electronics

MDPI

Article

HydraulicBridge: Covert Signaling Channel between Air-Gapped Systems Using Hydraulic-Pressure Fluctuations

Yongyu Liang [1,2], Hong Shan [1,2], Jun Zhao [1,2], Canju Lu [1,2] and Guozheng Yang [1,2,*]

[1] College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China; liangyongyu@nudt.edu.cn (Y.L.); shanhong@nudt.edu.cn (H.S.); zhaojun17@nudt.edu.cn (J.Z.); lucanju17@nudt.edu.cn (C.L.)

[2] Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China

* Correspondence: yangguozheng17@nudt.edu.cn

Abstract: To protect critical computing systems from network attacks, modern enterprises typically employ physical isolation measures to disconnect them from open networks such as the Internet. However, attackers can still infiltrate these closed networks through internal employees or supply chain vulnerabilities. This presents the primary challenge that attackers face: how to effectively manage and manipulate infected devices that are isolated from the external network. In this paper, we propose a new covert communication technology called HydraulicBridge, which demonstrates how air gap networks can communicate through covert water pressure-fluctuation channels. Specifically, we demonstrate how water pressure from water pipes can be used to communicate with infected hosts within an air gap network. Additionally, we provide experimental results demonstrating the feasibility of covert channels and test the communication speed in the experimental environment. Finally, we offer a forensic analysis and propose various methods for detecting and blocking this channel. We believe that this study provides a comprehensive introduction to previously unseen attack vectors that security experts should be aware of.

Keywords: air-gapped networks; covert channels; exfiltration; infiltration; hydraulic communication

Citation: Liang, Y.; Shan, H.; Zhao, J.; Lu, C.; Yang, G. HydraulicBridge: Covert Signaling Channel between Air-Gapped Systems Using Hydraulic-Pressure Fluctuations. *Electronics* **2024**, *13*, 3010. https://doi.org/10.3390/electronics13153010

Academic Editors: Zhipeng Cai, Sai Akshita Maradapu Vera Venkata, Zuobin Xiong and Tuo Shi

Received: 17 July 2024
Revised: 27 July 2024
Accepted: 29 July 2024
Published: 30 July 2024

1. Introduction

In recent years, with the popularization of the Internet in people's daily life and the significant increase in dependence, the forms of network threats have become increasingly diversified. These include illegal intrusion by hackers and the widespread spread of malware. These online behaviors not only leak sensitive information and damage computer systems but also cause website and network paralysis, resulting in extremely serious damage to individuals and organizations [1]. In view of this severe network security situation, some important places maintain an air gap network between internal computers and external computers for security and stability purposes. This means that data are transmitted through isolation methods, e.g., importing from the external network using optical drives or mobile hard disks, without direct connection to the Internet. Air gap isolation technology has become a crucial defense measure against increasingly rampant cyber threats to protect critical information assets in various sectors, including government [2], military [3], financial institutions, and industrial control systems. Thanks to strict network isolation methods, air gap networks remain one of the most effective means of protecting computer data.

However, air gap networks are not impregnable fortresses when it comes to security. Even under isolated network conditions, computer hardware, external devices, and various IoT facilities in a closed environment can still emit various types of signals, such as optical, electromagnetic, magnetic fields, acoustic, vibration, and thermal. Air gap bridging is a cunning technique that utilizes these signals as covert transmission media to silently send sensitive data to external networks. This covert channel reminds us that, even in seemingly

closed and isolated network environments, we need to maintain a high level of vigilance and comprehensive security measures.

1.1. Covert Channels-Related Works

In a concealed air gap channel, data need to be transmitted from a physically isolated closed network to an external network. Based on previous research, air gap malware can manipulate the load of air gap computer systems (PCs and their peripheral devices) to generate various types of signals. However, the available media for air gap covert channels are limited. Generally, it can be divided into four types of media: electromagnetic, acoustic, optical, and others (such as power lines, heat, and vibration). An air-gapped covert-channel environment is shown in Figure 1 [4].

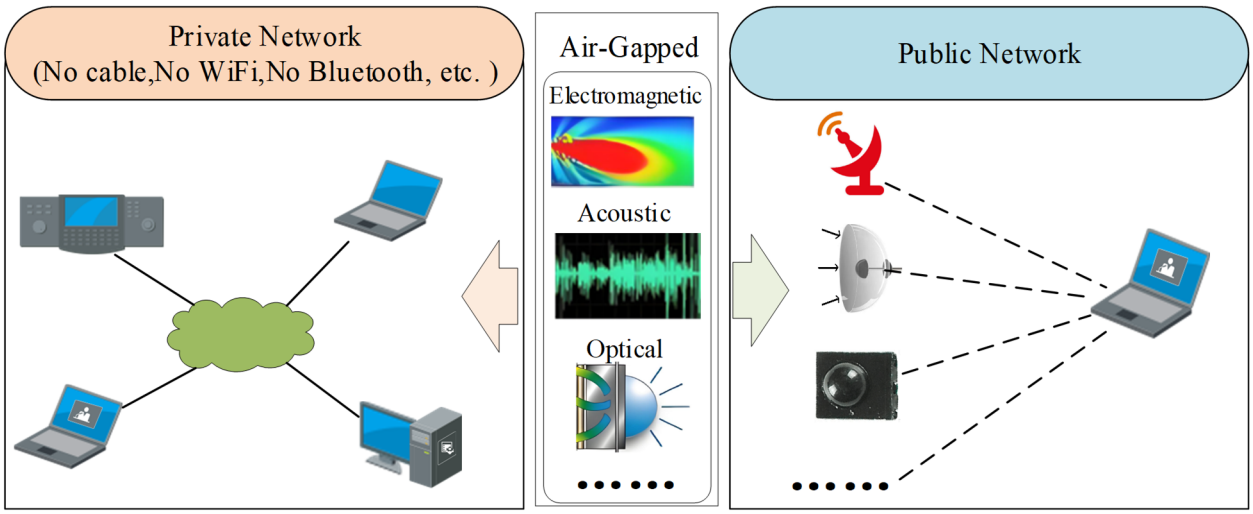


Figure 1. Air-gapped covert-channel environment.

When electricity flows through computers and their peripheral devices, it naturally generates magnetic fields and electromagnetic radiation. These electromagnetic radiations have become a viable channel for data transmission. For example, in 2022, Zihao Zhan et al. proposed BitJabber, which establishes a covert channel that can achieve a data rate of 100,000 bps, with an error rate of around 0.05%, based on the electromagnetic signals generated by DRAM clocks [5]. In 2023, Shakthi Sachintha et al. established a secret channel based on the electromagnetic radiation from Ethernet cables, achieving a data rate of 10 bps at a distance of two meters [6]. In 2024, Md Faizul Bari et al. proposed NoiseHopper, which transmits data up to a distance of approximately 5.5 m, within a range of 100 kilobits per second, by controlling embedded devices to emit electromagnetic waves [7].

When malicious software can manipulate devices to emit sound waves, this can also be a feasible channel. For example, Mordechai Guri proposed that CD-LEAK maliciously generates sound signals through optical CD/DVD drives with a communication distance of up to 8 m [8]. Li Duan et al. introduced the auditory-masking effect into the acoustic-masking communication system and achieved an accuracy of around 90%, even when the distance between the sound source and receiver is within 3 m [9]. In 2023, Ivan Miketic et al. established a communication link between two unauthorized entities sharing data, including integrated circuits [10]. Mordechai Guri et al. achieved communication between two air gap computers using their respective speakers, with a maximum communication distance of 9 m [11]. Hyeongjun Choi et al. proposed CASPER, which utilizes internal speakers on a computer motherboard to transmit data at any distance within 1.5 m and achieves a maximum transmission speed of 20 bps [12].

Malicious software can exploit luminescent sensors on computers or external devices. For instance, Jieun Lee proposed a tangible optical air gap-bridging method that demonstrated the feasibility of using smart light bulbs and other mobile communication

technology devices for gas gap bridging [13]. Zhanqi Liu et al. validated a sub-noise optical covert communication scheme and implemented covert communication in optical fibers [14]. LaserShark introduced a new method to infiltrate data into air-connected systems, enabling long-distance (25 m), bidirectional, and fast (18.2 kilobits per second) laser secret communication channels [15].

Other media that can be utilized include PowerHammer [16], proposed by Guri, which uses power lines to leak signals; HVACKer, proposed by Yisroel Mirsky et al., which utilizes air conditioning for bidirectional covert communication [17]; and Nikolay Matyunin's method of utilizing vibration to achieve covert communication through covered channels [18].

However, as some traditional air gap-network communication technologies are gradually gaining recognition from the public, corresponding defense measures have also been proposed. To our knowledge, our current paper is the first academic research on water-pressure covert channels and proposes targeted defense methods and strategies.

1.2. Our Contribution

Based on the research background mentioned above, we propose a new covert communication method called HydraulicBridge. It is an air gap channel that utilizes liquid pressure in pipelines to establish communication with internal computers in industrial facilities. HydraulicBridge encodes information into liquid pressure and transmits it through pipelines to pressure sensors within the system. These sensors then transmit the pressure data to a computer with control permissions, enabling infiltration. Simultaneously, computers within the organization control intelligent water valves of liquid pipelines in industrial systems (such as factories, water plants, or hydropower stations) to manipulate the liquid pressure and transmit information to the outside world, achieving exfiltration. The following points outline the contributions of our paper:

We proposed an air gap channel that utilizes pipeline liquid as an information medium and designed experiments to verify its feasibility. We innovatively utilized the pressure of the liquid as the air gap channel, manipulating the intelligent water valve to change the liquid pressure for transmitting information and using a water-pressure sensor as the receiver to obtain liquid pressure data. This provides a new concept for constructing air gap channels. To our knowledge, this is the first time that an air gap channel utilizing liquid pressure as an information medium has been proposed.

After achieving bidirectional communication, we discovered through the literature review that many methods proposed by previous researchers can only achieve unidirectional transmission, while our method allows for bidirectional transmission of information.

Based on experimental data, several communication encoding methods that can be used for HydraulicBridge have been proposed. We conducted experiments on the proposed method to verify its feasibility. Experiments were conducted on these encoding methods, and the results demonstrated that our simulated communication performed well.

The rest of this article is structured as follows: The Section 2 discusses the technical background, and the Section 3 provides scenarios for covert communication. The Sections 4 and 5, respectively, introduce the experimental setup of the channel and the protocol for covert water-pressure communication transmission. The Section 6 discusses the experimental results and analysis evaluation. The Section 7 covers evidence collection and countermeasures, while the Section 8 addresses conclusions and future research.

2. Technical Background

In this section, we provide a technical investigation of water-network automation management, including the core components of electric water valves and water-pressure sensors. This paper will help readers understand the technology and management architecture of automated water-network management, as well as the working principles of core components.

2.1. Automated Management Technology for Water Network

With the rapid development of Internet of Things (IoT) technology, the field of industrial automation is undergoing a profound transformation. In this context, various industrial systems, including factories, pharmaceutical factories, and water treatment plants, are embracing intelligent transformation by utilizing sensor networks such as smart water valves, electric water pumps, and water-pressure sensors to monitor and control liquid pipelines in real time with accuracy. A large number of high-frequency recorders, like water-pressure sensors, are widely deployed in the system to capture and record transient pressure changes; even small fluctuations are not missed. By continuously collecting and analyzing these data, intelligent water networks can achieve refined operation and management. This enables the system to accurately infer hydraulic status and system parameters based on measurement data (such as pressure and flow rate), thereby providing strong technical support for system safety monitoring.

Additionally, the application of IoT technology can enhance the maintainability of industrial systems. By continuously monitoring key parameters, the system is capable of identifying potential fault points and taking preventive measures before issues arise, thus avoiding large-scale shutdowns and production losses. Through deploying intelligent sensor networks and analyzing and utilizing massive data, industrial systems can achieve more efficient and cost-effective operation. With the continuous advancement of technology and increasing application depth, IoT technology will play an increasingly crucial role in the industrial field, promoting intelligent and automated industrial production. Figure 2 illustrates a typical intelligent water supply network that is generally divided into four levels: perception layer, transmission layer, data layer, and application layer [19].

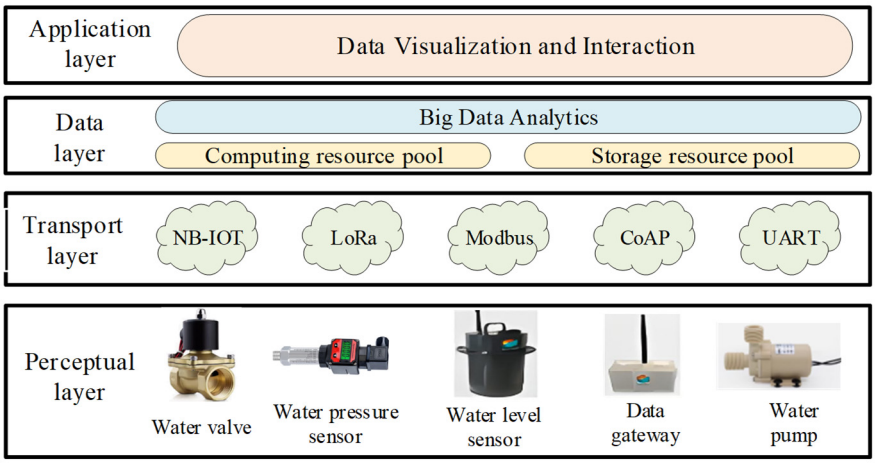


Figure 2. Typical water supply network's architecture.

The raw data of water management are collected by perception-layer devices, converted into protocols through the transmission layer, and then aggregated in the data layer for storage and classification. Finally, the analysis results are visualized and displayed in the application layer to assist in water management and decision-making.

However, it is precisely because of the widespread application and high interconnectivity of smart water networks that a feasible physical channel has been provided for hackers to maliciously infiltrate the control systems of water networks. This raises new security challenges, as hackers can manipulate water-pressure fluctuations using sensors and control devices in smart water networks to encode and transmit information, achieving covert communication. This method is similar to underwater acoustic communication technology, where information is transmitted by modulating underwater sound waves [20]. For instance, controllers can remotely operate electric water valves or pumps to send binary signals through specific patterns of pressure changes, encoding information in seemingly normal water-pressure fluctuations to mask their communication activities and achieve

covert control of the water-network control system. This type of covert channel possesses the following characteristics:

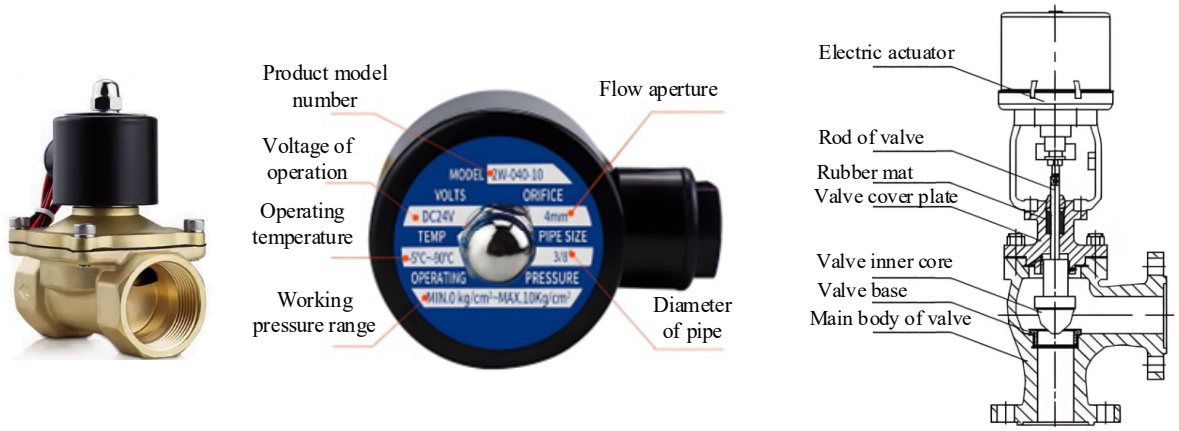
High concealment: The use of water-pressure fluctuations for communication has extremely high concealment, making it difficult for traditional security-monitoring equipment to detect these subtle physical changes.

Wide impact: Once hackers successfully infiltrate the water-network control system, they can not only interfere with the normal operation of industrial systems but also have a serious impact on public safety, such as tampering with water-quality data and maliciously controlling water-valve switches.

Difficulty in defense: Since water-pressure fluctuations are a natural phenomenon, traditional protection mainly focuses on a network-level traffic analysis, without delving into the signal details at the physical layer. It requires high technical expertise to identify and filter out malicious signals without affecting the normal operation of the system.

2.2. Electric Water Valve

In the water-network system, valves are key equipment for controlling water flow, and their working principle and performance play a crucial role in the stability and operational efficiency of the entire system. Valves are control components in fluid transportation systems, mainly used to open and close pipelines, control flow direction, and regulate parameters of the transported medium. In the smart water management system, smart water valves are connected to the central control system through IoT technology to achieve remote valve control. Sensors can also be installed on the valve to monitor real-time operation status, flow rate, pressure, and other parameters of the valve and transmit data to the central control system for analysis and processing. Once an abnormal situation is detected, an alarm signal will automatically be issued by the system to remind operators to handle it promptly. The intelligent water valve can automatically adjust its opening based on instructions from the central control system and data collected by sensors, achieving precise control of water flow. This intelligent regulation method can be flexibly adjusted according to actual needs, while improving the utilization efficiency and management level of water resources. The appearance and schematic diagram of the intelligent water valve are shown in Figure 3.



(**a**) (**b**) (**c**)

Figure 3. Physical depiction of an intelligent water valve includes (**a**) the appearance of the water valve, (**b**) a manual for the water valve, and (**c**) an internal structure diagram of the water valve.

2.3. Water-Pressure Sensor

Water-pressure sensors are common types of pressure sensors in the industry, widely used in various industrial automation environments, water conservancy and hydropower engineering, production automation systems, and transmission pipelines. Electronic water-pressure sensors typically consist of a small chip, an oscillator, an amplifier, and an output terminal. Their working principle is to directly apply the water pressure to the sensor's

diaphragm, causing it to produce a micro displacement proportional to the water pressure. The appearance and structure diagram of the water-pressure sensor are shown in Figure 4. This converts the pressure into electrical signals, which are then transmitted to the amplifier and output terminal for conversion and outputting of a corresponding real-time reading of the pressure value by electronic devices. A wiring diagram of a water-pressure sensor is shown in Figure 5.

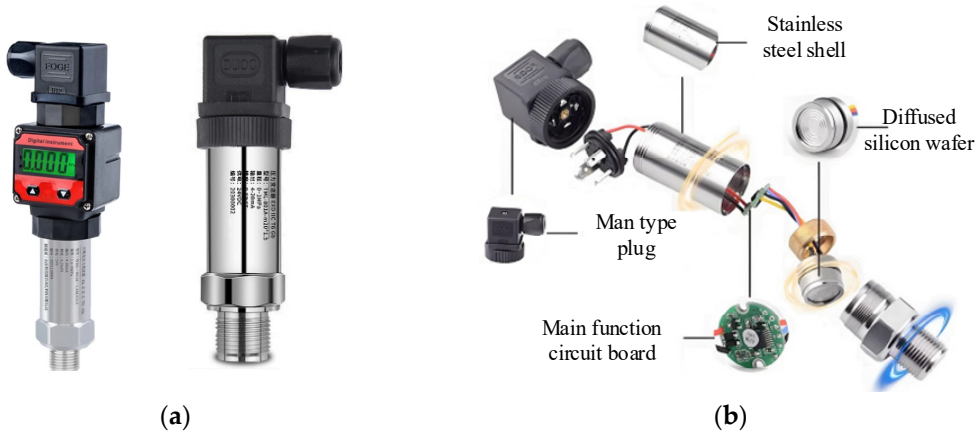


Figure 4. Water-pressure sensors. (**a**) The appearance of the water-pressure sensor. (**b**) Internal structure diagram of water-pressure sensor.

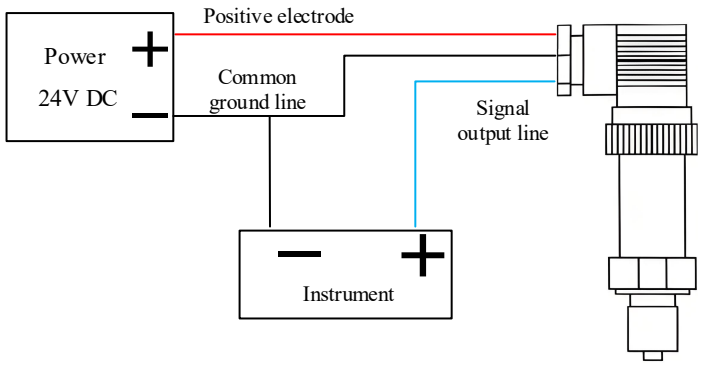


Figure 5. Wiring diagram of water-pressure sensor.

3. Covert Communication Scenario

In the envisioned scenario, the target host has been infected with covert communication software and has already been activated. When the preset working conditions are met, the software can silently collect sensitive data or information from inside the target computer, according to the predetermined instructions. To overcome the limitations of physical isolation, this sensitive information will be transmitted to external sources through non-traditional and difficult-to-detect communication channels, such as electromagnetic radiation leakage, power fluctuations, and even sound-wave signals. These media are often challenging to detect under ordinary surveillance, providing concealment for data transmission. Ultimately, by intercepting and decoding signals transmitted through these covert channels, recipients can obtain sensitive information or intelligence from within a tightly protected state in the target computer. A common covert channel-communication model is shown in Figure 6.

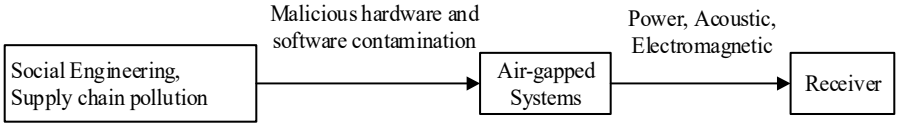


Figure 6. Common covert channel-communication model.

In the era of intelligence, intelligent devices for water resource management are widely utilized in various water supply systems, including remotely controllable intelligent water valves, water-pressure sensors, and water-quality sensors. Within a complex water supply system, there typically exists a central server and multiple branch centers. The central server has control over all equipment and valves within the entire water supply network, as well as access to all sensor data throughout the network. To ensure system security, core computers or computers storing sensitive content maintain air gap isolation from external network devices. However, isolated computers can be interconnected through a water network; thus, when one (or more) device controls its valve status to change it, the resulting alteration in water pressure at the other end of the pipe can be detected by a water-pressure sensor. If this process is properly controlled, certain devices can encode information to regularly open and close valves while transmitting information through changes in water pressure and receiving signals via alterations in the readings of water-pressure sensors. Consequently, bidirectional communication between infected devices can be achieved due to independent valve control and utilization of separate sets of intelligent devices.

When a host in the target system is infected with a virus, it can utilize the intelligent valves and water-pressure sensors under its control to transmit information. Due to the complexity and high precision of industrial systems, only a small number of computers are required to execute critical instructions for covert communication throughout the entire system. Additionally, due to the interconnectivity of the water-network system, information can also be disseminated through flooding, enabling adjacent monitoring computers to exchange information via the water network. The HydraulicBridge covert channel-communication model is shown in Figure 7.

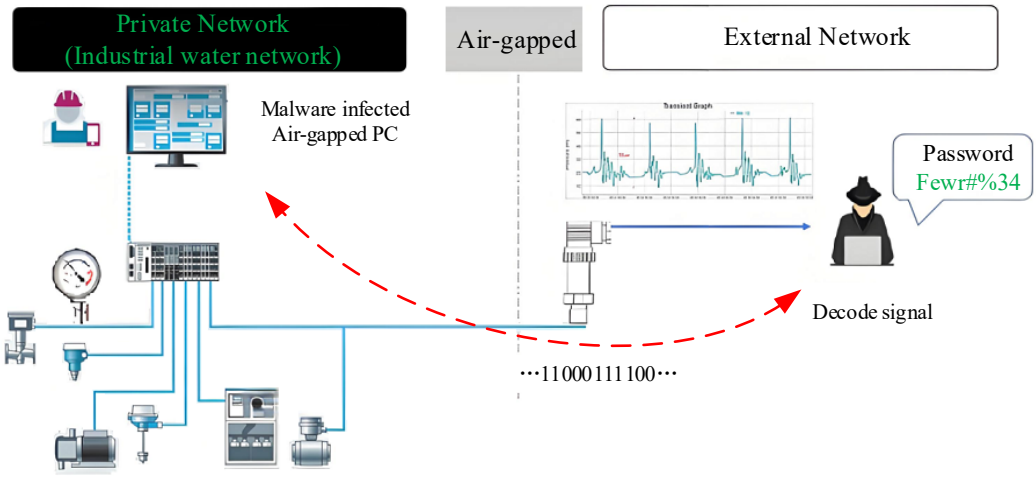


Figure 7. HydraulicBridge covert channel-communication model.

3.1. Signal Transmitter

This paper explores the use of physical media—water flow—as a carrier for data transmission. In the system, precision electric water-valve devices are installed, which are controlled by advanced microprocessors and can accurately adjust the speed and flow rate of water in the pipeline according to preset algorithms or real-time management instructions received. This process not only achieves intelligent management of water resources but also opens up new avenues for covert data transmission.

In the data-modulation stage, the management computer converts the binary data signal to be sent into a series of water flow-variation patterns through specific encoding techniques. For example, a high flow rate may represent "1" in binary, while a low flow rate represents "0". This data-modulation method is similar to amplitude modulation (ASK) in digital communication, but here the carrier wave is not radio waves but actual water flow. These patterns may manifest as minor adjustments in water-flow velocity, periodic fluctuations in flow rate, or specific sequences of on–off operations. They ensure that data

can be accurately embedded into the dynamics of water flow. In this way, the data act like a messenger carried on top of the flowing water and continuously transmitted to the outside world. This unique communication method is both covert and efficient, allowing data transmission within isolated networks.

The remote receiver deploys a highly sensitive network of water-pressure sensors, which can monitor and capture subtle changes in water flow pressure in real time. These changes are then converted into electrical signals, which are analyzed and decoded by specialized signal-processing systems, ultimately restoring the original data information. To ensure the integrity and accuracy of the data, strong data-processing capabilities at the receiving end, along with precise algorithm support, are required. This method of using water flow for data transmission is an innovative covert communication technology that not only utilizes existing water-pipe networks as a transmission medium but also provides a concealed communication method that is difficult to detect through traditional monitoring methods for specific environments.

3.2. Signal Receiver

The remote receiver relies first on highly accurate water-pressure sensors, which are carefully arranged at key locations in the pipeline to capture even the slightest fluctuations in water pressure. (1) Signal acquisition: Water-pressure sensors need to have extremely high sensitivity and stability, enabling them to accurately capture water-pressure signals carrying data in complex and changing environments. (2) Signal filtering: After capturing the water-pressure signal, the next step is to refine it by removing noise and interference, separating the effective signal carrying data, and minimizing background noise and irrelevant interference. This lays a solid foundation for subsequent decoding work. (3) Data decoding: After filtering, the pure signal immediately enters the decoding stage, which is a crucial step in converting physical signals into understandable data. The receiver needs to use a decoding algorithm that is consistent or compatible with that of the sender to map back the water-pressure fluctuations to their original digital information. This process resembles unlocking a password, as it requires a detailed analysis of the received signal to identify the binary code contained within. (4) Error detection and correction: During the process of data transmission, various interferences, such as signal attenuation and noise impact, are inevitably encountered, which may result in errors. Therefore, the receiver needs to utilize technologies like Forward Error Correction (FEC) and Cyclic Redundancy Check (CRC) to continuously monitor the data. Once an error is detected, the error-correction program is immediately activated to repair the data using redundant information, ensuring data integrity and accuracy. (5) Data restoration: After successfully completing all of the aforementioned processing steps, the receiving end can extract the original data from the physical signal in a complete and lossless manner.

4. Communication Experimental Device

In this section, we discuss the air gap-closure device we designed to control liquid pressure and verify the feasibility of our hypothesis. We established a model to simulate the impact of changes in valve status at a specific node in a water supply network on the network's water pressure, as well as whether the sensors at other nodes can detect changes in valve status, in order to evaluate the transmission performance of different nodes within the water supply network. Initially, we designated one node as the "transmitter" and another node as the "receiver". The transmitter's goal was to manipulate water pressure within the network, while the receiver aimed to detect disturbances in water pressure and exchange experiments for validating two-way traffic feasibility.

4.1. Experimental Method

We control the opening and closing of the water valve to create regular fluctuations in water pressure within the pipe. These fluctuations are then detected by a water pressure-monitoring sensor at the other end, enabling signal transmission. Considering that there

is a certain amount of raw water flow in the supply network, we aim to maximize the impact of changes in the valve state on the network to improve the signal-to-noise ratio and ensure accurate detection by distant nodes. We evaluated how different states of the water valve affect the network, selected two optimal valve states, controlled regular bouncing between these states, recorded readings from receiver water-pressure sensors, and analyzed them. We designed a set of rules for valve jumping and assessed performance through multiple experiments.

4.2. Experimental Environment

In order to simulate and study the fluctuation phenomenon of water pressure more accurately, we carefully designed and implemented a testing experiment. The test was conducted in a 15-story high-rise building with an average floor height of 3.8 m. The height difference between the 15th floor and the 1st floor is about 50 m. On this floor, the water supply comes from a main water pipe. We connected a water-pressure sensor to a faucet outlet on the first floor to monitor the water pressure of the first-floor water pipe and connected an intelligent water valve to a faucet outlet on the fifteenth floor to control the water flow rate at its outlet. A computer was used on the 15th floor to control the opening and closing time and angle of the intelligent water valve as a signal transmitter, while another computer was used on the 1st floor to collect real-time water pressure through a water-pressure sensor as a signal receiver. A diagram of the experimental environment is shown in Figure 8.

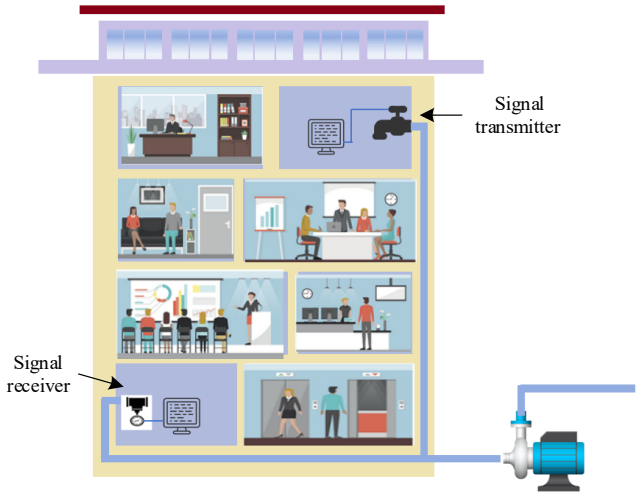


Figure 8. Experimental environment diagram.

4.2.1. Experimental Hardware

The core components used in the test include high-precision electric water valves and highly sensitive water-pressure sensors. This experiment aims to explore the laws of water-pressure changes and their impact on system performance by finely regulating water-flow dynamics.

We chose two electric water valves that feature rapid response and precise control capabilities. They can adjust the timing or opening angle of the valves based on preset programs or real-time instructions, thus achieving accurate control of the water flow. This adaptability ensures the ability to simulate various scenarios of water-flow changes during the experimental process. The model and detailed performance parameters of the electric water valve are shown in Table 1.

To accurately capture subtle fluctuations in water pressure, we equipped two highly sensitive and low-hysteresis water-pressure sensors. It monitors real-time changes in water pressure within the pipeline and converts the data into electrical signals for transmission, providing a reliable basis for a subsequent data analysis. The model and detailed performance parameters of the water pressure sensor are shown in Table 2.

Table 1. Performance parameters of water valves.

Model	Working Voltage	Range	Signal Type	Output-Signal Range	Accuracy
WNK WNK80MA	24 V DC	0–60 bar	Analog Type	4–20 mA/ 0.5~4.5 V	0.5%Fs
Holykell HPT200	12~36 V DC	0–50 bar	Analog Type	4–20 ma	0.15%Fs

Table 2. Performance parameters of water-pressure sensors.

Model	Working Voltage	Range	Operating Temperature Range
DFK	24~36 V DC	0.1~1.5 MPa	−5~180 degrees
KITZ EA200-TE-212	12~36 V DC	0–0.9 MPa	−5~80 degrees

The water-supply pipeline in our experimental building is made of a random copolymer polypropylene material, commonly known as a PPR pipe. This main pipeline connects the water distribution systems of all 15 floors. Additionally, each floor has a branch pipeline with an inner diameter of 28.7 mm and an outer diameter of 31.75 mm.

4.2.2. Software

We developed an efficient code program that integrates precise control logic for electric water valves. By implementing various control strategies—such as periodic opening/closing and gradual opening-angle adjustment—we can simulate different water-flow patterns, which may lead to fluctuations in water pressure. This control method not only enhances the flexibility of the experiment but also improves the representativeness of the results. We created a specialized program to fulfill data-recording needs during the experiment, allowing for real-time sampling and recording of the water-pressure sensor's output signal. To ensure data integrity and accuracy, we set a sampling rate of 30 Hz, capturing 30 water-pressure data points per second and effectively monitoring rapid pressure changes. Additionally, the program includes functions for data storage and preprocessing, aiding in subsequent analysis and processing. Post-experiment, we initially preprocess the collected raw data by steps including noise removal and missing value imputation to ensure that the data quality meets analysis requirements. Thereafter, we perform an in-depth analysis on the preprocessed data using statistical methods and signal-processing techniques. By computing statistical indicators like the mean, standard deviation, and fluctuation range of water pressure, we quantify the pressure-fluctuation characteristics. Finally, we apply the ASK signal-decoding algorithm to decode the signal and recover the communication data.

5. Water Pressure-Transmission Protocol

In developing a new communication system based on water-pressure fluctuations, we designed and implemented a comprehensive communication protocol to standardize the processes of signal generation, transmission, reception, and decoding. This protocol integrates modern signal-processing technology with the principles of fluid mechanics, aiming to achieve stable and efficient data transmission. The following provides a detailed description of the communication protocol.

5.1. Sender Protocol: Signal Generation and Encoding

Electric water-valve control: The computer at the sending end is responsible for generating the data stream to be transmitted and converting it into control instructions for the electric water valve. Specifically, we defined the encoding rules for binary "0" and "1": when "0" needs to be sent, the electric water valve remains closed, resulting in constant water pressure; when "1" needs to be sent, the electric water valve opens, causing a significant decrease in water pressure. The opening and closing actions of the valve

are precisely controlled by a computer program to ensure the accuracy and stability of the signal.

Signal modulation: In order to improve the anti-interference ability and transmission efficiency of the signal, we adopt amplitude shift keying (ASK) as the main modulation method. Specifically, we set two different pressure-level thresholds, corresponding to binary "0" and "1", respectively. In this way, by controlling the on/off state of the electric water valve, it is possible to effectively switch between the two pressure levels, thereby forming a water pressure-fluctuation signal carrying data information. The core code can be found in Algorithm 1.

Algorithm 1 Water valve switch signal-modulation algorithm

```
#Input: Payload, Cycle
for bit in Payload:
    if bit == 1
        HighWaterFlow()
        Sleep(Cycle)
    else
        LowWaterFlow()
        Sleep(Cycle)
#Output ← Water pressure-fluctuation signal
```

5.2. Receiver Protocol: Signal Reception and Decoding

Water pressure-sensor monitoring: The core component at the receiving end is a high-precision water-pressure sensor, which is placed far away from the transmitting end to capture water pressure-fluctuation signals propagated through the pipeline. The sensor continuously monitors changes in water pressure at fixed time intervals (e.g., 30 samples per second) and converts analog signals into digital signals for subsequent processing.

Signal preprocessing: The raw signal received may contain various noises and interferences, making the signal-preprocessing stage crucial. Firstly, a low-pass filter is used to remove high-frequency noise and preserve the basic characteristics of the signal. Then, the rising and falling edges of the signal are identified through differential algorithms to further locate the boundaries of the data bits and prepare for subsequent decoding.

Signal decoding: The decoding process involves mapping the preprocessed signal back to the original binary data stream. A specific pressure threshold is defined as the decision point, where signals above this threshold are considered "0" and signals below the threshold are considered "1". To improve the robustness of decoding, a forward error correction (FEC) mechanism was introduced, which can recover the original data even in cases of poor signal quality. The core decoding algorithm can be found in Algorithm 2.

Algorithm 2 Decoding algorithm of water-pressure signal

```
#Input: WaterPressureSignal, Threshold
#Signal preprocessing
  NewSignal = SignalPreprocessing(WaterPressureSignal)
#Signal decoding
for bit in NewSignal:
   if bit >= Threshold:
        decoded_bits.append('1')
   else:
        decoded_bits.append('0')
return ''.join(decoded_bits)
#Output ← decoded_bits
```

5.3. Bit Wide Encoding

When the water valve of the transmitter is opened or closed, a distinct impulse signal can be detected at the receiving end. By utilizing this characteristic, bit-width encoding can be employed to decode the time interval between two impulse signals received at the receiving end. The detailed encoding mapping table is shown in Table 3.

Table 3. Communication protocol encoding table.

Time Interval of Impulse Signal (s)	Code
m	0
n	1
e	end

By employing this meticulously designed communication protocol, we have successfully transmitted data utilizing water-pressure fluctuations, establishing a technical foundation for the exploration of covert communication technologies in fluid media.

5.4. Data Frame

By employing appropriate encoding methods, a well-designed frame structure can enhance the quality and reliability of communication. Our frame structure design primarily focuses on ensuring the reliability and integrity of information transmission. Our data frame's structure diagram is shown in Figure 9.

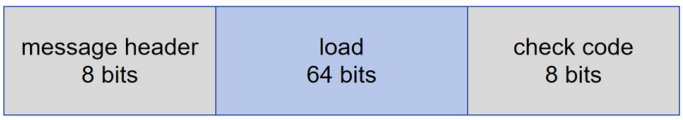


Figure 9. Data frame's structure diagram.

The data frame we designed consists of an 80-bit binary sequence, which includes three parts, "header", "payload", and "checksum", as shown in the Figure 9. The header is 8 bits long and is positioned at the beginning of each frame. It serves for both positioning and synchronization with the receiver. Additionally, the header may include frame-related information, such as frame length. The payload consists of 64 bits of valid information, which represents the binary sequence of the original data to be transmitted, including keys and instructions. The checksum is generated using cyclic redundancy check (CRC) and is 8 bits in length.

It is important to choose an appropriate header to facilitate effective data location by the receiver. When selecting the header, the state of the water valve should be taken into account to avoid triggering the water valve under normal operating conditions as much as possible. Furthermore, considering the presence of noise, the reliability of water-pressure channel transmission is not guaranteed. Therefore, when appending a checksum to the frame, the level of noise should be considered to determine whether the length of the checksum should be increased.

6. Analysis and Evaluation of Experimental Results

In the previous section, we explored the feasibility of water-pressure communication. When external personnel need to communicate in this manner, the water-pressure fluctuations used to carry signals should be minimized as much as possible to ensure minimal interference with normal users during communication. In this section, we mainly discuss the results obtained from the experiments described in the previous section. Based on the experimental findings, we summarized several important experimental parameters and conducted a specific analysis on the two elements of interest in the experiment.

6.1. Fluctuations in Water Pressure

The magnitude of water pressure is the most important factor we focus on. In our model, we transmit information by controlling the changes in water pressure, so we need to analyze the patterns of water-pressure changes as comprehensively as possible.

Turn on and off of water valve: The moment at which the state of the water valve changes in a water pipeline has the greatest impact on the water pressure within the pipeline. As illustrated in Figure 10, the water-pressure signals collected during the opening and closing of the water valve are displayed. Due to the influence of the water hammer effect [21], the water pressure first decreases significantly when the faucet is opened and then stabilizes to a constant value after oscillating. Conversely, when the water valve is closed, the water pressure first increases significantly and then stabilizes to a constant value after oscillating.

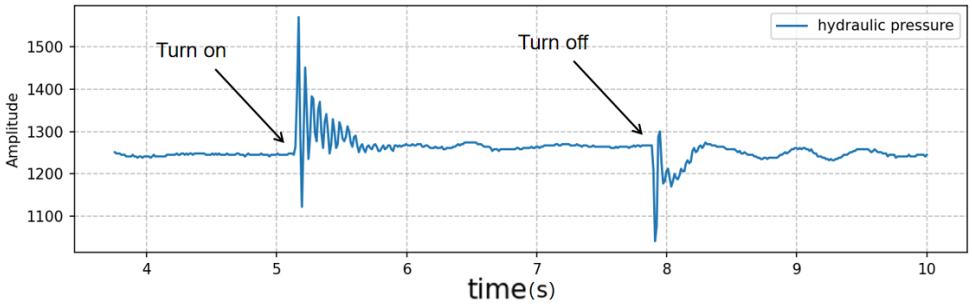


Figure 10. The pressure-signal waveform of the intelligent water valve's on and off.

The water hammer effect refers to the phenomenon of pressure fluctuations caused by the sudden blockage or alteration of fluid flow velocity within a pipeline system. When the fluid flow is abruptly stopped or its rate is altered, the fluid's inertia causes it to continue moving, resulting in a rapid increase in pressure and the propagation of pressure waves. This pressure fluctuation is depicted in Figure 11 [22].

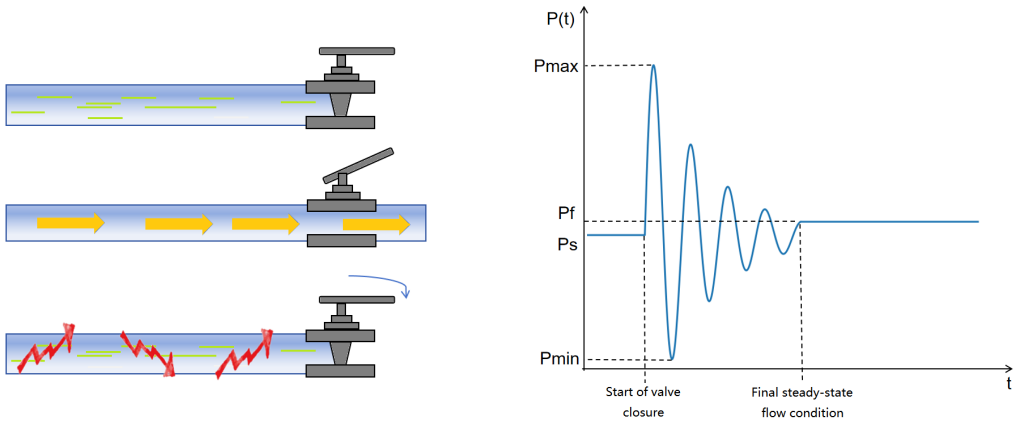


Figure 11. (**a**) Principle diagram of water hammer effect. (**b**) Water hammer-effect waveform diagram of water pressure.

To a certain extent, the impact of the water hammer effect is not entirely negative. Its significant characteristics and high-frequency vibration frequency are also beneficial for the design of filters and signal extraction. We can use filters to filter the received signal, making it easier for the receiving end to observe changes in the water valve state and capture information. A waveform diagram of the water-pressure signal during the operation of the water valve is shown in Figure 12.

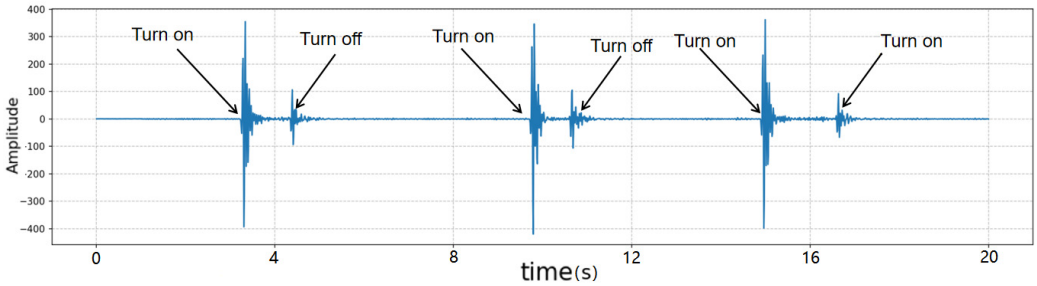


Figure 12. Waveform diagram of water-pressure signal during operation of water valve.

6.2. Water-Pressure Channel

We analyzed the impact of symbol width on communication quality and found that when the transmission frequency of the "transmitter" is too high, that is, the frequency of valve opening and closing is too fast, it may cause the waveform of the water valve's opening and closing to overlap. We set the water valve to switch on and off at a high frequency, with a time interval of less than one second between the on and off. In this experiment, even after filtering, the water-pressure signal cannot distinguish the state of the water valve, resulting in the inability of the receiving end to demodulate the information from the transmitting end, as shown in Figure 13. On the other hand, repeated high-frequency switching actions may quickly cause abnormal alarms in the system.

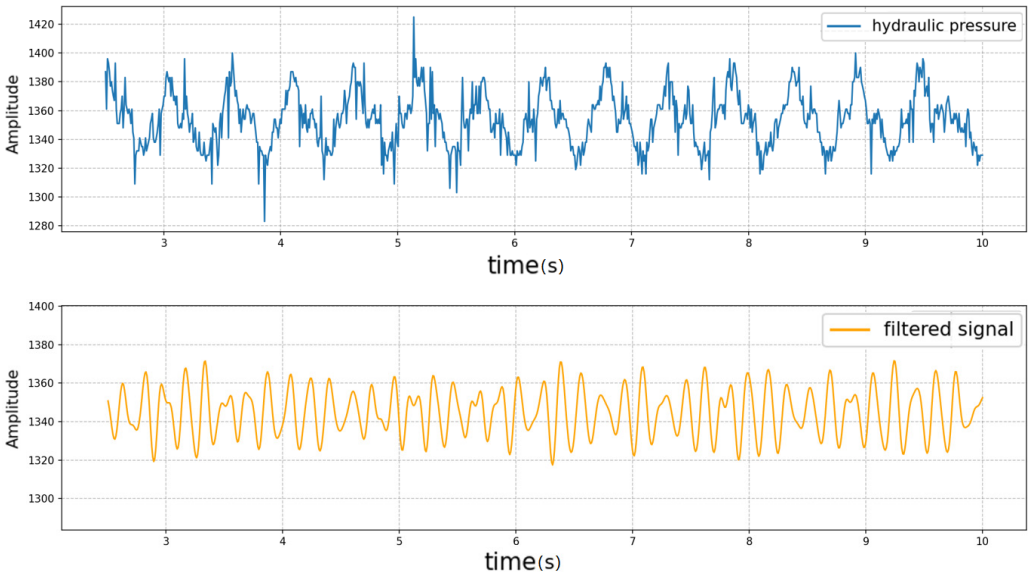


Figure 13. The symbols representing water-pressure signals overlapping.

Figure 14 shows a schematic diagram simulating the transmission of the "001001" sequence. When the distance between two impulse signals is close (m), it is considered a "0". When the distance is far (n), it is considered a "1". If the distance becomes greater, it is decoded as "end", indicating the end of the transmission. This means that the communication rate in our experimental environment is 1 bps.

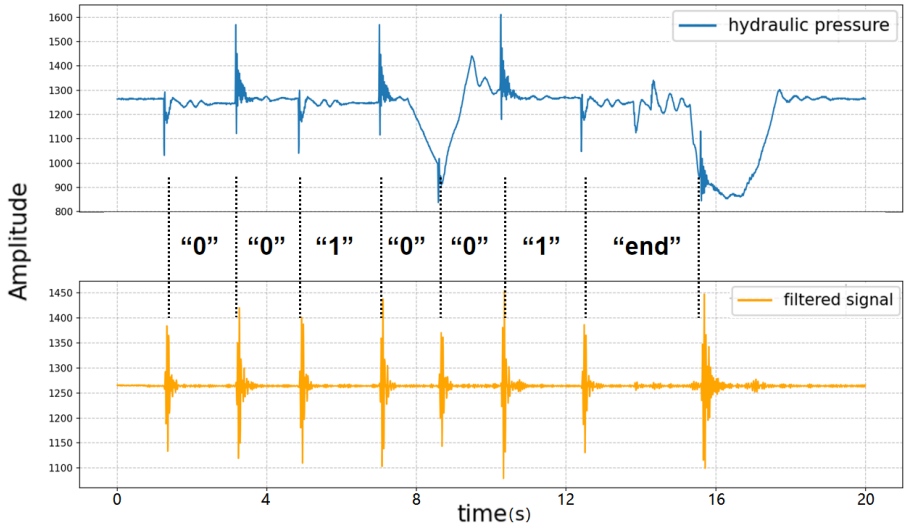


Figure 14. Decoding water-pressure signal.

7. Countermeasures

The concealment and potential harm of HydraulicBridge communication are significant, necessitating preventative measures from various angles. In this section, we primarily introduce several methods for preventing HydraulicBridge covert communication.

Strengthen the detection of water-pressure fluctuations in the security prevention of water supply networks: Abnormal fluctuations in water pressure should be considered an indication of potential vulnerabilities or virus invasions, necessitating immediate identification of the source of the problem.

Strengthen security measures for devices and computers. When external personnel initiate implementation actions, they should first infect the device's computer, thereby triggering the water valve and sensor. Therefore, if viruses can be isolated in the air-gapped network or detected and deleted when they infect computers, we can effectively prevent HydraulicBridge. Secondly, for physical devices, strict access control and authentication mechanisms should be implemented to ensure that only authorized personnel can operate and configure devices in the water network. Additionally, all devices should regularly update their firmware and patch known security vulnerabilities.

Set up device-status logs: When using the HydraulicBridge, it is necessary to frequently call the intelligent water valve and water-pressure sensor. If a status log can be established for the water valve or water-pressure sensor, any abnormalities can be detected in the log, effectively preventing malfunctions of the HydraulicBridge. Additionally, develop detailed emergency plans to ensure that the water network can be quickly restored to normal operation in the event of damage.

8. Conclusions and Future Research

This paper proposes a concealed transmission method based on water pressure, called HydraulicBridge. When the computer of the water-network monitoring system is infected with specific malicious software, it can utilize the existing hardware of the target system without requiring additional hardware or any other modifications. This achieves generality and transparency in terms of hardware. Malicious attackers can infiltrate and exfiltrate information into an air gap network through water pipes. HydraulicBridge utilizes the water supply network in the target system as a channel and leverages water-pressure fluctuations as carriers of information, proposing a targeted communication protocol. Our experiments demonstrated the effectiveness of a communication protocol based on water-pressure fluctuations and showed that its communication rate can reach 1 bit/s in buildings with a height difference of 50 m. Finally, we studied prevention methods for this covert

transmission method and proposed a technique to prevent covert communication using HydraulicBridge.

Author Contributions: Formal analysis, C.L.; writing—review and editing, Y.L. and H.S.; supervision, J.Z. and G.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in the study are included in the article; further inquiries can be directed to the corresponding author.

Acknowledgments: We would like to thank the editors and anonymous reviewers for their detailed comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Roseline, S.A.; Geetha, S. A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks. *Comput. Electr. Eng.* **2021**, *92*, 107143. [CrossRef]
2. Mansfield-Devine, S. Security through isolation. *Computer Fraud. Secur.* **2010**, *2010*, 8–11. [CrossRef]
3. Sarkar, S.; Chakraborty, A.; Saha, A.; Bannerjee, A.; Bose, A. Securing Air-Gapped Systems. In Proceedings of the International Ethical Hacking Conference 2019: eHaCON 2019, Kolkata, India, 17–25 August 2019; Springer: Singapore, 2020.
4. Park, J.; Yoo, J.; Yu, J.; Lee, J.; Song, J. A Survey on Air-Gap Attacks: Fundamentals, Transport Means, Attack Scenarios and Challenges. *Sensors* **2023**, *23*, 3215. [CrossRef]
5. Zhan, Z.; Zhang, Z.; Koutsoukos, X. A high-speed, long-distance and wall-penetrating covert channel based on em emanations from dram clock. *J. Hardw. Syst. Secur.* **2022**, *6*, 47–65. [CrossRef]
6. Sachintha, S.; Le-Khac, N.A.; Scanlon, M.; Sayakkara, A.P. Data exfiltration through electromagnetic covert channel of wired industrial control systems. *Appl. Sci.* **2023**, *13*, 2928. [CrossRef]
7. Bari, F.; Sen, S. NoiseHopper: Emission Hopping Air-Gap Covert Side Channel with Lower Probability of Detection. In Proceedings of the 2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Tysons Corner, VA, USA, 6–9 May 2024; pp. 21–32.
8. Guri, M. CD-LEAK: Leaking Secrets from Audioless Air-Gapped Computers Using Covert Acoustic Signals from CD/DVD Drives. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020; pp. 808–816.
9. Duan, L.; Zhang, K.; Cheng, B.; Ren, B. Privacy threats of acoustic covert communication among smart mobile devices. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9179100. [CrossRef]
10. Miketic, I.; Dhananjay, K.; Salman, E. Covert Channel Communication as an Emerging Security Threat in 2.5D/3D Integrated Systems. *Sensors* **2023**, *23*, 2081. [CrossRef] [PubMed]
11. Guri, M.; Solewicz, Y.; Elovici, Y. Speaker-to-speaker covert ultrasonic communication. *J. Infor-Mation Secur. Appl.* **2020**, *51*, 102458. [CrossRef]
12. Choi, H.; Jung, J.H.; Yoon, J.W. CASPER: Covert Channel Using Internal Speakers. *Sensors* **2023**, *23*, 2970. [CrossRef]
13. Lee, J.; Yoo, J.; Lee, J.; Choi, Y.; Yoo, S.K.; Song, J. Optical Air-Gap Attacks: Analysis and IoT Threat Implications. *IEEE Netw.* **2024**, *165*, 105507. [CrossRef]
14. Liu, Z.; Zhu, H.; Zhang, X.; Chen, S.; Xu, X.; Li, F. Subnoise optical covert communication based on amplified spontaneous emission light. *Opt. Express* **2023**, *31*, 40261–40269. [CrossRef]
15. Kühnapfel, N.; Preußler, S.; Noppel, M.; Schneider, T.; Rieck, K.; Wressnegger, C. LaserShark: Establishing Fast, Bidirectional Communication into Air-Gapped Systems. In Proceedings of the 37th Annual Computer Security Applications Conference, New York, NY, USA, 6–10 December 2021; pp. 796–811.
16. Guri, M.; Zadov, B.; Bykhovsky, D.; Elovici, Y. PowerHammer: Exfiltrating Data from Air-Gapped Computers Through Power Lines. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1879–1890. [CrossRef]
17. Mirsky, Y.; Guri, M.; Elovici, Y. Hvacker: Bridging the air-gap by manipulating the environment temperature. *Magdebg. J. Sicherheitsforschung* **2017**, *14*, 815–829.
18. Matyunin, N.; Wang, Y.; Katzenbeisser, S. Vibrational covert channels using low-frequency acoustic signals. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Paris, France, 3–5 July 2019.
19. Pérez-Padillo, J.; Morillo, J.G.; Ramirez-Faz, J.; Roldán, M.T.; Montesinos, P. Design and Implementation of a Pressure Monitoring System Based on IoT for Water Supply Networks. *Sensors* **2020**, *20*, 4247. [CrossRef] [PubMed]
20. Kim, Y.; Lee, H.; Seol, S.; Park, B.; Chung, J. Underwater Biomimetic Covert Acoustic Communications Mimicking Multiple Dolphin Whistles. *Electronics* **2023**, *12*, 3999. [CrossRef]

21. Pal, S.; Hanmaiahgari, P.R.; Karney, B.W. An overview of the numerical approaches to water hammer modelling: The ongoing quest for practical and accurate numerical approaches. *Water* **2021**, *13*, 1597. [CrossRef]
22. Kandil, M.; Kamal, A.M.; El-Sayed, T.A. El-Sayed. Effect of pipematerials on water hammer. *Int. J. Press. Vessel. Pip.* **2020**, *179*, 103996. [CrossRef]