two fake neighbors via a wormhole link will establish false neighboring relationships with them with probability*

$$P_f \leq \frac{\sigma^2 \sin^2(2\sigma)}{4} \,. \tag{8}$$

Proof: Without loss of generality, we consider the scenario in Fig. 3, where B and C are true neighbors. According to the DV-NDP operations, A will establish false neighbor relationships with B and C if the following conditions

$$\begin{cases} |\widehat{\theta_{H_2X}} + \widehat{\theta_{H_1A}} - \pi| \leq 2\sigma \,, \\ |\widehat{\phi_{H_2X}} - \widehat{\phi_{H_1A}} \pm \pi| \leq 2\sigma \,, \end{cases} \tag{9}$$

hold for $X \in \{B, C\}$.

Denote by $\mathcal{C}_{1,X}$ and $\mathcal{C}_{2,X}$ the events that the first and second condition in Eq. (9) hold for node $X \in \{B, C\}$. Also let $\mathcal{C}_{\overline{BC}}$ be the event that nodes B and C are true neighbors. Then P_f can be estimated as

$$\begin{aligned} P_f &= \Pr(\mathcal{C}_{1,B}, \mathcal{C}_{1,C}, \mathcal{C}_{2,B}, \mathcal{C}_{2,C}, \mathcal{C}_{\overline{BC}}) \\ &\leq \Pr(\mathcal{C}_{1,B}, \mathcal{C}_{1,C}, \mathcal{C}_{2,B}, \mathcal{C}_{2,C}) \\ &= \Pr(\mathcal{C}_{1,B})\Pr(\mathcal{C}_{1,C})\Pr(\mathcal{C}_{2,B})\Pr(\mathcal{C}_{2,C}) \\ &= \frac{\sigma^2 \sin^2(2\sigma)}{4} \,, \end{aligned} \tag{10}$$

where the last equation is due to the proof of Theorem 1. ■

In the above proof, we do not evaluate $\Pr(\mathcal{C}_{\overline{BC}})$ because it depends on the transmission and reception ranges of H_2 which cannot be assumed.

In general, DV-NDP has a much lower P_f than B-NDP. This, however, comes with the price that some true neighbors may not be able to establish neighboring relationships due to the lack of a common true neighbor. We have the following theorem regarding P_s of DV-NDP.

THEOREM *3: With DV-NDP, two true neighbors with transmission range R in a $\mathbf{D}^3$ cubic area can establish a neighboring relationship with probability*

$$P_s \approx \frac{5(N-2)\pi R^3}{8\mathbf{D}^3} \,, \tag{11}$$

where N is the number of nodes.

Proof: Consider Fig. 5 as an example. Suppose that nodes A and B are true neighbors separated by a distance $d \leq R$. The volume of the intersection area of the two spheres can be computed as

$$V(d) = 2\int_{\frac{d}{2}}^{R} \pi(R^2 - t^2)\, dt = \pi(\frac{4R^3}{3} - R^2 d + \frac{d^3}{12}) \,, \tag{12}$$

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

where R is the transmission range of each node. For a given d, each of the other $N-2$ nodes appears in this intersection with probability $V(d)/\mathbf{D}^3$. Nodes A and B can establish a neighbor relationship if at least one of them is within this intersection, which happens with probability

$$P_s(d) = 1 - (1 - \frac{V(d)}{\mathbf{D}^3})^{N-2} \approx \frac{(N-2)V(d)}{\mathbf{D}^3} ,$$

because $V(d) \ll \mathbf{D}^3$.

Then P_s can be computed as

$$\begin{aligned} P_s &= \int_0^R P_s(t)p(d=t)\,dt \\ &\approx \int_0^R \frac{(N-2)\pi(\frac{4R^3}{3} - R^2t + \frac{t^3}{12})}{\mathbf{D}^3} \cdot \frac{3t^2}{R^3}\,dt \qquad (13) \\ &= \frac{5(N-2)\pi R^3}{8\mathbf{D}^3}. \end{aligned}$$

■

C. SDV-NDP: A Strict Double-Verification Neighbor Discovery Protocol

In this subsection, we turn DV-NDP into a deterministic scheme, called the Strict Double-Verification NDP (SDV-NDP for short), with little modification.

Protocol Description

From Fig. 3, we can observe that DV-NDP may fail only when $\overrightarrow{H_2B}$ and $\overrightarrow{H_2C}$ are very close to each other. If such cases can be avoided, we can detect wormhole links for sure. For this purpose, SDV-NDP requires each node to verify that any two nodes among three are not too close. Continue the example used in describing DV-NDP. In the final decision step of DV-NDP, in addition to the inequalities checks as in Eq. (9), A, B, and C all individually check that at least one inequality of each following inequality pairs holds: $|\widehat{\theta_{AB}} - \widehat{\theta_{AC}}| > 4\sigma$ and $|\widehat{\phi_{AB}} - \widehat{\phi_{AC}}| > 4\sigma$; $|\widehat{\theta_{BC}} - \widehat{\theta_{BA}}| > 4\sigma$ and $|\widehat{\phi_{BC}} - \widehat{\phi_{BA}}| > 4\sigma$; $|\widehat{\theta_{CB}} - \widehat{\theta_{CA}}| > 4\sigma$ and $|\widehat{\phi_{CB}} - \widehat{\phi_{CA}}| > 4\sigma$. If so, they can establish pairwise neighboring relationships. Since they make the decisions based on the same information, they can reach a consensus.

Performance Analysis

We now analyze the performance of SDV-NDP and have the following theorem.

THEOREM *4: With SDV-NDP, a node with two fake neighbors via a wormhole link will establish false neighboring relationships with them with probability* $P_f = 0$.

Proof: Similar to the proof of Theorem 5, we consider the scenario in Fig. 3 as an example. Due to the wormhole link H_1H_2, A is actually checking $|\widehat{\theta_{H_2B}} - \widehat{\theta_{H_2C}}| > 4\sigma$ and $|\widehat{\phi_{H_2B}} - \widehat{\phi_{H_2C}}| > 4\sigma$, respectively, while believing that it is checking $|\widehat{\theta_{AB}} - \widehat{\theta_{AC}}| > 4\sigma$ and $|\widehat{\phi_{AB}} - \widehat{\phi_{AC}}| > 4\sigma$. Now we prove that the inequality checks in Eq. (9) will fail if either of the two additional inequalities holds. For example, assuming that $|\widehat{\theta_{H_2B}} - \widehat{\theta_{H_2C}}| > 4\sigma$, the two inequalities related to the inclination angle in Eq. (9)

$$\begin{cases} |\widehat{\theta_{H_2B}} + \widehat{\theta_{H_1A}} - \pi| \le 2\sigma, \\ |\widehat{\theta_{H_2C}} + \widehat{\theta_{H_1A}} - \pi| \le 2\sigma, \end{cases} \qquad (14)$$

cannot hold at the same time. We prove this by contradiction. Assume that all these three inequalities hold. Then we have $|\widehat{\theta_{H_2B}} + \widehat{\theta_{H_1A}} - \pi| \ge |\widehat{\theta_{H_2B}} - \widehat{\theta_{H_2C}}| - |-\widehat{\theta_{H_2C}} - \widehat{\theta_{H_1A}} + \pi| > 2\sigma$, where we have used the property $|x-y| \ge |x| - |y|$. This clearly results in a contradiction. Similarly, if $|\widehat{\phi_{H_2B}} - \widehat{\phi_{H_2C}}| > 4\sigma$, the inequalities $|\widehat{\phi_{H_2B}} - \widehat{\phi_{H_1A}} \pm \pi| \le 2\sigma$ and $|\widehat{\phi_{H_2C}} - \widehat{\phi_{H_1A}} \pm \pi| \le 2\sigma$ cannot be satisfied simultaneously. ■

SDV-NDP can detect any wormhole link at the cost of decreasing P_s as compared to DV-NDP, to which we have not been able to give a closed-form solution. Instead, we will evaluate P_s using simulations in Section V.

D. MA-NDP: A Mobility-Aware Neighbor Discovery Protocol

Nodes in UANs may move proactively or unpredictably due to underwater current. So far we have ignored the impact of node mobility during neighbor discovery. In this subsection, we present a mobility-aware NDP (MA-NDP for short) which can be built upon B-NDP, DV-NDP, or SDV-NDP. In the following, we illustrate MA-NDP using B-NDP for simplicity.

Protocol Description

We first examine the impact of node mobility. Consider Fig. 6 as an example. Assume that node A moves with a velocity $\overrightarrow{V_{AB}}$ relative to node B. Suppose that A follows B-NDP to broadcast a request at location L. Due to the low propagation speed of acoustic signals, A has moved to location L' by the time it receives the response from B. It is easy to see that Eq. (2) no longer holds. Instead, now we have

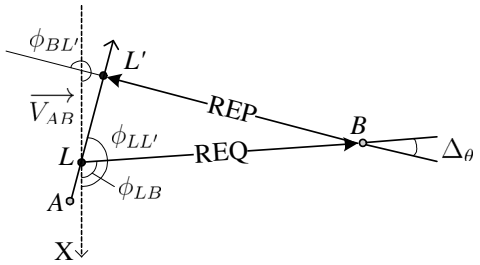


Fig. 6. The impact of node mobility.

$$\begin{cases} \theta_{LB} + \theta_{BL'} + \Delta\theta = \pi , \\ \phi_{LB} - \phi_{BL'} - \Delta\phi = \pm\pi , \end{cases} \qquad (15)$$

where $\Delta\theta$ is plotted in Fig. 6. For simplicity, $\Delta\phi$ is not shown but can be well understood. Intuitively, the comparisons of DoA estimations in B-NDP must tolerate the maximum possible $\Delta\theta$ and $\Delta\phi$. Note that B may also have moved to a new location when receiving A's last reply, but this has no impact on DoA estimations which are done only for A's request and B's reply.

We first estimate the maximum value of $\Delta\theta$. Let $\overrightarrow{V_{Aw}}$ and $\overrightarrow{V_{Bw}}$ denote the velocities of A and B relative to their surroundings, respectively, and $\overrightarrow{w_A}$ and $\overrightarrow{w_B}$ the absolute velocities

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

of the underwater current around A and B, respectively. We assume that $\overrightarrow{V_{Aw}}$ and $\overrightarrow{V_{Bw}}$ do not change during the protocol execution. Then $\overrightarrow{V_{AB}}$ is given by

$$\overrightarrow{V_{AB}} = \overrightarrow{V_{Aw}} + \overrightarrow{w_A} - \overrightarrow{V_{Bw}} - \overrightarrow{w_B} \ . \tag{16}$$

Assume that A broadcasts the request at time t and receives B's reply at time $t + \Delta t$ according to its local clock. For simplicity, we neglect message transmission and processing delays which are considerably shorter than the propagation delays. Let c denote the propagation speed of underwater acoustic waves. We have

$$\begin{cases} |LL'| = |\overrightarrow{V_{AB}}| \cdot \cos\alpha \cdot \Delta t \ , \\ |LB| + |L'B| = c \cdot \cos\alpha \cdot \Delta t \ , \end{cases} \tag{17}$$

where α is the angle between $\overrightarrow{V_{AB}}$ and the Y-Z plane, and $|\overrightarrow{V_{AB}}| \cdot \cos\alpha$ is the $\overrightarrow{V_{AB}}$'s component on the Y-Z plane.

Given Δt, $\Delta\theta$ is maximized when the triangle $LL'Q$ is an isosceles triangle. Then we have

$$\Delta\theta_{max} = 2\arcsin\frac{|LL'|}{|LB| + |L'B|} = 2\arcsin\frac{|\overrightarrow{V_{AB}}|}{c} \ , \tag{18}$$

which is actually independent of Δt.

Assume that $\overrightarrow{V_{Aw}}$ and $\overrightarrow{V_{Bw}}$ are known by nodes A and B, respectively, but $\overrightarrow{w_A}$ and $\overrightarrow{w_B}$ are not. We let $\overrightarrow{V_{A-B}} = \overrightarrow{V_{Aw}} - \overrightarrow{V_{Bw}}$ and assume that $\overrightarrow{w_A}$ and $\overrightarrow{w_B}$ are two random vectors with their absolute values w_A and w_B uniformly distributed in $[0, \nu]$. Then $|V_{AB}|$ is maximized when $\overrightarrow{w_A} = (\nu, \theta_{V_{A-B}}, \phi_{V_{A-B}})$ and $\overrightarrow{w_B} = (\nu, \pi - \theta_{V_{A-B}}, \pi + \phi_{V_{A-B}})$, i.e., when $\overrightarrow{w_A}$ has the same direction as $\overrightarrow{V_{A-B}}$, $\overrightarrow{w_B}$ is in the opposite direction to $\overrightarrow{w_A}$, and both w_A and w_B attain the maximum value ν. Then we can have

$$\Delta\theta_{\max} = 2\arcsin\frac{|\overrightarrow{V_{A-B}}| + 2\nu}{c} \ . \tag{19}$$

Similarly, we can have the maximum value of $\Delta\phi$ as

$$\Delta\phi_{\max} = 2\arcsin\frac{|\overrightarrow{V_{A-B}}| + 2\nu}{c} \ . \tag{20}$$

Now we introduce the MA-NDP operations. Roughly speaking, two nodes exchange their relative velocities and DoA estimations. Then they compare mutual DoA estimations and accept each other as a true neighbor if certain conditions are met. More specifically, assume that node A initiates neighbor discovery by broadcasting a request as in B-NDP.

$$A \to * : \ ID_A, n_A, \overrightarrow{V_{Aw}}, \langle \text{prior-data} \rangle_{K_A^{-1}} \ .$$

On receiving the request, B estimates θ_{AB} and ϕ_{AB} as $\widehat{\theta_{AB}}$ and $\widehat{\phi_{AB}}$, respectively, and verifies the signature as in B-NDP. If succeeds, B unicasts the following message.

$$B \to A : \ ID_A, ID_B, \widehat{\theta_{AB}}, \widehat{\phi_{AB}}, n_B, \overrightarrow{V_{Bw}}, \langle \text{prior-data} \rangle_{K_B^{-1}} \ .$$

On receiving the reply, A estimates θ_{BA} and ϕ_{BA} as $\widehat{\theta_{BA}}$ and $\widehat{\phi_{BA}}$, respectively, and then verifies the signature. If the signature is authentic, A considers B has authentic public/private keys. Next, A computes $\Delta\theta_{max}$ and $\Delta\phi_{max}$ as in Eqs. (19) and (20) and checks if the following inequalities hold.

$$\begin{cases} |\widehat{\theta_{AB}} + \widehat{\theta_{BA}} - \pi| \le \Delta\theta_{max} + 2\sigma \\ |\widehat{\phi_{AB}} - \widehat{\phi_{BA}} \pm \pi| \le \Delta\phi_{max} + 2\sigma \ . \end{cases} \tag{21}$$

If so, A accepts B as a true neighbor and sends the following reply.

$$A \to B : \ ID_B, ID_A, \widehat{\theta_{BA}}, \widehat{\phi_{BA}}, \langle \text{prior-data} | n_A | n_B \rangle_{K_A^{-1}} \ .$$

On receiving the reply, B first verifies the signature. If the signature verification is successful, B proceeds to compute $\Delta\theta_{max}$ and $\Delta\phi_{max}$ as in Eqs. (19) and (20) and check whether the inequalities in Eq. (21) hold. If so, B accepts A as a true neighbor. Since A and B make their decisions based on the same information, they can reach a consensus. DV-NDP and SDV-NDP can be modified accordingly to accommodate node mobility during protocol execution.

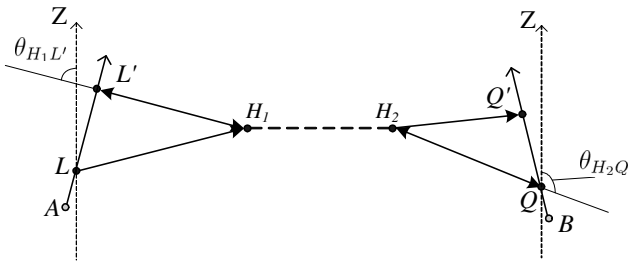


Fig. 7. Wormhole attacks against MC-NDP.

Performance Analysis

We now analyze the performance of MA-NDP. We have the following theorem regarding the wormhole resilience of MA-NDP, where we assume that two nodes move with the same speed v for simplicity.

THEOREM *5: Assume that A and B moving with the same speed v in two independently random directions are fake neighbors via a wormhole link. They will falsely accept each other as a true neighbor under MA-NDP (built on B-NDP) with probability*

$$P_f = \frac{1}{4\pi}\int_0^{\pi} g(\varphi)\sin(g(\varphi))\, d\varphi \ , \tag{22}$$

where $g(\varphi) = 2(\arcsin\frac{v\sqrt{2-\cos\varphi}+2\nu}{c} + \sigma)$.

Proof: Without loss of generality, consider Fig. 7 as an example. Assume that A broadcasts the neighbor-discover request at location L and receives a reply from B tunneled via the wormhole link at location L', while B receives the broadcast request from A at location Q and the last reply from A at location Q', both tunneled via the wormhole link. Recall that A estimates the DoA when receiving B's reply and that B estimates the DoA when receiving A's request. The wormhole attack will succeed only if the following conditions hold.

$$\begin{cases} |\widehat{\theta_{H_2Q}} + \widehat{\theta_{H_1L'}} - \pi| \le \Delta\theta_{max} + 2\sigma \ , \\ |\widehat{\phi_{H_2Q}} - \widehat{\phi_{H_1L'}} \pm \pi| \le \Delta\phi_{max} + 2\sigma \ , \end{cases} \tag{23}$$

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

where $\Delta\theta_{\max} = \Delta\phi_{\max} = 2\arcsin\frac{|V_{A-B}|+2\nu}{c}$ as given in Eqs. (19) and (20). Note that if the wormhole link endpoints H_1 and H_2 move during the MA-NDP execution, then we can view H_1 and H_2 in Eq. (23) as the locations at which H_1 broadcasts B's reply and H_2 broadcasts A's request, respectively. Similar to the proof of Theorem 1, for a given $\Delta\theta_{max}$, we have

$$P_f(\Delta\theta_{max}) = \frac{(\Delta\theta_{max}+2\sigma)\sin(\Delta\theta_{max}+2\sigma)}{4} . \quad (24)$$

Assume that A and B move with the same speed v in two independently random directions. The angel formed by $\overrightarrow{V_{Aw}}$ and $\overrightarrow{V_{Bw}}$, denoted by φ, is uniformly distributed in $[0,\pi]$. For a given φ, we then have

$$|\overrightarrow{V_{A-B}}| = v\sqrt{2-2\cos\varphi} . \quad (25)$$

It follows that, for given φ,

$$P_f(\varphi) = \frac{g(\varphi)\sin(g(\varphi))}{4} , \quad (26)$$

where $g(\varphi) = 2(\arcsin\frac{v\sqrt{2-\cos\varphi}+2\nu}{c} + \sigma)$.

Finally, we can derive

$$P_f = \int_0^\pi P_f(\varphi)p(\varphi)\,d\varphi = \frac{1}{4\pi}\int_0^\pi g(\varphi)\sin(g(\varphi))\,d\varphi .$$

■

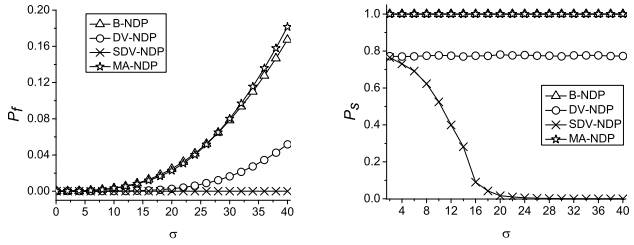
In addition, every two true neighbors can establish a neighboring relationship under MA-NDP, and we thus have $P_s = 1$.

V. Performance Evaluation

In this section, we use simulations to evaluate the proposed four protocols. We simulate a UAN with 800 nodes uniformly distributed in a $5 \times 5 \times 5$ km^3 cubic area. Each node has a transmission range 500 m. Note that we are not interested in the network connectivity which has no impact on our schemes. The following configurations are used unless otherwise stated. We set $\sigma = 10^\circ$ to show our schemes' high tolerance to large measurement errors, while recent experimental study shows that $\sigma < 2^\circ$ in practice [22]. In addition, nodes are static for B-NDP, DV-NDP, and SDV-NDP, and they move at a speed of 20 m/s in random directions for MA-NDP. We also assume that the propagation speed of acoustic signals is 1500 m/s and that the water current speed ν is 2 m/s. For our purpose, the simulation code is written in C++. Each measurement is the average over 100 runs, each with a different random seed.

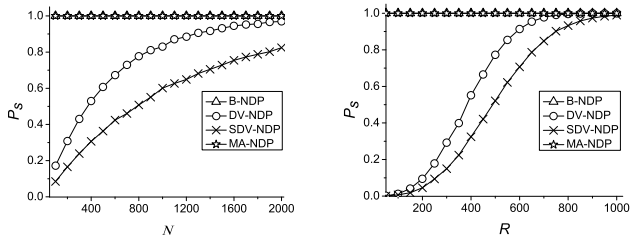
A. Simulation Results

1) The impact of σ: Fig. 8(a) shows the impact of the DoA measurement error σ on P_f. It is not surprising to see that the larger σ, the higher P_f, and vice versa. Note that all the four protocols do not require highly accurate DoA estimations. For example, even if $\sigma = 10^\circ$, which is often considered rather inaccurate in practice, all of them can prevent establishing fake neighboring relationships with probability higher than 0.98. In general, MA-NDP has the highest P_f due to node mobility, followed by B-NDP, while DV-NDP and SDV-NDP have a P_f close and equal to zero, respectively.



(a) P_f vs. σ (b) P_s vs. σ

Fig. 8. The impact of σ.



(a) P_s vs. N (b) P_s vs. R

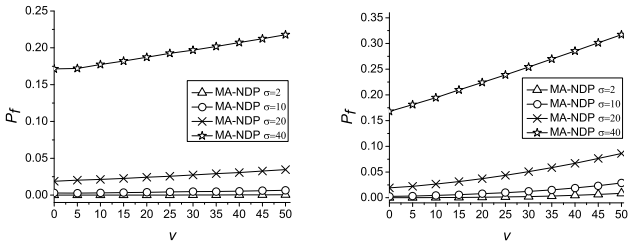
Fig. 9. The impact of N and R.

Fig. 8(b) shows the impact of σ on P_ss. We can see that B-NDP and MA-NDP both have $P_s = 1$, and DV-NDP has $P_s \approx 0.77$ independent of σ. These results coincide with our previous theoretical analysis. In contrast, the P_s of SDV-NDP decreases rapidly as σ increases and approaches zero when $\sigma = 24^\circ$ due to the added constraints on DoA comparisons. It is worth noting that a P_s smaller than one does not mean that the network will be disconnected, as two nodes that fail to establish direct neighboring relationship may still be able to communicate via other intermediate nodes.

2) The impact of N and R: Fig. 9(a) and Fig. 9(b) show the impact of the number N of nodes and the transmission range R on P_s. We can see that the P_ss of B-NDP and MA-NDP are not affected by N or R, while those of DV-NDP and SDV-NDP both increase as N or R increases. These results are expected because DV-NDP and SDV-NDP both involve three nodes for a successful execution, and the larger N or R, the higher the possibility of three nodes being mutually true neighbors.

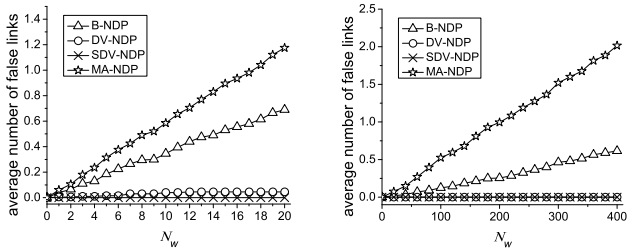
3) The impact of v: Fig. 10(a) shows the impact of the moving speed v on MA-NDP under different σs. As we can see, v has limited impact on P_f. The reason is that v is relatively small in contrast to the propagation speed, i.e., 1500 m/s, and in practice few underwater vehicles can move with a speed over 50 m/s, i.e., 100 knots. The same trend is observed in Fig. 10(b), in which the moving speed is uniformly distributed in $[0, 2v]$.

4) The impact of multiple wormhole links: Fig. 11(a) and Fig. 11(b) show the average number of false neighboring relationships established under different numbers of wormhole links, where σ are set to 10° and 2°, respectively. Here we assume that the wormhole endpoints have the same transmis-



(a) Fixed v (b) Random v

Fig. 10. The impact of v on MA-NDP.



(a) $\sigma = 10°$ (b) $\sigma = 2°$

Fig. 11. The impact of number of wormhole links.

sion and reception ranges as UAN nodes. From Fig. 11(a), we can see that our protocols can effectively prevent establishing false neighboring relationships. In particular, when $\sigma = 10°$, the adversary need deploy more than 15 wormhole links to successfully establish one false neighboring relationship for MA-NDP and much more for the other protocols. In addition, Fig. 11(b) shows that when $\sigma = 2°$, which is more practical in reality [22], the adversary need place over 200 wormhole links to create a false neighboring relationship under MA-NDP and B-NDP, and it is almost impossible for the adversary to launch a successful wormhole attack against DV-NDP and SDV-NDP.

B. Summary

We summarize the evaluation results as follows.

- B-NDP can prevent fake neighbors from establishing neighboring relationships with very high probability while enabling all true neighbors to discover each other.
- DV-NDP can prevent fake neighbors from establishing neighboring relationships with probability close to one at the cost of few lost links.
- SDV-NDP can detect any wormhole link for sure at the price of more lost links than in DV-NDP.
- MA-NDP can detect randomly positioned wormhole links with very high probability and accommodate node mobility.

In practice, B-NDP and MA-NDP are suitable for UANs with relatively low density and applications where network connectivity and end-to-end latency are of primary concerns. In contrast, DV-NDP and SDV-NDP are more suitable for applications with relatively high node density and extremely high requirements for wormhole resilience.

ACKNOWLEDGMENT

This work was supported in part by the US National Science Foundation under grants CNS-0716302 and CNS-0844972 (CAREER). We would also like to thank anonymous reviewers for their constructive comments and helpful advice.

REFERENCES

[1] E. M. Sozer, M. Stojanovic, and J. G. Proakis, "Undersea acoustic networks," *IEEE Journal of Oceanic Engineering*, vol. OE-25, no. 1, pp. 72–83, Jan. 2000.
[2] J. Proakis, E. Sozer, J. Rice, and M. Stojanovic, "Shallow water acoustic networks," *IEEE Communications Magazine*, vol. 39, no. 11, pp. 114–119, Nov 2001.
[3] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: Research challenges," *Ad Hoc Networks (Elsevier)*, vol. 3, pp. 257–279, May 2005.
[4] P. Papadimitratos, *et al.*, "Secure neighborhood discovery: a fundamental element for mobile ad hoc networking," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132–139, February 2008.
[5] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE J. Select. Areas Commun., Special Issue on Security in Wireless Ad Hoc Networks*, vol. 24, no. 2, pp. 247–260, Feb. 2006.
[6] S. Capkun, L. Buttyn, and J.-P. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks," in *ACM SASN'03*, Fairfax, VA, USA, Oct. 2003, pp. 21–32.
[7] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "TrueLink: A practical countermeasure to the wormhole attack," in *ICNP'06*, Santa Barbara, CA, Nov. 2006, pp. 75–84.
[8] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," in *IEEE INFOCOM'03*, San Francisco, CA, Apr. 2003, pp. 1976–1986.
[9] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wirel. Netw.*, vol. 13, no. 1, pp. 27–59, 2007.
[10] K. Bonne Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *SecureComm'07*, Nice, France, Sept. 2007, pp. 331–340.
[11] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *INFOCOM'07*, Anchorage, Alaska, USA, May 2007, pp. 107–115.
[12] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," in *ICNP'09*, Princeton, NJ, Oct. 2009, pp. 314–323.
[13] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *NDSS'04*, San Diego, CA, Feb. 2004.
[14] R. Shokri, *et al.*, "A practical secure neighbor verification protocol for wireless sensor networks," in *WiSec'09*, Zurich, Switzerland, Mar. 2009, pp. 193–200.
[15] J. Kong, *et al.*, "Low-cost attacks against packet delivery, localization and time synchronization services in under-water sensor networks," in *ACM WiSe'05*, Cologne, Germany, 2005, pp. 87–96.
[16] W. Wang, J. Kong, B. K. Bhargava, and M. Gerla, "Visualisation of wormholes in underwater sensor networks: a distributed approach." *IJSN*, vol. 3, no. 1, pp. 10–23, 2008.
[17] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Secure neighbor discovery in wireless networks: formal investigation of possibility," in *ASIACCS'08*, Tokyo, Japan, Mar. 2008, pp. 189–200.
[18] ——, "Towards provable secure neighbor discovery in wireless networks," in *ACM FMSE'08*, Alexandria, VA, Oct. 2008, pp. 31–42.
[19] B. Van Veen and K. Buckley, "Beamforming: a versatile approach to spatial filtering," *ASSP Magazine*, vol. 5, no. 2, pp. 4–24, April 1988.
[20] Y. Zhou, P. Yip, and H. Leung, "Tracking the direction-of-arrival of multiple moving targets by passive arrays: algorithm," *IEEE Transactions on Signal Processing*, vol. 47, no. 10, pp. 2655–2666, Oct 1999.
[21] D. J. Wright and D. J. Barlett, *Marine and Coastal Geographical Information Systems*, 1st ed. Taylor & Francis, Apr. 2007.
[22] W. Zhang, L. Guan, G. Zhang, C. Xue, K. Zhang, and J. Wang, "Research of DOA estimation based on single MEMS vector hydrophone," *Sensors*, vol. 9, no. 9, pp. 6823–6834, Aug. 2009.
[23] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *CRYPTO'01*, Santa Barbara, CA, Aug. 2001, pp. 213–229.