Visualisation of wormholes in underwater sensor networks: a distributed approach

Weichao Wang*

Department of Software and Information Systems,
University of North Carolina at Charlotte, NC 28223, USA
E-mail: weichaowang@uncc.edu
*Corresponding author

Jiejun Kong

Computer Science Department,
University of California,
Los Angeles, CA 90095, USA
E-mail: jkong@cs.ucla.edu

Bharat Bhargava

Department of Computer Sciences,
Purdue University, W. Lafayette, IN 47907, USA
E-mail: bb@cs.purdue.edu

Mario Gerla

Computer Science Department,
University of California,
Los Angeles, CA 90095, USA
E-mail: gerla@cs.ucla.edu

Abstract: We propose a distributed mechanism, Dis-VoW, to detect wormhole attacks in under-water sensor networks. In Dis-VoW, every sensor reconstructs local network layout using multi-dimensional scaling. It detects the wormholes by visualising the distortions in edge lengths and angles among neighbouring sensors. The contributions include:

- Dis-VoW does not depend on any special hardware
- it provides a localised wormhole detection mechanism adapting to network topology changes
- it integrates techniques from social science and scientific visualisation to attack network security problems.

The simulation results show that Dis-VoW can detect most of the fake neighbour connections without introducing many false alarms.

Keywords: wormhole attack; underwater sensor networks; localised reconstruction; distributed detection; visualisation.

Reference to this paper should be made as follows: Wang, W., Kong, J., Bhargava, B. and Gerla, M. (2008) 'Visualisation of wormholes in underwater sensor networks: a distributed approach', *Int. J. Security and Networks*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: 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 IEEE, ACM and ASEE.

Jiejun Kong is a post-doctoral researcher in Computer Science Department, University of California at Los Angeles (UCLA). He is interested in developing efficient, scalable and secure network protocols for wireless networks. His research topics include secure and anonymous routing, authentication, access control, distributed data harvesting and network security modelling in mobile wireless networks, in particular those with challenging network constraints and with high security demands, such as mobile ad hoc networks and underwater sensor networks.

Bharat Bhargava is a Professor in the Department of Computer Sciences and the School of Electrical and Computer Engineering at Purdue University, Indiana. He received his PhD from Purdue University. He is a fellow of IEEE and IETE. He has been awarded the charter Gold Core Member distinction by the IEEE Computer Society. In 1999, he received the IEEE Technical Achievement Award for a major impact of his decade long contributions to foundations of adaptability in communication and distributed systems.

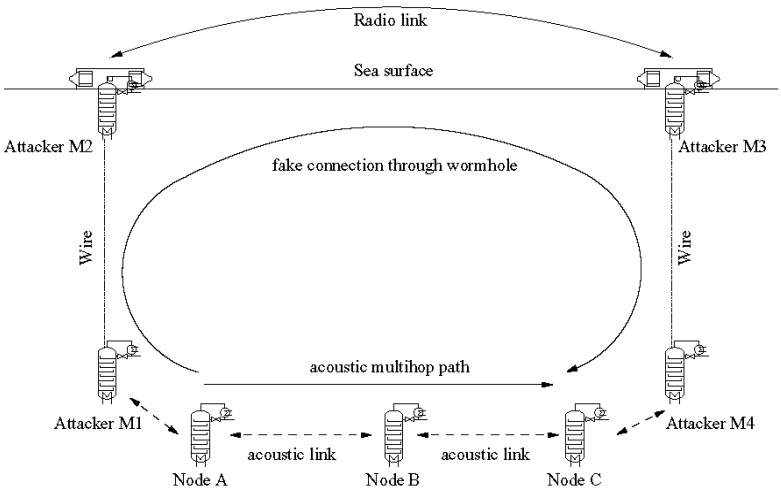
Mario Gerla received a graduate Degree in Engineering from the Politecnico di Milano, in 1966, and the MS and PhD Degrees in Engineering from UCLA in 1970 and 1973, respectively. He joined the Faculty of the UCLA Computer Science Department in 1977. His research interests cover the performance evaluation, design and control of distributed computer communication systems; high speed computer networks; wireless LANs (Bluetooth); ad hoc wireless networks and next generation internet. He is an IEEE fellow.

1 Introduction

The still largely unexplored vastness of the ocean, covering about 70% of the surface of the Earth, has attracted many investigators. Among various monitoring and exploration tools, underwater sensor networks (Xie and Gibson, 2000; Sozer et al., 2000; Proakis et al., 2001; Akyildiz et al., 2005; Kong et al., 2005a) play an important role in the investigation of emergent events, including marine incidents (e.g., monitoring oil spill areas) and military operations (e.g., submarine hunting or rescuing). The sensors can be deployed in a timely manner to cover a large body of water, and the information can be collected efficiently through a self-organised network. These features of underwater sensor networks satisfy the requirements of building a scalable and distributed data acquisition environment for the applications mentioned above.

Underwater sensor networks, although sharing many properties with their land-based counterparts, pose some new challenges to security. For example, low cost attacks on packet delivery and localisation in such environments have been investigated by Kong et al. (2005b). In this paper, we focus on the detection of wormhole attacks. Since the sensors use a shared acoustic channel to send information in underwater environments, the malicious nodes can eavesdrop on the packets, tunnel them to another location in the network, and retransmit them. This attack generates a false scenario that the original sender is in the neighbourhood of the remote location. One example of wormhole attacks is illustrated in Figure 1. The malicious nodes M1 to M4 use wires and a radio channel to accomplish the tunnelling procedure so that node A and C will assume that they are direct neighbours. The attacks generate fake neighbour connections and can be used to conduct the 'rushing attack' (Hu et al., 2003b) to compromise the routing topology.

Figure 1 Wormhole attacks in underwater sensor networks



Wormhole attacks pose severe threats to both routing protocols and some security enhancements in underwater sensor networks. For example, the sensors may depend on the neighbour discovery procedures to construct local network topology. If the neighbour discovery beacons are tunnelled through wormholes, the good nodes will get false information about their neighbours. This may lead to the choice of a non-existent route. The impacts of wormholes on the route discovery procedures in a sensor network have been studied by Hu and Evans (2004) and Kong et al. (2005b). The simulation results show that when there are more than two wormholes in the network, more than 50% of the data packets will be attracted to the fake connections and get discarded.

The special features of underwater environments greatly increase the difficulties in developing a wormhole detection mechanism. First, as opposed to land-based sensor networks, the positions of sensors are not restricted by the terrain of the deployment area and the relative distances among them will continuously change because of water current. Therefore, wormholes can be formed dynamically when the network topology changes. Second, the sensors have to use acoustic signals to transfer information. Acoustic signals transfer at only about 1500 m/s in water, which is much slower than the speed of radio waves. This slow propagation speed provides a longer interval for the malicious nodes to accomplish the tunnelling procedure. Therefore, a distributed wormhole detection mechanism must be developed to identify the fake neighbour connections based on the localised network topology.

Several approaches (Hu et al., 2003a; Capkun et al., 2003; Hu and Evans, 2004; Wang and Bhargava, 2004; Poovendran and Lazos, 2007) have been proposed to defend against wormhole attacks in land-based wireless networks. However, several difficulties may prevent these approaches from being applied to the underwater environment. For example, since GPS signals become very weak under water, the sensors cannot accurately determine their positions. Therefore, it is difficult to verify a neighbour relation by calculating the distance between two sensors based on their coordinates. Moreover, the round-trip time of a packet transfer cannot be used to verify a neighbour relation when the slow propagation speed of acoustic signals is considered.

MDS-VoW (Wang and Bhargava, 2004) is a wormhole detection mechanism that does not depend on any special hardware. When trying to apply MDS-VoWto underwater sensor networks, we find that two problems must be solved:

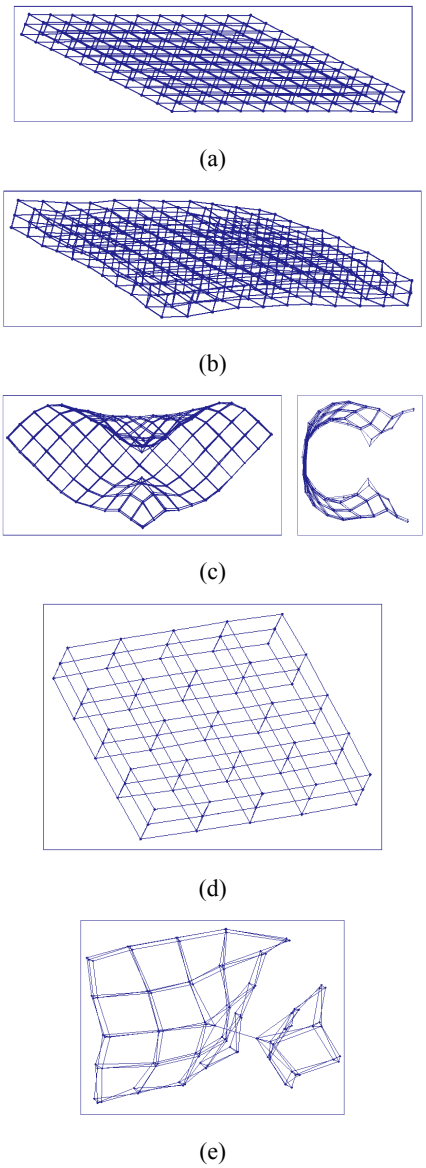
- MDS-VoW assumes that the sensors are deployed in a two dimensional space. However, in underwater sensor networks, the nodes can move freely in a three-dimensional (3D) environment.
- MDS-VoW is a centralised mechanism in which a controller will execute all computation and detection operations.

When frequent topology changes caused by water current are considered, a distributed approach is preferred.

In this paper, we propose a new mechanism, Distributed Visualisation of Wormhole (Dis-VoW), to defend against such attacks in underwater sensor networks. In Dis-VoW, every sensor will collect the distance estimations from its neighbours and reconstruct the local network topology within two hops using Multi-Dimensional Scaling (MDS). It will then use the distortions in edge lengths and angles among neighbouring sensors in the reconstructed network to locate the fake neighbour connections.

Before presenting the details of the mechanism, we illustrate the impacts of wormholes on network reconstruction through several examples. Figure 2(a) shows the original layout of a sensor network in a 3D environment when the nodes are placed as an $11 \times 11 \times 3$ grid. A part of neighbour connections among the sensors are illustrated as lines to assist the understanding of the topology. Figure 2(b) shows the global reconstruction of the network using MDS when there is no wormhole in the network, and we find that the layout is preserved very well. In Figure 2(c), a wormhole links two sensors that are not neighbours, and MDS bends the reconstructed network to fit the fake neighbour connection. In Figure 2(d) and (e), we show the reconstruction results of the same part of the network within two hops to a sensor, without and with a wormhole in it, respectively. Through the reconstruction results, we can easily see the distortions caused by the fake neighbour connection. Dis-VoW will detect these distortions and use them to locate the wormhole.

Figure 2 Impacts of wormholes on network reconstruction: (a) original sensor layout: an $11 \times 11 \times 3$ grid; (b) global reconstruction result when no wormhole exists; (c) global reconstruction result when a wormhole exists: the figures show the result from the front and left side; (d) localised reconstruction: no wormhole and (e) localised reconstruction: one wormhole



(a) (b) (c) (d) (e)

Dis-VoW consists of four steps:

- Every sensor will estimate the distances to its neighbours using the round-trip time of acoustic signals.
- Through broadcasting these distances, every sensor will be able to use MDS to reconstruct the local topology within two hops.
- Every sensor will examine the reconstructed network. If distortions are discovered, the wormhole detection method will be activated so that the fake neighbour connections can be located.
- The detected wormholes will be avoided during routing discovery and packet forwarding so that network safety and performance are preserved.

As we will demonstrate, the proposed mechanism can effectively identify the fake neighbour connections. The contributions of Dis-VoW can be summarised as follows:

- The proposed mechanism does not depend on any special hardware and the unit cost of sensors will not be impacted.
- Since every sensor reconstructs the network topology and detects the wormholes in a localised manner, the computation and storage overhead is affordable for a weak node such as a sensor. Therefore, distributed detection can be conducted when the network topology changes.
- Techniques from social science and scientific visualisation are integrated to solve network security problems.

The remainder of the paper is organised as follows: In Section 2, we review the previous research that contributes to our approach. Section 3 describes the building blocks of Dis-VoW and the algorithm in detail. Section 4 presents the experimental results acquired through simulation. Two scenarios, grid placement and random placement of the sensors, are studied. Section 5 discusses the safety of Dis-VoW, the frequency to conduct wormhole detection, and future work. Section 6 concludes the paper.

2 Related work

2.1 Underwater sensor networks

There has been an increasing interest in monitoring the marine environment for scientific exploration, commercial exploitation, and coastline protection. The ideal vehicle for these applications is a scalable underwater sensor network, which employs a large number of distributed, unmanned, and untethered wireless nodes to locally gather information in a timely manner. Some preliminary research has been conducted by Xie and Gibson (2000), Sozer et al. (2000), Proakis et al. (2001), Dunkels et al. (2004) and Kong et al. (2005a). This self-organising, self-reconfigurable network provides effective supports in sensing, monitoring, and reconnaissance.

The underwater sensor network paradigm is different from land-based sensor networks. The acoustic link features a long latency and a low bandwidth, while the sensor nodes are with low or medium group mobility due to water current. Therefore, extended research is required for security enforcement in this scalable environment to protect localised sensing and coordinated networking.

2.2 MDS and its applications in wireless networks

Multi-dimensional scaling was originally a technique developed in behavioural and social sciences for studying relationships among objects. The inputs to MDS are measures of the difference or similarity between object pairs (Davison, 1983). The output of MDS is a layout of the objects in a low-dimensional space. In this paper, the input is the distance matrix among the sensors. The mechanism can reconstruct the network topology and calculate a virtual position for every node. We adopt the classical metric MDS in the proposed mechanism since the distances are measured in a Euclidean space. More details of MDS can be found in Davison (1983) and Torgeson (1965).

MDS has been used to solve localisation and positioning problems in wireless networks. In Shang et al. (2003), a solution using classical metric MDS is proposed to achieve localisation from mere connectivity information. The algorithm is more robust to measurement errors and requires fewer anchor nodes than previous approaches. A distributed mechanism for sensor positioning using MDS has been presented by Ji and Zha (2004). It develops a multi-variate optimisation-based iterative algorithm to calculate the positions of sensors. Another approach (Biswas and Ye, 2004) for sensor network localisation adopts semidefinite programming relaxation to minimise errors for fitting the distance measurements. These mechanisms usually assume an attack-free scenario and focus on improving the positioning accuracy and routing efficiency.

2.3 Wormhole detection

Wormhole attacks on mobile ad hoc networks were independently discovered by Dahill et al. (2001), Papadimitratos and Haas (2002) and Hu et al. (2003a). Below we describe several approaches that have been developed to defend against such attacks in land-based wireless networks and analyse the difficulties in applying them to underwater environments.

The adoption of directional antennas (Ko et al., 2000; Choudhury et al., 2002) by wireless nodes can help detect wormhole attacks. In Hu and Evans (2004), the neighbour relation between a pair of nodes will be verified based on the directions of the received signals from each other and a shared third node. Only when the directions of both pairs are verified, is the neighbour relation confirmed.

One approach that does not depend on synchronised clocks to detect wormholes is proposed by Capkun et al. (2003). Every node is assumed to be equipped with a special hardware that can respond to a one-bit challenge without any delay. The challenger measures the round trip time of the signal to estimate the distance between the nodes. The probability that an attacker can guess all bits correctly decreases exponentially as the number of challenges increases.

Packet leash is proposed by Hu et al. (2003a) for wormhole prevention. A leash is information added to a packet to restrict its transmission distance. Geographic leashes use location information and loosely synchronised clocks together to verify a neighbour relation. In temporal leashes, the packet transmission distance is calculated based on the propagation delay and signal transmission speed.

MDS-VoW (Wang and Bhargava, 2004) is a centralised mechanism for wormhole detection in sensor networks that does not depend on any special hardware. After reconstructing the layout of sensors using multi-dimensional scaling, MDS-VoW detects wormholes by visualising the anomalies introduced by the attacks, which bend the reconstructed surface to fit the fake neighbour connections. Through detecting the bending feature, wormholes are located and fake neighbour connections are identified.

A wormhole prevention mechanism based on graph theory is proposed by Poovendran and Lazos (2007). Using the geometric random graphs induced by the communication range constraint of the nodes, the researchers present the necessary and sufficient conditions for detecting and defending against wormholes. They also present a defense mechanism based on local broadcast keys. However, several special nodes called guards that are equipped with GPS are required in the approach, which is not easy to implement in underwater environments.

Although existing approaches to wormhole detection can effectively defend against such attacks in some network settings, they do not satisfy the special requirements of underwater environments. They either depend on some special hardware, which may increase the unit cost of sensors, or require a centralised controller, which cannot adapt to frequent topology changes caused by sensor movement. Therefore, a new approach must be developed to protect the networks.

2.4 Distance estimation between wireless nodes

Several mechanisms have been developed to estimate the distance between a pair of wireless nodes. Existing solutions include using received signal strength (Ladd et al., 2002); Time-of-Arrival and Time Difference of Arrival (Priyantha et al., 2000; Savvides et al., 2001; Capkun et al., 2003); and triangulation (Savarese et al., 2001b; Niculescu and Nath, 2003).

Since acoustic signals transfer relatively slowly in water, the sensors can use a not-so-accurate clock to measure the round-trip time of a packet to estimate the distance between two nodes. We assume that the clock drift does not exceed a maximum value ρ. If, in the real world, the length of a time duration is t, and C is the time measured by a sensor, we have: $1 - \rho \le (\mathrm{d}C/\mathrm{d}t) \le 1 + \rho$. The clocks embedded in wireless nodes can easily achieve a relative accuracy of $\rho = 10^{-6}$ (Römer, 2001). We have developed a single round protocol to estimate the upper bound and lower bound of the distance between two sensors, which will be discussed in detail in Section 3.3.

2.5 Key distribution in sensor networks

During the distance estimation procedures, both the challenges and the replies must be protected by secret keys to prevent a malicious node from impersonating remote peers. To avoid one compromised sensor leading to the collapse of the whole system, we do not use group communication keys. Therefore, either pairwise keys or pre-distributed secrets should be adopted. If pair-wise keys are used, the secrets can be determined before the sensors are deployed (Boyd and Mathuria, 1998). The disadvantages include the fast increase in the number of keys and the difficulty in updating them when new sensors are added. A random key pre-distribution approach for sensor networks is proposed by Eschenauer and Gligor (2002), which allows any pair of sensors to share a key with a certain probability. Various approaches have been proposed to improve the safety and key sharing probability. The methods include q–composite and multi-path key reinforcement (Perrig et al., 2003), cooperative protocol (Pietro et al., 2003), the usage of Blom's key predistribution scheme (Du et al., 2003), pseudo random function, and bivariate polynomials (Liu and Ning, 2003).

3 Visualisation of wormholes

3.1 Motivation

In this section, we introduce several attacks on underwater sensor networks and illustrate the reasons that wormhole attacks are especially attractive to adversaries.

Since the available bandwidth of an underwater acoustic channel is very narrow, jamming attacks seem to be a natural choice of the malicious nodes. However, such attacks will reveal the positions of the jammers and attract physical countermeasures. Researchers have also investigated using CDMA techniques to defend against such attacks (Freitag et al., 2001; Azou et al., 2002).

With the advances in low power cryptography (Kitsos et al., 2005), symmetric encryption algorithms can be executed by sensors or even RFID tags (Feldhofer et al., 2004). Therefore, we assume that the malicious nodes cannot recover the secret keys solely based on the eavesdropped ciphertext.

Wormhole attacks do not risk revealing the positions of attackers or assume the compromise of some wireless nodes. Since only eavesdropping and retransmission are required, the attacks can be conducted by low cost units while a severe impact on network connectivity and performance can be caused. At the same time, the adoption of a stronger encryption or authentication mechanism will

not solve the problem. These properties make wormhole attacks especially attractive to the malicious nodes in underwater sensor networks.

3.2 System assumptions

We adopt a unit sphere model to describe the connectivity among sensors. Two underwater sensors are considered to be neighbours when the distance between them is shorter than r, where r is defined as the communication range. We assume that the links among sensors are bidirectional and two neighbouring nodes can always send packets to each other. This assumption will hold when the power of the sensors has not been exhausted.

The computation complexity of MDS is $O(n^3)$, where n is the number of sensors in the reconstructed network. To determine whether or not a sensor will be overwhelmed by the computation operations of the proposed mechanism, we executed the MDS programon a PC with 400 MHz CPU and 256 M RAM. We use two bytes to represent the distance between two sensors, and it can provide an accuracy of 0.1 m in a 1 km^3 cube area. When the reconstructed network contains $n = 120$ sensors, the proposed mechanism needs 28.8 KByte to store the 120×120 distance matrix. It takes the machine shorter than 15 seconds to reconstruct the network. Moreover, if we adopt the key distribution methods discussed in Section 2.5, the integrity and safety of the distance measurement packets can be protected by symmetric encryption or one way functions. The computation overhead of these security primitives on real mobile devices has been studied by Hu et al. (2003a) and Kong et al. (2005b). Therefore, both the computation and storage overheads of localised network reconstruction are affordable to a mobile device such as an iPAQ PDA.

Since most acoustic systems operate at a frequency below 30 KHz, the available bandwidth of a channel is very limited. For example, the highest rate reported so far is around 1 Mb/s at the range of 60 m radius (Kaya and Yauchi, 1989). As surveyed by Kilfoyle and Baggeroer (2000), research systems and commercial systems have highly variable link capacities, but the attainable range × rate product can hardly exceed 40 km-Kb/s. Longrange acoustic signals that operate over several tens of kilometers may have a capacity of only several tens of bits per second, while a short-range system operating over several tens of meters may have tens of kilobits per second. In our simulation, we set the communication range at 150 m and the link rate at 200 Kb/s.

An important feature of underwater sensors is their moderate mobility. When the impacts of water current are considered, the sensors show a group movement pattern as well as the changes of relative distances. The speed of ocean currents has been studied in various projects (Coble et al., 1987; Gross, 1990). The reported values range from 0.02 m/s to 1.5 m/s. In our study, we set the sensor movement speed at 1–1.2 m/s (about 2 knots). These settings can be replaced with minor effort when a more accurate movement model of underwater sensors becomes available.

3.3 Building blocks of Dis-VoW

3.3.1 Distance estimation between neighbouring sensors

After deployment, every sensor needs to measure the distances to its neighbours so that the values can be used in localised reconstruction. Since the propagation speed of acoustic signals in water is relatively slow, the clock drift has a very limited impact on the measurement accuracy. Therefore, we adopt a Time-of-Arrival approach to accomplish this task. We assume that two neighbouring sensors know each other's identity and a shared secret has been determined using the methods in Section 2.5. To reduce the impacts of node movements on the measurement accuracy, we propose a one-round protocol to determine the upper and lower bounds of the distance between two sensors.

A *Prover*, P, and a *Verifier*, V, try to measure the distance between them and they share a secret key K_{PV}. We assume that the real distance between them is d_{PV} the measured value is $\overline{d_{PV}}$, the signal propagation speed is v, the channel bandwidth is w, and symmetric encryption is adopted. The protocol executes as follows:

- V chooses a random nonce, x, and uses the encryption function e to calculate the L'-bit challenge that contains $e_{K_{PV}}(x)$. V sends the challenge to P and starts its clock at local time t_0 when the first bit of the challenge is transferred.
- P applies K_{PV} to decrypt the challenge and recover x. Then P uses a hash function h to calculate the L-bit reply that contains $h(x)$ and sends it back to V.
- V stops the local clock at t_1 when the last bit of the reply is received. It returns $T = t_1 - t_0$.

Using the hash result in the reply prevents an attacker from getting both the plain text and ciphertext of x. If V sends out the challenge at t_0, the *Prover* P will receive the challenge at $t_0 + (d_{PV}/v) + (L'/w)$. If the sum of the calculation time and cross layer processing delay in P is T_{cal} before the reply is sent back, V will get the reply at $t_0 + (2d_{PV}/v) + (L' + L/w) + T_{\text{cal}}$. T_{cal} will impact both the upper bound and lower bound of the distance estimation results.

T_{cal} is impacted by various factors such as the CPU speed of the sensor and the number of tasks to be processed before the current task. If the shortest processing time $T_{\min}$ and the longest latency $T_{\max}$ can be predetermined, we will have:

$$\frac{(T-(L+L')/w-T_{\max})\cdot v}{2} \le d_{PV} \le \frac{(T-(L+L')/w-T_{\min})\cdot v}{2}. \quad (1)$$

The computation time in P is easy to estimate. We assume that the sensors adopt an 8-round RC5 (Rivest, 1994; Baldwin and Rivest, 1996) encryption method, whose security analysis can be found in Kaliski and Yin (1995). RC5 has been combined with TinyOS (Levis et al., 2004) in several projects (Subramonian et al., 2003; Karlof et al., 2004). The experiments show that an iPAQ 3670 PDA can decrypt a 128-bit data block within 8 μs. The computation efficiency of hash functions on a similar device has been studied by Hu et al. (2003a), which shows that 220 K times hash calculation can be accomplished in one second. Therefore, the total computation time in P is shorter than 20 μs.

The cross layer processing delay depends on the workload of the sensor and is more difficult to estimate. To restrict the impacts of T_{cal} on the distance estimation accuracy, we adopt an alternative approach. Every *Prover P* will start a local timer when it receives the last bit of challenge. If the challenge has stayed in P for a time duration longer than T_{hold} and the reply has not been sent back yet, P will discard the reply and cancel the distance estimation. The *Verifier V* will re-initiate the procedure later. In this way we can choose a suitable value of T_{hold} so that the error of d_{PV} can be predetermined and both the upper and lower bounds of the distance can be derived. In our simulation, we set T_{hold} to 2 ms so that the error of the measured distance is shorter than 3 m.

Although the proposed mechanism can accurately estimate the distance between two sensors that are real neighbours, the malicious nodes can manipulate the delay of the packets in a wormhole to introduce errors into the measurement results. To investigate the impacts of these errors on the detection accuracy of Dis-VoW, we have conducted extended simulation under various distance estimation error rates and the results will be presented in Section 4.

3.3.2 Localised reconstruction

After measuring the distances to its neighbours, a sensor will broadcast these values in a packet. The packet will contain four parts: the sender's identity, the neighbours' identities, the distances, and the keyed hash values to protect the integrity of the information. For example, a sensor, s, will broadcast $(s,(s_1,\overline{d_{ss_1}}),\ldots,(s_q,\overline{d_{ss_q}}),$ $h_{K_{ss_1}}(s,(s_1,\overline{d_{ss_1}}),\ldots,(s_q,\overline{d_{ss_q}})),\ldots,h_{K_{ss_q}}(s,(s_1,\overline{d_{ss_1}}),\ldots,(s_q,\overline{d_{ss_q}})))$, where s_1 to s_q are the neighbours.

After receiving the distance reports from its neighbours, a sensor will be aware of the network topology within two hops and it can reconstruct the local network using MDS. For those connections whose measurements from both ends are available, s will calculate the average values and put the results at suitable positions in the distance matrix. If the measured distance is longer than the communication range, this neighbour relation will be aborted to avoid wormholes. The distance from a sensor to itself is 0. After the distances between the sensor pairs that can hear each other are calculated, a classical shortest-path algorithm, such as Dijkstra's algorithm, can be used to calculate the shortest distance between every sensor pair. When all positions in the distance matrix have been filled, MDS can be used to rebuild the network, and a virtual position for every sensor will be generated. The examples of localised reconstruction under two different scenarios (attack-free and under attack) are illustrated in Figure 2(d) and (e).

3.3.3 Detection of wormhole

In this section, we first explain the distortions in the reconstructed networks that are caused by wormhole attacks. Experimental results are then presented to illustrate how the distortions can be used to locate the wormholes and identify the fake neighbour connections.

3.3.3.1 Impacts of wormholes

If we have n sensors in the network, we can generate an $n \times n$ distance matrix, D, as shown in Figure 3, in which every item d_{j-k} represents the distance between sensor j and k. If we choose sensor i as the origin of a space, we can build a $(n-1)\times(n-1)$ matrix, B_i, in which every item b_{jik} is determined as:

$$b_{ijk} = \frac{1}{2}(d_{i-j}^2 + d_{i-k}^2 - d_{j-k}^2) \quad (j,k \neq i). \tag{2}$$

Figure 3 Generate B_i from the distance matrix D

$$\begin{bmatrix} 0 & d_{1-2} & d_{1-3} & \cdots & d_{1-n} \\ d_{2-1} & 0 & d_{2-3} & \cdots & d_{2-n} \\ d_{3-1} & d_{3-2} & 0 & \cdots & d_{3-n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ d_{n-1} & d_{n-2} & d_{n-3} & \cdots & 0 \end{bmatrix} \rightarrow \begin{bmatrix} b_{1i1} & b_{1i2} & \cdots & b_{1in} \\ b_{2i1} & b_{2i2} & \cdots & b_{2in} \\ \cdots & \cdots & \cdots & \cdots \\ b_{ni1} & b_{ni2} & \cdots & b_{nin} \end{bmatrix}$$

This value can be viewed as the scalar product of the vectors $\vec{ij}$ and $\vec{ik}$. For the three sensors i, j, and k, we can apply the cosine law and get the following result.

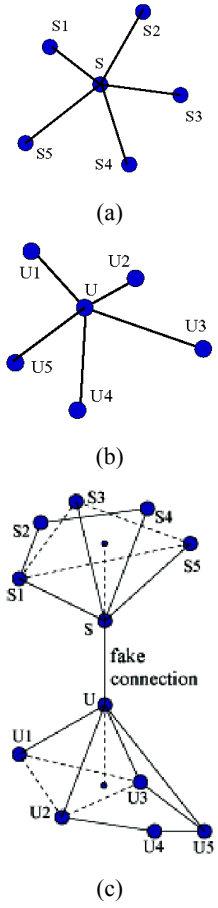
$$b_{ijk} = d_{i-j} d_{i-k} \cos\theta_{ijk}. \tag{3}$$

Young and Householder (1938) have shown that this matrix B_i can be factored as $B_i = X_i, X_i^T$, in which X_i is the coordinate matrix of the sensors in the space with node i as the origin. The MDS algorithm can be viewed as a procedure to calculate X_i. Therefore, any changes in the distance matrix will impact the final reconstruction result. Although the original approach by Young and Householder assumes that the distances are accurate, an error matrix can be added to achieve the least squares bias when the distances are fallible.

With this analysis, a simple example can be used to illustrate the impacts of a wormhole on localised network reconstruction. We have two groups of sensors: sensor s and its real neighbours s_1 to s_5, and sensor u and its real neighbours u_1 to u_5. Each group can be fitted into a 2D

space. The two groups of sensors are far away from each other in the real network and their layouts are shown in Figure 4(a) and (b). Now we assume that a wormhole attack is conducted and a fake neighbour connection has been established between s and u. We choose sensor s as the origin of the space and generate matrix B_s to illustrate the impacts of the wormhole.

Figure 4 Distortions in localised reconstruction: (a) sensor S and its neighbours; (b) sensor U and its neighbours and (c) localised reconstruction



Let us consider the triangle formed by sensors s, u, and s_1. Since su is the only fake neighbour connection generated by the wormhole, we can use the Dijkstra's method to calculate $d_{s_1u} = d_{su} + d_{ss_1}$. Based on equation (3), the angle θ_{s_1su} should be equal to π, which means that the wormhole will move node s_1 to the extension line of us. Similar conditions will happen to the other neighbours s_2 to s_5, and u_1 to u_5. Since the real neighbour connections among these sensors will try to preserve the original layout during reconstruction, the final reconstruction result will be the joint impact of these two factors, as shown in Figure 4(c).

From this example, we find that a wormhole can be viewed as an extra force that will push the sensors away from their original positions, thus leading to the following distortions. The distances and angles among the neighbouring sensors in the reconstructed network will be very different from the values in the real layout. A good estimation of the distances and angles in the real layout can be acquired from the measurements in Section 3.3.1. Below we present experimental results to show these distortions.

3.3.3.2 Distortions in edge length

We adopt a grid placement of sensors as shown in Figure 2(a). Four different scenarios of localised network reconstruction are examined:

- no wormhole exists within two hops
- one wormhole exists
- two independent wormholes exist
- multiple fake neighbour connections through the same wormhole exist.

The distortions in edge lengths can be measured by the average differences between the measured distances among neighbouring sensors and the lengths of the reconstructed connections. We consider node i and all sensors within two hops to it, which can be represented by the set N_i. If the measured distance between two neighbouring sensors j and k is $\overline{d_{jk}}$, and the length of the reconstructed connection is d'_{jk}, the average difference can be calculated as:

$$\overline{diff_i} = \frac{\sum \left\| \overline{d_{jk}} - d'_{jk} \right\|}{m}, \tag{4}$$

where $\{j, k \in N_i,\ j \neq k\}$, and m is the total number of neighbour relations in the reconstructed network. The ratios between $\overline{diff_i}$ and the communication range, r, under different scenarios are shown in Table 1. We find that when no wormhole exists in the localised network, the reconstruction result will preserve the distances among sensors very well. On the contrary, as soon as the fake neighbour connections are included, the average difference will have a sharp increase. We can use this increase to detect the existence of a wormhole in the reconstructed network.

Table 1 Distortions in edge lengths in reconstructed networks

Scenarios	$\overline{diff_i}/r$ (%)
No wormhole	5.3
One wormhole	24.7
Two wormholes	24.3
One wormhole multiple connections	25.6

3.3.3.3 Distortions in angles

The distortions in angles can be used to locate the fake neighbour connections. In the example shown in Figure 4(c), the real neighbours of node s will be moved from their original positions, which will lead to the changes of the angles among these sensors. For every such an angle, two values can be determined:

- θ_M, which can be calculated based on the measured distances from Section 3.3.1
- θ_R, which can be acquired from the reconstructed network.

The distortions in angles can be measured by the differences between these two groups of values.

We define a new variable *wormhole indicator* (*wi*) for every sensor *i* based on the differences in angles:

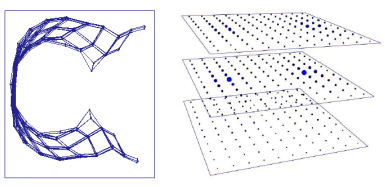
$$\text{wormhole indicator}(i) = \frac{\sum \theta_{diff-ijk}}{q(q-1)};$$
$$\theta_{diff-ijk} = \begin{cases} 0, & \text{if } \theta_{M-ijk} - \theta_{R-ijk} \le \theta_{th}; \\ 1, & \text{if } \theta_{M-ijk} - \theta_{R-ijk} > \theta_{th}. \end{cases} \quad (5)$$

where *i*, *j* and *k* are neighbours, and *q* is the degree of connectivity of sensor *i*. From the definition we find that wormhole indicator is a normalised variable with the value range [0, 1]. Every sensor will calculate the *wi* value of itself and exchange it with the neighbours to locate the fake neighbour connections.

θ_{th} in equation (5) represents the threshold that is used to distinguish the changes in angles caused by distance measurement inaccuracy from the distortions caused by wormhole attacks. In our simulation, θ_{th} has a format of $c \cdot (vT_{\text{hold}}/0.5r)$, in which vT_{hold} represents the distance measurement inaccuracy, r is the communication range, and c is a constant. When T_{hold} is not very long, $vT_{\text{hold}}/0.5r$ roughly describes the change in angles caused by the distance measurement inaccuracy. In our simulation, we set $c = 4$.

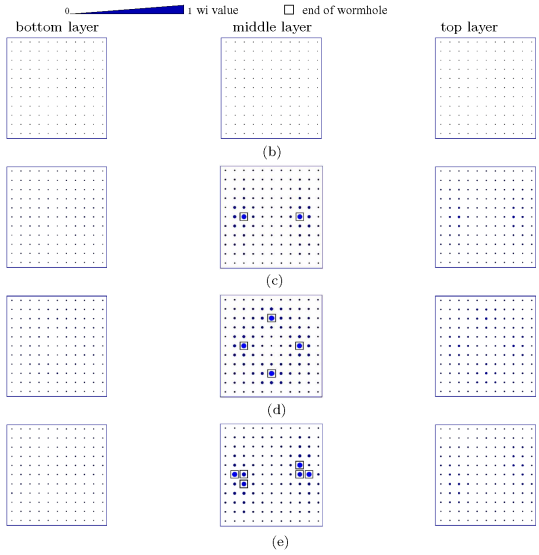
We have conducted extended simulation and the wormhole indicator values under different scenarios are illustrated in Figure 5. We show the *wi* values of the sensors in different layers separately. From the figures, we find that the ends of wormholes have the largest distortions in angles and they can be easily identified. In the following experiments, a neighbour connection will be labelled as a wormhole if both ends of the link have a *wi* value larger than 0.3.

Figure 5 Wormhole indicator values under different scenarios. The radius of a sensor is proportional to its wormhole indicator value. The ends of wormholes can be easily identified: (a) global reconstruction result and the view of wormhole indicator values in a 3D space when one wormhole exists; (b) wormhole indicator values when no wormhole exists; (c) wormhole indicator values when one wormhole exists; (d) wormhole indicator values when two wormholes exist and (e) wormhole indicator values when nine fake neighbour connections are established through the same wormhole



(a)

Figure 5 Wormhole indicator values under different scenarios. The radius of a sensor is proportional to its wormhole indicator value. The ends of wormholes can be easily identified: (a) global reconstruction result and the view of wormhole indicator values in a 3D space when one wormhole exists; (b) wormhole indicator values when no wormhole exists; (c) wormhole indicator values when one wormhole exists; (d) wormhole indicator values when two wormholes exist and (e) wormhole indicator values when nine fake neighbour connections are established through the same wormhole (continued)



3.4 *The Dis-VoW algorithm*

With the readiness of all building blocks, we now walk through the steps of the Dis-VoW algorithm.

- After deployment, every sensor will estimate the distances to the nodes that it can hear using the protocol described in Section 3.3.1.
- Every sensor will broadcast the neighbour list and the distances so that its neighbours will be aware of the topology within two hops. The Dijkstra's method is used to calculate the shortest distance between every sensor pair and generate the distance matrix.
- Using classical metric MDS, every sensor will reconstruct the network within two hops and calculate a virtual position for every node in it.
- Every sensor will calculate its wormhole indicator value.

It will locate the wormholes as described in Section 3.3.3, and the detected fake neighbour connections will be avoided during routing discovery and packet forwarding.

4 Experimental study

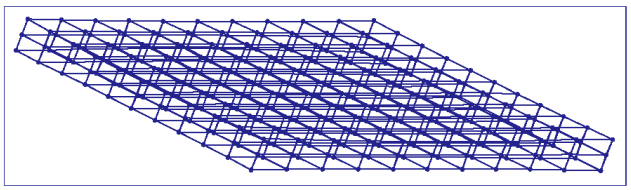
The detection accuracy of Dis-VoWis studied through simulation using *ns*2. We assume that sound travels in water at the speed of 1500 m/s, and we ignore the variations in velocity caused by the changes in temperature, pressure, and salinity of water. We assume that the communication range

of the sensors is 150 m, and any two sensors having a distance shorter than this can directly communicate with each other. Based on these assumptions, the maximum propagation delay between two neighbouring nodes is 100 ms. We also assume that the bandwidth of the acoustic channel is 200 Kb/s. At the MAC layer, we adopt a variation of the protocol proposed by Rodoplu and Park (2005) to reduce collisions among neighbours.

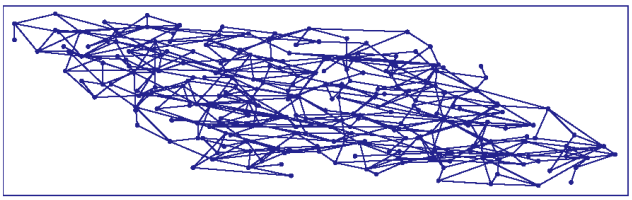
Since Dis-VoW is a distributed approach, every sensor will reconstruct the network topology within two hops and conduct localised wormhole detection. The sensors are deployed in a three-dimensional space with the size of $700 \times 700 \times 140$ m. We use this layout to simulate a scenario in which the sensors are deployed in a water area with a certain depth range.

Two deployments of sensors are examined: grid placement placement and random placement. In the grid placement, the sensors are deployed in three layers at different depths and the distance between two neighbouring layers is 70 m. In each layer, 11×11 sensors are placed at an interval of 70 m along imaginary vertical or horizontal lines. A total number of 363 sensors are used and the average degree of connectivity is 18.4. In a random placement, we apply the dart throwing method proposed by Mitsa and Parker (1991) to place the sensors randomly and roughly uniformly in the 3D space. A total number of 256 sensors are deployed, and a similar degree of connectivity is maintained. Two examples of the placements are shown in Figure 6(a) and (b).

Figure 6 Examples of network topology used for simulation. Only a part of neighbour connections are illustrated as lines in the figures: (a) an example layout of grid placement: a 11 × 11 × 3 grid and (b) an example layout of random placement



(a)



(b)

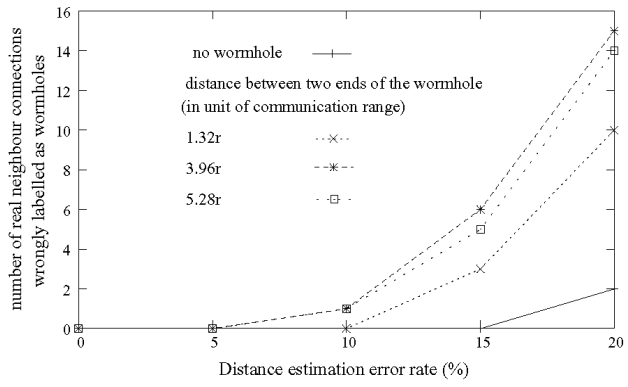
Since the sensors communicate with each other through shared acoustic channel, the distances to different neighbours of a node cannot be measured at the same moment. The differences in measurement time and the relative motion among sensors will introduce an inaccuracy into network reconstruction. To investigate the impacts of this inaccuracy on the detection capability of Dis-VoW, we apply an error to the measured distances. If the real distance between two sensors is $d (d \le r)$ and the error rate is e_m, a random value drawn from the uniform distribution $[d \times (1 - e_m),\ d \times (1 + e_m)]$ will be used as the measured value. Since the relative moving speed among sensors is slow, we examine different values of e_m from 0 to 0.2. Every data point in the following figures represents the average value over ten trials using different error files.

4.1 Grid placement

In grid placement of sensors, two groups of experiments are conducted to examine the detection accuracy of the proposed mechanism. In the first group, only one wormhole exists in the network. We strategically select three pairs of sensors on the diagonal of the middle layer in the grid as the potential victims of the wormhole so that more routes will be impacted by the fake neighbour connection. The real distances between the three pairs of sensors are 1.32, 3.96, and 5.28 times the communication range. Different values of e_m from 0 to 0.2 are examined. The detection accuracy and the number of real neighbour connections that are wrongly labelled as wormholes are of special interest.

The simulation shows that Dis-VoW successfully identifies all fake neighbour connections when there is only one wormhole in the network and the distance error rate e_m is not larger than 0.2. Figure 7 shows the number of real neighbour connections that are wrongly labelled as wormholes. Compared to the results in Wang and Bhargava (2004), Dis-VoW has an improved detection accuracy. The main reason is that the new method is a distributed approach. Therefore, if the wormhole is not within two hops to a sensor, its localised reconstruction will not be affected and no false alarm will be introduced.

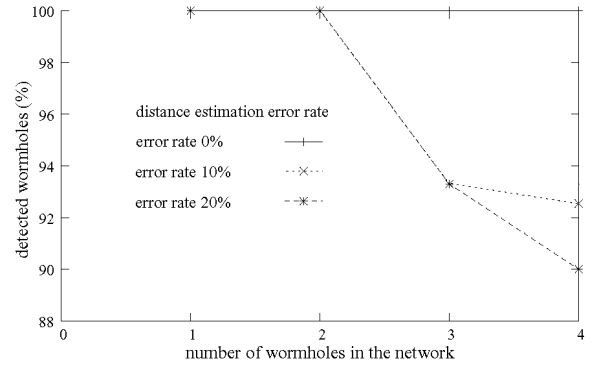
Figure 7 Detection accuracy of Dis-VoW under different error rates e_m



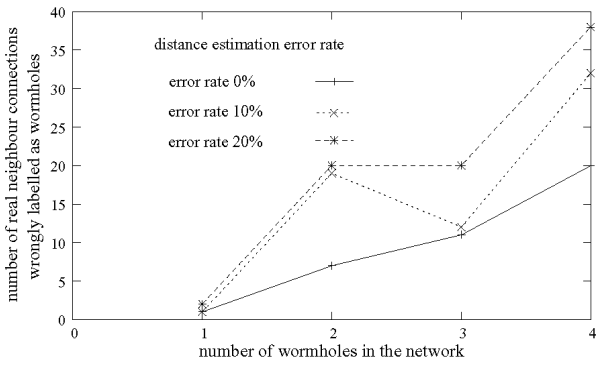
In the second group of experiments, we examine the detection accuracy of Dis-VoW when the number of wormholes in the network increases. The victims of the attacks are randomly and independently selected from the sensors as long as the distance between the two ends of a wormhole is longer than the communication range. The results are illustrated in Figure 8. Compared to the

values in Figure 7, the detection accuracy of Dis-VoW will decrease when the number of wormholes increases. The main reason leading to the decrease is as follows: although the victims of attacks are randomly and independently selected, as the number of wormholes increases, the probability will also increase that they are close to each other and multiple wormholes will impact the same localised network reconstruction jointly. Coexistence of multiple wormholes in a small area will lead to more complex distortions. Multiple rounds of detection may be required to deal with such conditions and more details will be discussed in Section 5.

Figure 8 Detection accuracy of Dis-VoW with different numbers of wormholes: (a) detection accuracy vs. the number of wormholes and (b) number of real neighbour connections wrongly labelled as wormholes vs. the number of wormholes



(a)

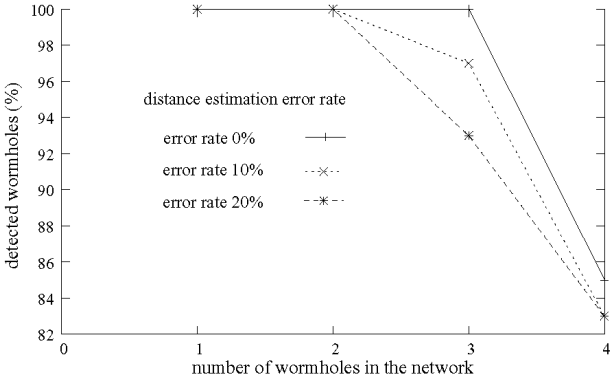


(b)

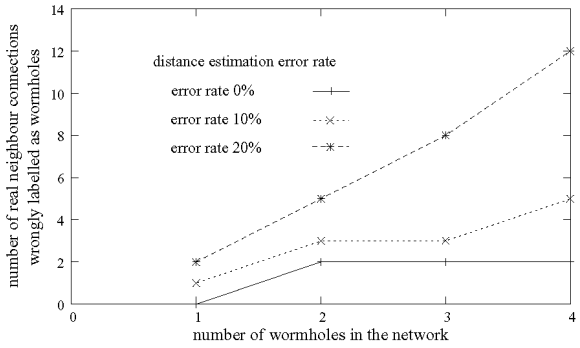
4.2 Random placement

An example of random placement of sensors is illustrated in Figure 6(b). To maintain a similar degree of connectivity as in the grid placement, we apply the dart throwing method (Mitsa and Parker, 1991) to deploy the nodes and we require that the distance between any pair of sensors will not be shorter than 60 m. In the illustrated example, a total number of 256 sensors are placed and the average degree of connectivity is 18.3. The simulation results of the grid placement show that Dis-VoW can detect most of the fake neighbour connections when there is only one wormhole in the network. Therefore, we focus on the scenarios in which multiple wormholes exist in this group of experiments. The victims are randomly and independently selected from the sensors. Results are shown in Figure 9. We find that the curves in Figure 9 are very similar to those in Figure 8. The results show that the deployment of sensors does not impact the detection accuracy of Dis-VoW to a large extent because of its localised property.

Figure 9 Detection accuracy of Dis-VoWin random placement of sensors: (a) detection accuracy vs. the number of wormholes and (b) number of real neighbour connections wrongly labelled as wormholes vs. the number of wormholes



(a)



(b)

Comparing the results illustrated in Figures 7–9 for different sensor deployments, we find that Dis-VoWcan identify most of the fake neighbour connections when there is only one wormhole in the network. The proposed mechanism is robust against distance estimation errors. When there are multiple wormholes in the network, the approach can still provide a decent detection accuracy without introducing many false positive alarms.

5 Discussions

The proposed mechanism does not require the sensors to be equipped with any special hardware. It detects wormholes by visualising the distortions in the reconstructed networks that are caused by the attacks. The localised network reconstruction and wormhole detection procedures reduce the computation and storage overhead so that Dis-VoW can be executed by sensors with a relatively weak processing capability.

5.1 Differences between MDS-VoW and Dis-VoW

Although both MDS-VoW and Dis-VoW use multidimensional scaling to reconstruct the network topology, they have the following differences. First, MDS-VoW is a centralised mechanism and Dis-VoW is a distributed approach. Therefore, only Dis-VoW can be executed by sensors with a relatively weak processing capability. Dis-VoW also provides improved scalability to the size of the network and better adaptability to frequent topology changes. Second, MDS-VoW assumes that the sensors are deployed in a two-dimensional space and only Dis-VoW can be applied to 3D network environments. Third, MDS-VoW detects wormholes based on the distortions in global network topology and Dis-VoW uses localised information. Finally, Dis-VoW demonstrates much better detection accuracy than MDS-VoWwhen there are multiple wormholes in the network.

5.2 Security of Dis-VoW

Dis-VoW is a security enhancement to sensor networks to defend against wormhole attacks. Therefore, its robustness must be carefully studied to avoid introducing new vulnerabilities. During the execution of Dis-VoW, a sensor will interact with its neighbours under three conditions:

- distance estimation
- exchange of distance estimation results
- exchange of localised wormhole detection results.

Below we discuss possible attacks during these interactions and their countermeasures. Since every pair of neighbouring sensors can establish a secret key using the mechanisms described in Section 2.5, the packets between them can be protected by symmetric encryption or keyed hash functions and the malicious nodes cannot change the contents. The malicious nodes can selectively discard the packets going through a wormhole. In Dis-VoW, we require that any sensor failing to accomplish the distance estimation procedure or the exchange of distance estimation results will not be considered as a real neighbour. In this way, the malicious nodes cannot hide a fake neighbour connection by discarding these packets. To prevent the malicious nodes from disabling the propagation of the localised wormhole detection results, we require every sensor to attach the previous round detection results to its replies to the distance estimation challenges. Since the replies will contain a nonce generated by the challenger, the freshness of the information is guaranteed and resend attacks cannot be conducted.

A clever attacker can manipulate the buffering time of the distance estimation packets in a systematic manner to generate a fake network topology that does not conflict with the real sensor layout. Defending against such attacks is beyond the scope of this paper and will be investigated in future work.

5.3 Control of false positive alarms

During wormhole detection procedures, if some real neighbour connections are wrongly labelled as wormholes, false positive alarms will be caused. The breaks of these connections will lead to an increase in the average path length and end-to-end delay among sensors. In the worst case, if all connections of a sensor are broken because of false positive alarms, an isolated node will be generated and the events detected by this sensor cannot be reported. Therefore, false alarms must be controlled.

An extra step can be adopted by Dis-VoW to reduce false positive alarms. With all the detected fake neighbour connections (could include some false alarms) excluded, a second round of localised reconstruction can be conducted. The rebuilt network would be very similar to the real layout of sensors and we can determine whether a 'detected wormhole' is a false alarm by examining the distance between the sensor pair. This method will add the excluded connections back to the network one-by-one so that the real wormholes leading to the distortions can be located. This method will double the computation overhead at a sensor to improve the detection accuracy of Dis-VoW. It is extremely helpful in the environments when the average degree of connectivity is not large.

5.4 Frequency to conduct wormhole detection

Relative motion among sensors will lead to network topology changes and allow wormholes to be formed dynamically. Therefore, wormhole detections must be conducted repeatedly during the network lifetime. The detection can be conducted in a proactive or a reactive manner. In the proactive approach, the sensors will choose an interval T_i and conduct wormhole detections every T_i seconds. This interval determines the longest time that a wormhole can exist before it is located. Compared to this scheme, the reactive method is more efficient. Since a wormhole can be formed only when a neighbour relation between two nodes changes, a sensor can estimate the time that the next change happens and initiate the detection reactively.

5.5 Future work

There are several immediate extensions to the proposed mechanism. In land-based sensor networks, if the nodes are not equipped with any special hardware, the measured distances among sensors may have a large error. For example, the distance that is estimated based on the received signal strength can have an error from 5% to 40% of the radio range (Savarese et al., 2001a). The network that is reconstructed based on these inaccurate values can be very different from the real sensor layout, and more false alarms will be introduced into the system. Therefore, a robust wormhole detection mechanism with improved tolerance to distance estimation errors is required for these

environments. The ultimate objective of the research is to design an approach that can detect and identify wormholes based solely on the connectivity information.

The simulation results in Section 4 show that the joint impacts of multiple wormholes may cause the detection accuracy of the proposed mechanism to deteriorate. For the wireless nodes with a more powerful processing capability, multiple rounds of localised detection can be conducted. The identified fake neighbour connections will be excluded during the next round of reconstruction and detection. The method described earlier in this section can be adopted to reduce false positive alarms.

6 Conclusions

As a distributed approach, Dis-VoW defends against wormhole attacks in underwater sensor networks without depending on any special hardware. Using the distances measured by the propagation delay of acoustic signals, every sensor reconstructs the local network topology using multi-dimensional scaling. Dis-VoW detects wormholes by visualising the distortions in edge lengths and angles among neighbouring sensors. A normalised variable wormhole indicator is defined based on these distortions to identify fake neighbour connections. Dis-VoW consists of multiple steps and each step can be improved independently.

The detection accuracy of the proposed mechanism is evaluated through simulation. The results show that Dis-VoW can detect most of the fake neighbour connections without introducing many false positive alarms, even when there are multiple wormholes in the network. Since Dis-VoW reconstructs networks and detects wormholes in a distributed manner, the scheme will introduce a limited amount of computation and storage overhead to the sensors. The security of Dis-VoW, the methods to reduce false positive alarms, and the frequency to conduct wormhole detections are discussed to provide a more comprehensive view of the proposed mechanism.

Extensions to Dis-VoW are under construction. We plan to apply the distributed detection mechanism to landbased sensor networks in 3D environments. We will investigate the joint impacts of multiple wormholes on localised network reconstruction. The research will lead to a more accurate, robust, and efficient solution to defend against wormhole attacks.

References

Akyildiz, I., Pompili, D. and Melodia, T. (2005) 'Underwater acoustic sensor networks: research challenges', *Elsevier's Journal of Ad Hoc Networks*, Vol. 3, No. 3, pp.257–279.

Azou, S., Pistre, C. and Burel, G. (2002) 'A chaotic direct sequence spread-spectrum system for underwater communication', *Proceedings of IEEE-Oceans*, Biloxi, Mississippi, pp.2409–2415.

Baldwin, R. and Rivest, R. (1996) 'The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS algorithms', *IETF RFC 2040*, URL: http://www.ietf.org/rfc/rfc2040.txt.

Biswas, P. and Ye, Y. (2004) 'Semidefinite programming for ad hoc wireless sensor network localization', *Proceedings of ACM/IEEE IPSN*, Berkeley, California, pp.46–54.

Boyd, C. and Mathuria, A. (1998) 'Key establishment protocols for secure mobile communications: a selective survey', *Lecture Notes in Computer Science*, Vol. 1438, pp.344–355.

Capkun, S., Buttyán, L. and Hubaux, J. (2003) 'SECTOR: secure tracking of node encounters in multi-hop wireless networks', *Proceedings of ACM Workshop on Security of Ad hoc and Sensor Networks*, Fairfax, Virginia, pp.21–32.

Choudhury, R., Yang, X., Ramanathan, R. and Vaidya, N. (2002) 'Using directional antennas for medium access control in ad hoc networks', *Proceedings of ACM MobiCom*, Atlanta, Georgia, pp.59–70.

Coble, C., Elaine, M. and Dale, R. (1987) *Earth Science*, Prentice-Hall, Englewood Cliffs, NJ.

Dahill, B., Levine, B., Royer, E. and Shields, C. (2001) *A Secure Routing Protocol for Ad Hoc Networks*, University of Massachusetts, Tech Report CS-02-32, Amherst, MA.

Davison, M. (1983) *Multidimensional Scaling*, John Wiley & Sons, New York.

Du, W., Deng, J., Han, Y. and Varshney, P. (2003) 'A pairwise key pre-distribution scheme for wireless sensor networks', *Proceedings of ACM CCS*, Washington DC, pp.42–51.

Dunkels, A., Feeney, L., Grönvall, B. and Voigt, T. (2004) 'An integrated approach to developing sensor network solutions', *Proceedings of the Second Internationa Workshop on Sensor and Actor Network Protocols and Applications*, Boston, Massachusetts.

Eschenauer, L. and Gligor, V. (2002) 'A key-management scheme for distributed sensor networks', *Proceedings of ACM CCS*, Washington DC, pp.41–47.

Feldhofer, M., Dominikus, S. and Wolkerstorfer, J. (2004) 'Strong authentication for RFID systems using the AES algorithm', *Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Cambridge, MA, pp.357–370.

Freitag, L., Stojanovic, M., Singh, S. and Johnson, M. (2001) 'Analysis of channel effects on direct sequence and frequency hopped spread spectrum acoustic communications', *IEEE Journal of Oceanic Engineering*, Vol. 26, No. 4, pp.586–593.

Gross, M. (1990) *Oceanography*, Merrill, Columbus.

Hu, L. and Evans, D. (2004) 'Using directional antennas to prevent wormhole attacks', *Proceedings of Network and Distributed System Security Symposium*, San Diego, CA.

Hu, Y., Perrig, A. and Johnson, D. (2003a) 'Packet leashes: a defense against wormhole attacks in wireless ad hoc networks', *Proceedings of IEEE INFOCOM*, San Francisco, CA, pp.1976−1986.

Hu, Y., Perrig, A. and Johnson, D. (2003b) 'Rushing attacks and defense in wireless ad hoc network routing protocols', *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, San Diego, CA, pp.30–40.

Ji, X. and Zha, H. (2004) 'Sensor positioning in wireless ad-hoc sensor networks with multidimensional scaling', *Proceedings of IEEE INFOCOM*, Hong Kong, pp.2652–2661.

Kaliski, B. and Yin, Y. (1995) 'On differential and linear cryptanalysis of the RC5 encryption algorithm', *Lecture Notes in Computer Science, Proceedings of CRYPTO'95*, pp.171–184.

Karlof, C., Sastry, N. and Wagner, D. (2004) 'TinySec: a link layer security architecture for wireless sensor networks', *Proceedings of ACM Conference on Embedded Networked Sensor Systems*, Baltimore, pp.162–175, MA.

Kaya, A. and Yauchi, S. (1989) 'An acoustic communication system for subsea robot', *Oceans*, pp.765–770.

Kilfoyle, D. and Baggeroer, A. (2000) 'The state of the art in underwater acoustic telemetry', *IEEE Journal of Oceanic Engineering*, Vol. OE-25, No. 1, January, pp.4–27.

Kitsos, P., Koufopavlou, O., Selimis, G. and Sklavos, N. (2005) 'Low power cryptography', *Second Conference on Microelectronics, Microsystems and Nanotechnology*, pp.343–347.

Ko, Y., Shankarkumar, V. and Vaidya, N. (2000) 'Medium access control protocols using directional antennas in ad hoc networks', *Proceedings of IEEE INFOCOM*, pp.13–21.

Kong, J., Cui, J., Wu, D. and Gerla, M. (2005a) 'Building underwater ad-hoc networks and sensor networks for large scale real-time aquatic applications', *Proceedings of IEEE MILCOM*¸. Atlantic City, NJ.

Kong, J., Ji, Z., Wang, W., Gerla, M., Bagrodia, R. and Bhargava, B. (2005b) 'Low-cost attacks against packet delivery, localization and time synchronization services in under-water sensor networks', *Proceedings of ACM Wireless Security (WiSe'05)*, pp.87–96; An extended version is Technical Report CSD-TR040051, *UCLA Computer Science Department*, December 2004.

Ladd, A., Bekris, K., Rudys, A., Marceau, G., Kavraki, L. and Wallach, D. (2002) 'Robotics-based location sensing using wireless ethernet', *Proceedings of ACM MobiCom*, Atlanta, Georgia, pp 227–238.

Levis, P., Madden, S., Gay, D., Polastre, J., Szewczyk, R., Woo, A., Brewer, E. and Culler, D. (2004) 'The emergence of networking abstractions and techniques in TinyOS', *Proceedings of the Symposium on Networked Systems Design and Implementation*¸. San Fransisco, CA, pp.1–14.

Liu, D. and Ning, P. (2003) 'Location-based pairwise key establishments for static sensor networks', *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp.72–82.

Mitsa, T. and Parker, K. (1991) 'Digital halftoning using a blue-noise mask', *Proceedings of the International Conference on Acoustics, Speech, and Signal Processing,* pp.47–56.

Niculescu, D. and Nath, B. (2003) 'Ad hoc positioning system (APS) using AoA', *Proceedings of IEEE INFOCOM*, San Francisco, CA, pp.1734–1743.

Papadimitratos, P. and Haas, Z. (2002) 'Secure routing for mobile ad hoc networks', *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, San Antonio, TX.

Perrig, A., Chan, H. and Song, D (2003) 'Random key predistribution schemes for sensor networks', *Proceedings of Symposium on Security and Privacy*, Oakland, CA, pp.197–213.

Pietro, R., Mancini, L. and Mei, A. (2003) 'Random keyassignment for secure wireless sensor networks', *Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp.62–71.

Poovendran, R. and Lazos, L. (2007) 'A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks', *ACM Journal on Wireless Networks (WINET)*, Vol. 13, No. 1, pp.27–59.

Priyantha, N., Chakraborty, A. and Padmanabhan, H. (2000) 'The cricket location support system', *Proceeding of ACM MobiCom*, pp.32–43.

Proakis, J., Sozer, E., Rice, J. and Stojanovic, M. (2001) 'Shallow water acoustic networks', *IEEE Communications Magazine*, November, pp.114–119.

Rivest, R. (1994) 'The RC5 encryption algorithm', *Proceedings of International Workshop on Fast Software Encryption*, pp.86–96.

Rodoplu, V. and Park, M. (2005) 'An energy-efficient MAC protocol for underwater wireless acoustic networks', *Proceedings of MTS/IEEE OCEANS*¸ pp.1198–1203.

Römer, K. (2001) 'Time synchronization in ad hoc networks', *Proceedings of the ACM MobiHoc*, Long Beach, CA, pp.173–182.

Savarese, C., Langendoen, K. and Rabaey, J. (2001a) 'Robust positioning algorithms for distributed ad-hoc wireless sensor networks', *Proceedings of USENIX Technical Annual Conference*, pp.317–328.

Savarese, C., Rabaey, J. and Beutel, J. (2001b) 'Locationing in distributed ad-hoc wireless sensor networks', *Proceedings of ICASSP*, pp.2037–2040.

Savvides, A., Han, C. and Srivastava, M. (2001) 'Dynamic fine-grained localization in ad-hoc networks of sensors', *Proceedings of ACM MobiCom*, Rome, Italy, pp.166–179.

Shang, Y., Ruml, W., Zhang, Y. and Fromherz, M. (2003) 'Localization from mere connectivity', *Proceedings of ACM MobiHoc*, Annapolis, Maryland, pp.201–212.

Sozer, E., Stojanovic, M. and Proakis, J. (2000) 'Undersea acoustic networks', *IEEE Journal of Oceanic Engineering*, Vol. OE-25, No. 1, January, pp.72–83.

Subramonian, V., Huang, H. and Datar, S. (2003) *Priority Scheduling in TinyOS: A Case Study*, Tech Report CSE-TR-74, Washington University, St. Louis, MO.

Torgeson, W. (1965) 'Multidimensional scaling of similarity', *Psychometrika*, Vol. 30, pp.379–393.

Wang, W. and Bhargava, B. (2004) 'Visualization of wormhole attacks in sensor networks', *Proceedings of ACM Workshop on Wireless Security (WiSe)*, Philadelphia, PA, pp.51–60.

Xie, G. and Gibson, J. (2000) *A Networking Protocol for Underwater Acoustic Networks*, Technical Report TRCS-00-02, Department of Computer Science, Naval Postgraduate School, Monterey, CA.

Young, G. and Householder, A. (1938) 'Discussion of a set of points in terms of their mutual distances', *Psychometrika*, Vol. 3, pp.19–22.