Virtually Isolated Network: A Hybrid Network to Achieve High Level Security

Jia Xu, Jianying Zhou

Virtually Isolated Network: A Hybrid Network to Achieve High Level Security *

Jia Xu[1] and Jianying Zhou[2]

[1] Singtel, Singapore
jia.xu@singtel.com
[2] Singapore University of Technology and Design, Singapore
jianying_zhou@sutd.edu.sg

Abstract. This paper proposes a hybrid network system (called as "Virtually Isolated Network") that combines an existing low bandwidth isolated network and the Internet, to implement a low cost overlay network with high bandwidth and high level security (precisely, information-theoretic security), without sacrificing security of the existing isolated network. Our approach consists of two main ideas: (1) Connect an isolated network and the Internet in a proper way using 4 physical unidirectional links (also known as "Data Diode" or "Air Gap"), so that the isolated network remains physically isolated; (2) Hide a small part of ciphertext from adversary by exploiting the property of isolated network and using a secret sharing approach.

Keywords: isolated network, hybrid network, unidirectional network link, encryption, secret sharing, information dispersal algorithm, information-theoretic security

1 Introduction

Many existing critical industry systems (e.g. power generation plants, nuclear plants, chemical plants, subway/metro transportation system, etc.) leverage their physical and cyber security on closed or isolated system. They prevent unauthorized entrance using high walls and security guards. Their network systems are physically disconnected from the Internet, making remote attacks via the Internet impossible. If the strict physical security protection is always enforced properly, for example, no one is allowed to setup new wired or wireless communication from the closed system to outside, USB port is disabled, then only

* The first author is supported by the National Research Foundation, Prime Ministers Office, Singapore under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd. The second author is supported by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-31) and administered by the National Cybersecurity R&D Directorate. Part of this work was done when the first author worked in Institute for Infocomm Research, Singapore.

a very low (or ideally zero) bandwidth of convert channel between the isolated network and the Internet is possible to escape from detection by existing cyber and physical security solutions.

We found that some legacy isolated industry control systems have very small bandwidth in their backbone isoloated network, due to historical reason. For example, some metro system has relative large LAN speed in each metro station, but the backbone network connecting each station with the centralized control server has only 2Mbps bandwidth. Such limited backbone network bandwidth is becoming the bottleneck of the whole isolated industry network, since more new services are introduced with time, e.g. CCTV real time video. It will require a huge investment and take a lot of time to upgrade the physical cable network: In a modern city, laying a new fiber path for a long distance is very challenging and may introduce significant side effect to urban transportation system. Therefore, there is an urgent demand to boost the bandwidth of existing legacy isolated network at low cost.

In this paper, we will propose a hybrid network architecture, by connecting an existing isolated network and the Internet in a smart way such that the isolated network remains isolated from the Internet, without sacrificing the security level of the existing isolated network. Meanwhile, we will propose a new encryption method using "encrypt-then-secret-sharing" approach, split the ciphertext into two parts and transmit separately via two communication channels of the hybrid network. Essentially, our novel encryption method can achieve unconditional security, assuming the adversary cannot monitor or eavesdrop the two communication channels simultaneously. Eventually, we are able to boost the bandwidth of legacy isolated network by about 60 times at a very low cost. Our main contributions include

- We design a *unidirectional* hybrid network architecture to connect isolated network and Internet, in a way that the isolated network remains physically isolated. Such unidirectional network is very useful to constantly transmit sensor data from field sensors to a data collection server in an isolated network. Our solution can significantly increase the bandwidth of legacy isolated network at low cost.
- We design a novel data protection method by combining encryption and secret-sharing. By hiding partial ciphertext from adversary, our new method can achieve unconditional security.

The rest of this paper is organized as below: Section 2 will discuss the related works. Section 3 will describe the hybrid network architecture and protocol. Section 4 will propose our novel encryption method. Section 5 will show our experiment result. Section 6 will conclude the paper.

2 Related Works

Symmetric encryption scheme (e.g. AES, Blowfish [3], and Triple DES [4].) could be the most widely adopted cryptographic primitive to protect data confidentiality, especially for large volume of data. AES [2] is a typical example of symmetric encryption scheme, and has been widely adopted in industry due to its security and efficiency for more than one decade.

In additional to encryption techniques, another well-known cryptographic primitive that can be used to protect data confidentiality is "secret-sharing" scheme invented by Shamir [10]. Compared to encryption scheme (e.g. AES [2]) which can only achieve conditional security, secret-sharing scheme may achieve unconditional security (also known as information-theoretic security), assuming the adversary cannot collect sufficient number of shares.

Despite its strong security, Shamir's secret sharing scheme has significant drawbacks when protecting data confidentiality: (1) for (t, n)-secret sharing scheme, the storage overhead is as large as $(n-1)$ times of size of the secret (i.e. the plaintext to be protected); (2) the reconstruction [7] (or decoding) process is not as efficient as DES or AES.

Rabin [8] proposed "information dispersal algorithm" with zero storage overhead, such that the sum of sizes of all shares is equal to the size of secret message size. His solution is conceptually simple: Let row vector $\boldsymbol{m} = (m_0, m_1, \ldots, m_n)$ be the secret message. Choose an invertible n by n matrix $\mathbf{T}$ with inverse matrix $\mathbf{T}^{-1}$. By multiplying row vector $\boldsymbol{m}$ with matrix $\mathbf{T}$, we obtain the n shares $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1}) = \boldsymbol{m} \times \mathbf{T}$. Accordingly, the original secret message $\boldsymbol{m}$ can be recovered by matrix multiplication $\boldsymbol{m} = \boldsymbol{c} \times \mathbf{T}^{-1}$. Recently, Resch and Plank [9] coined the term "All or Nothing" (AONT, for short) for information dispersal algorithm. Othman and Mokdad [1] proposed to protect communication confidentiality by sending each share of message in distinct network path from the same sender to the same receiver (Figure 1).

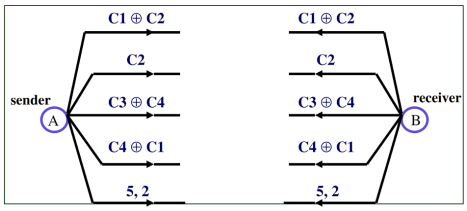

Fig. 1. Enhancing Data Security in Ad Hoc Networks based on Multipath Routing

In the example shown in the above figure, the message is divided into 4 equal-length parts C_1, C_2, C_3 and C_4, and each part is delivered via a distinct

[3] https://www.schneier.com/academic/blowfish/

[4] http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf

network path from the sender to the receiver. Readers can easily figure out how to recover all of 4 parts $C_1 \ldots C_4$ on the receiver side, if all transmissions are free of errors.

Alternatively, Krawczyk [5] attempted to make each share shortened, by dividing ciphertext of the long secret message into n pieces, and then apply Shamir's secret sharing scheme over the encryption key. Thus, the storage overhead is linear in short encryption key size and is a fraction of secret message size.

It is also worthy to pointing out, in network coding techniques (e.g. [6,3,11,4]), data streams could be merged or divided in any intermedia communication node. Unlike this work, their purpose is to improve the network throughput, efficiency and scalability, as well as resilience to attacks and eavesdropping.

3 Network Architecture

We will construct a unidirectional *Virtually Isolated Network* (VIN for short). If bidirectional communication is required, then two sets of VIN can be combined to achieve bidirectional communication, at the cost that security level of the existing isolated network will be downgraded from physical isolation to software isolation.

3.1 Network Hardware Components

The network hardware components of virtually isolated network are described as below, and summarized in Table 1. Their interconnection is illustrated in Figure 2.

- **Sender**: The Sender device will encrypt incoming data stream and split it into two output streams with possibly unequal sizes. The smaller output stream will be sent to Repeater 1 via a unidirectional physical network link (a.k.a data diode or air gap), and the larger output stream will be sent to Repeater 3 via another unidirectional physical network link, too. Ideally, the Sender device is recommended to be designed as a minimum single feature hardware/software system, more precisely, a customized FPGA chip running a customized driver, since unnecessary hardware or software components may potentially introduce more vulnerabilities.
- **Receiver**: The Receiver device will receive two input streams via unidirectional network link from Repeater 2 and Repeater 4, merge them together and decrypt them. Like the Sender device, ideally, the Receiver device will also be designed as a minimum single feature hardware/software system, more precisely, a customized FPGA chip running a customized driver.
- **Repeater** 1,2,3,4: Repeater 1 (3, respectively) will receive data stream via unidirectional network link from Sender, and relay the data stream to Repeater 2 (4, respectively) via *bidirectional* isolated network (Internet, respectively). These Repeater devices will run generic hardware/software system

with customized configuration. Except availability protection, no special security protection is required.
- (Existing) **Isolated Network**: A network which is physically disconnected with the Internet. Without loss of generality, we assume this is a TCP/IP network in this work.
- (Existing) **Internet**: The global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billions of devices worldwide [5].

Computation Hardware and Software Specification

- The computation hardware in Sender/Receiver device could be a customized single feature FPGA, which has only TCP/IP network stack, encryption and error correcting code functionality. Software in Sender/Receiver is a minimum driver, and no full OS (like Linux, Windows, etc) is required.
- The computation hardware and software in Repeater devices could be standard commercial products. Repeaters should have storage as buffer. We will develop our own software to convert between the UDP data stream (on unidirectional network link side) and TCP data stream (on bidirectional network link side).

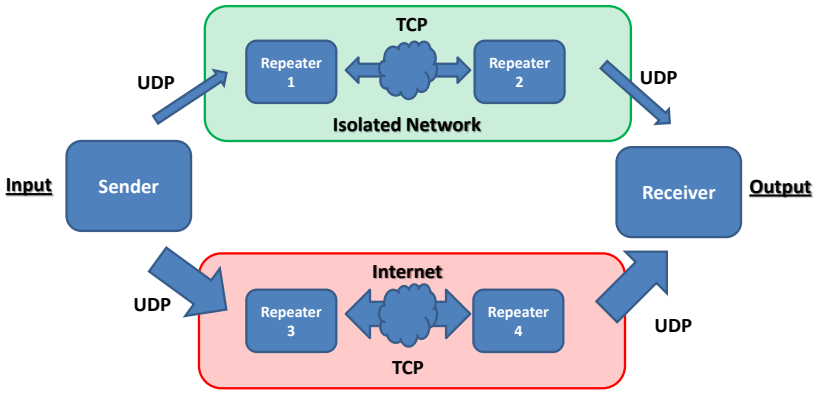

Fig. 2. Network Architecture Diagram of Virtually Isolated Network

All of Sender, Receiver and Repeater devices are well protected against physical attack or unauthorized access. Digital protection mechanism of privacy and integrity of communication data lies in both Sender and Receiver devices. Even if all Repeater devices are compromised, the privacy and integrity of the communication data should not be affected, although availability of communication data could be jeopardized.

[5] Source: `https://en.wikipedia.org/wiki/Internet`

Table 1. Hardware Components of Virtually Isolated Network

Device	Hardware	Software	Network Input	Network Output	Security Risk	Protection
Sender	FPGA (A.E., ECC, TCP/IP)	driver	bidirectional	2 unidirectional	confidentiality and integrity	crypto, minimum system, frequent key refresh, physical protection
Receiver	FPGA (A.E., ECC, TCP/IP), buffer storage	driver	2 unidirectional	bidirectional	confidentiality and integrity	crypto, minimum system, frequent key refresh, Physical Protection
Repeater1,3	generic (TCP/IP), buffer storage	generic OS	1 unidirectional	bidirectional	availability	physical protection, multi-path routing
Repeater2,4	generic (TCP/IP)	generic OS	bidirectional	1 unidirectional	availability	physical protection, multi-path routing

Note: A.E. refers to Authenticated Encryption. ECC refers to Error Correcting Code.

We will construct a new cryptographic algorithm for Sender and Receiver devices, which can split a data stream into two streams in a secure manner. We will design a minimum hardware/software system for Sender and Receiver devices, instead of adopting a generic hardware/software system for Sender and Receiver devices, since a generic system is much more complex and consists of a lot of features and functionalities, which are not required by the virtually isolated network and could potentially bring more vulnerabilities to the entire system. To ensure availability of the constructed virtually isolated network, we will guard Repeater devices with strong physical protection mechanism, and adopt multi-path routing with redundant data packets between Repeaters in Internet, as showed in Figure 3.

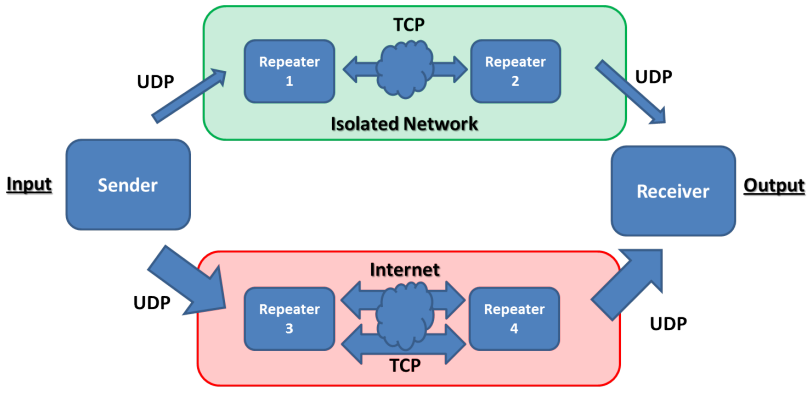

Fig. 3. Multi-path Routing between Repeater 3 and 4

3.2 Network Communication

Network Protocol The Sender or Receiver communicates with Repeater (1-4) using UDP protocol, and Repeater 1 (3, respectively) and Repeater 2 (4, respectively) communicate using TCP protocol, as illustrated in Figure 2.

The transmission reliability of bidirectional link relies on standard TCP ACK-and-Resend mechanism. Furthermore, multiple-path delivery [6] (as illustrated in Figure 3) of redundant data packet can increase availability against denial of service attack. The underlying UDP protocol by itself is not reliable against data loss. The transmission reliability of unidirectional link relies on the following factors:

- Highly reliable unidirectional communication link, therefore order is preserved, although UDP protocol is used (e.g. one-way fiber connection, Li-Fi, light-based communication);
- Very short distance (e.g. smaller than 10 cm);
- Highly controlled environment, thus very low environment noise;
- Error correcting code.

Journey of a data block from Sender device to Receiver device Every data block sent from Sender to Receiver will be identified by a sequence number [7], which is unique among all data blocks within a proper time period. When a data block is split into two smaller data slices by Sender, the two smaller data slices will have the same sequence number as the original data block. The sequence number will have two roles:

- Ensure correct order among data blocks at the Receiver device;
- Allow Receiver to match a data slice from Repeater 2 and a data slice from Repeater 4, and merge the two data slices to restore the original data blocks.

We remark that: (1) To differentiate from TCP sequence number, we may refer the sequence number for data block as "VIN sequence number". (2) VIN sequence number should not be encrypted. (3) When a large data block with VIN sequence number i is divided into multiple IP packets, each of the resulting IP packet should be labeled as (i, j), $j = 0, 1, 2, \ldots$, where the first index i helps to distinguish them from other VIN data blocks and the second index j, helps to maintain the correct order among themselves.

1. Sender encrypts a given data block m with VIN sequence number i using secret key K, and splits the resulting ciphertext c into two ciphertext shares c_0 and c_1. Optionally, Sender may encode c_0 and/or c_1 using error correcting code (ECC).
2. Sender device sends data c_0 (c_1, respectively) with VIN sequence number i via UDP protocol to Repeater 1 (3, respectively).

[6] `https://en.wikipedia.org/wiki/Multipath_routing`

[7] This could be simply a 32 bits count number and the number will loop back after 2^{32} blocks.

3. Repeater 1 (3, respectively) generates a TCP packet based on the received UDP packet, where the VIN sequence number is set to i and the payload is identical to the payload of received UDP packet. Repeater 1 encapsulates this TCP packet into a standard IP packet with Repeater 1's (3's, respectively) IP address as source address and Repeater 2's (4's, respectively) IP address as destination address, and sends this IP packet to Repeater 2 (4, respectively).
4. Once receiving an IP packet from Repeater 1 (3, respectively), Repeater 2 (4, respectively) will generate a UDP packet with the same VIN sequence number, where the payload of UDP packet is identical to the payload of the received TCP packet. Repeater 2 (4, respectively) sends this UDP packet to Receiver device.
5. Once receiving the UDP packets from Repeater 2 (4,respectively), the Receiver device will retrieve the payload c_0 (c_1, respectively), from a group of UDP packets with the same VIN sequence number i.
6. Receiver device will match ciphertext share c_0 from Repeater 2 with ciphertext share c_1 from Repeater 4 according to their VIN sequence number, then decrypt ciphertext (c_0, c_1) using the shared secret key K, to obtain the message block m. If required, Receiver device will decode c_0 and/or c_1 using ECC.

Communication Delay The communication latency of the proposed hybrid network will be the encryption/decryption time plus the maximum of the network latency time in the two communication channels. The speed of our proposed encryption method is estimated as at least a half of speed of the underlying block cipher (e.g. AES). Both the isolated network and Internet can run SSL protocol with acceptable network delay. Therefore, the total network delay in our proposed hybrid network will be only marginally longer than the two communication channels.

Unidirectional Network and Bidirectional Network Compared to bidirectional network, there is an inherited theoretical limitation for unidirectional communication network: *Sender cannot get any feedback from Receiver or Repeaters, and thus cannot adjust its sending speed according to the network congestion status. Furthermore, Sender cannot know which data packet may be lost, and will not re-send the lost packet.*

Fortunately, in practice, this limitation can be reduced to minimum. From Figure 2, we can find that UDP protocol over unidirectional link is only used to connect Sender/Receiver device with Repeaters, and TCP protocol over bidirectional link is employed to connect Repeaters. As we discussed in Section 3.2, the unidirectional link could achieve extremely high reliability, and the TCP connections between Repeaters can recover possible data loss using standard ACKed-Resend mechanism. Therefore, as long as Repeaters have a sufficiently large buffer storage and sending speed of Sender device is set to a proper value according to the long-term network statistics of the Internet and the isolated

network, the unidirectional VIN could achieve practically reliable end-to-end communication in most of time.

3.3 Security Features Guaranteed by Hardware Architecture

The existing isolated network is still physically disconnected from the Internet. More precisely, in our setting in Figure 2, there is still no physical network path from the Internet (in light red color in Figure 2) to the existing isolated network (in light green color in Figure 2), and no physical network path from the existing isolated network to the Internet either.

Two VINs can be combined to provide bidirectional communication. In this case, theoretically, there will be a physical link between the Internet and the existing isolated network. This physical link could be effectively cut-off by cryptographic protection and software method (like firewall) in the Sender/Receiver device.

Note that, the existing isolated network is assumed to be well disconnected from the Internet and the physical site of the isolated network is also well protected from any physical attack. However, the computer/network devices inside the isolated network might potentially have vulnerabilities or even trapdoors and malwares, possibly embedded by vendors or distributors.

4 Our Proposed Encryption-then-Secret-Sharing Method

In the VIN network, Sender will encrypt every data block and split the ciphertext into two shares. The smaller share will be sent to the isolated network and the larger share to the Internet.

4.1 Our Secret Sharing Method

Let positive integers ρ and τ be system parameters. We define our secret-sharing (or information dispersal) scheme $(\mathsf{KGen}, \mathsf{Split}, \mathsf{Merge})$ with help of two secure hash functions $h(\cdot)$ and $H(\cdot)$ as below.

- $\mathsf{KGen}(1^\lambda) \to k$: Randomly choose a λ-bit string $k \in \{0,1\}^\lambda$ and output k.

- $\mathsf{Split}(k; u) \to (x, y)$ where $u \in \{0,1\}^{\rho(\tau+1)}$, $x \in \{0,1\}^\rho$ and $y \in \{0,1\}^{\rho\tau}$.
  1. Divide the bit string u into a prefix v and a suffix w such that $u = v\|w$ and $|w| = \tau|v|$, i.e. the bit length of w is τ times of v. Here τ is a system parameter (e.g. $\tau = 10$ or 20).
  2. Compute $\bar{v} := h_k(v)$ where $h_k(\cdot)$ is a secure length-preserving keyed hash function. Note that in our application, the length of u is typically a few times of 256.
  3. Compute $y = w \oplus (\bar{v}\|\bar{v}\|\bar{v}\|\cdots)$.
  4. Compute $x = v \oplus H_k(y)$, where $H_k(\cdot)$ is a proper secure keyed hash function with fixed output length.

5. Output (x, y).

– $\mathsf{Merge}(k; x, y) \to u$
  1. Compute $v = x \oplus H_k(y)$.
  2. Compute $\bar{v} := h_k(v)$.
  3. Compute $w = y \oplus (\bar{v} \| \bar{v} \| \bar{v} \| \cdots)$.
  4. Output $v \| w$.

4.2 Our Novel Encrytion Scheme

Let $(\mathsf{KGen}, \mathsf{Split}, \mathsf{Merge})$ be as defined in previous subsection. Let $(\mathsf{KG}, \mathsf{E}, \mathsf{D})$ be a given encryption scheme (e.g. AES in a proper mode of operation). Our proposed encryption scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is defined as below

– $\mathsf{KeyGen}(1^\lambda) \leftarrow (k_0, k_1)$:
  1. Compute key $k_0 \leftarrow \mathsf{KG}(1^\lambda)$.
  2. Compute key $k_1 \leftarrow \mathsf{KGen}(1^\lambda)$.
  3. Output (k_0, k_1).

– $\mathsf{Enc}(k_0, k_1; M) \to (C_0, C_1)$
  1. Encrypt plaintext M to obtain $\bar{C} \leftarrow \mathsf{E}(k_0; M)$.
  2. Split $\bar{C}$ into two shares $(C_0, C_1) \leftarrow \mathsf{Split}(k_1; \bar{C})$.
  3. Output (C_0, C_1).

– $\mathsf{Dec}(k_0, k_1; C_0, C_1)$
  1. Merge C_0 and C_1 as $\bar{C} \leftarrow \mathsf{Merge}(k_1; C_0, C_1)$.
  2. Decrypt $\bar{C}$ as $M \leftarrow \mathsf{D}(k_0; \bar{C})$.
  3. Output M.

4.3 Security Analysis

It is easy to see that, under the standard setting of encryption scheme, if the adversary knows both C_0 and C_1, our proposed scheme is at least as secure as the underlying encryption scheme $(\mathsf{KG}, \mathsf{E}, \mathsf{D})$, which we can instantiate with any existing well-known encryption scheme (e.g. AES in practice, or some theoretical semantic secure ciphers).

Theorem 1 *Let* $(k_0, k_1) \leftarrow \mathsf{KeyGen}(1^\lambda)$ *and* $(C_0, C_1) \leftarrow \mathsf{Enc}(k_0, k_1; M)$. *Then we have*

$$\mathbf{H}(M|C_1, k_0, k_1) = |C_0| \tag{1}$$

$$\mathbf{H}(M|C_0, k_0, k_1) = |C_1|. \tag{2}$$

Proof. Recall the definition of function Split and Merge in Section 4.1. We have the property that

$$(x, y) = \mathsf{Split}(k_1; u) \iff u = \mathsf{Merge}(k_1; x, y), \tag{3}$$

where $x \in \{0,1\}^{\rho}$ and $y \in \{0,1\}^{\rho\tau}$, $u \in \{0,1\}^{\rho(\tau+1)}$.

So for a given value of k_0, k_1 and C_1, $M = \mathsf{Dec}(k_0, k_1; C_0, C_1) = \mathsf{D}(k_0; \mathsf{Merge}(k_1; C_0, C_1))$ is a injective (i.e. one-to-one) function of C_0. Therefore, Equality 1 holds. Equality 2 can be proved in a similar way. □

5 Experiment

5.1 Physical Unidirectional Network Link

Physical Unidirectional Network link [8] has been used to prevent sensitive information leakage from secure network to insecure network for a decade. It is also known as "Data Diode". "Air gap" [9] is another similar term. Commercial unidirectional network links are available on the market, e.g. Waterfall gateway and Fox DataDiode. But prices of those devices are very expensive. In theory, it is easy to construct a unidirectional network link using cheap consumer level fiber network communication device. As quoted from Wikipedia page [10],

> "*The most common form of a unidirectional network is a simple, modified, fiber-optic network link, with send and receive transceivers removed or disconnected for one direction, and any link failure protection mechanisms disabled. Commercial products rely on this basic design, but add other software functionality that provides applications with an interface which helps them pass data across the link.*"

However, some subtle issues have to be addressed before we could DIY a unidirectional network link successfully:

- In TCP/UDP protocol level, only UDP is applicable, because no returning route provided for TCP acknowledgement mechanism.
- In IP protocol level, automatic IP configuration service (e.g. DHCP) should be disable and IP addresses for each PC node should be configured manually.
- In MAC protocol level, the ARP protocol should be disabled and the mapping between IP address and MAC address should be manually inserted into the ARP table in each PC node.
- In each fiber device, link fault pass-through (LFP) feature should be disabled.
- Add a third fiber device and connect its outgoing port (Tx) with the incoming port (Rx) of the sender fiber device, where all incoming ports (e.g. Rx and Ethernet port) of the third fiber device remains empty. This third

[8] `https://en.wikipedia.org/wiki/Unidirectional_network`
[9] `https://en.wikipedia.org/wiki/Air_gap_(networking)`
[10] `https://en.wikipedia.org/wiki/Unidirectional_network`

dummy fiber device will send carrier signal to the sender fiber device, so that the sender fiber device can send out data as expected. We remark that, in our experiment, this step is essential, even if we have already disabled link fault pass-through feature.

Using the above method, we manage to construct a single unidirectional network link using 3 fiber transmitter devices at a cost less than 100 US dollars.

5.2 Our Experiment

We setup a testbed with 6 PC (Intel i7 CPU, SSD hard disk, multiple network interfaces in a PC) and 4 unidirectional network links, as in Figure 2. We set our Internet communication channel bandwidth as 60 times larger than the isolated network bandwidth. We generate random test files of size ranging from 1MB to 100MB, and achieve throughput about 7MBps (i.e. 56Mbps) with no errors. Our result shows that, with high quality hardware support, we could be able to achieve about 60 times expansion in bandwidth of secure (isolated) network at low cost (See details in Table 2 and Table 3).

Table 2. VIN experiment data. In this experiment, the size of larger share is 60 times larger than the smaller shares, which means our VIN nextwork bandwdith could be 61 larger than the isolated network bandwidth.

File Size (megabytes)	Transmission Speed (kilobyte per sec)
1	6898.923
10	7128.661
50	7178.287
100	7187.595

Table 3. Our VIN technique can effectively boost the bandwidth of secure isolated network. In the experiment, our VIN network only utilizes a small portion (45%) of isolated network bandwidth capacity to eventually constitute a hybrid network with about 7 megabyte per second throughput, where the security of this hybrid network is closer to the isolated network and could be much more secure than the Internet if the isolated network is properly isolated from outside.

Isolated Network Capacity	Small channel of VIN	Large channel of VIN	VIN
2 Mbps	0.9 Mbps	54 Mbps	54.9 Mbps

Note that the unit “Mbps” denotes megabit per second.

6 Conclusion

In this paper, we proposed a hybrid network, called as "Virtually Isolated Network". In this hybrid network, an isolated network and the Internet are connected using unidirectional network links in a way that the isolated network remains physically isolated. All data in this hybrid network will be encrypted and then split into two (possibly unequal) shares using secret-sharing approach. The smaller share will be delivered via the isolated network and the larger share will be delivered via the Internet. Due to the physical isolation property, any adversary cannot obtain both shares at the same time. Consequently, our method achieves unconditional security by hiding partial ciphertext from adversary.

References

1. Ben Othman, J., Mokdad, L.: Enhancing Data Security in Ad Hoc Networks Based on Multipath Routing. Journal of Parallel and Distributed Computing 70, 309–316 (2010)
2. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard (2002)
3. Ho, T., Medard, M., Koetter, R., Karger, D.R., Effros, M., Shi, J., Leong, B.: A random linear network coding approach to multicast. IEEE Transactions on Information Theory 52(10), 4413–4430 (Oct 2006)
4. Koetter, R., Médard, M.: An algebraic approach to network coding. IEEE/ACM Transactions on Networking 11(5), 782–795 (Oct 2003)
5. Krawczyk, H.: Secret Sharing Made Short. In: Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology. pp. 136–146. CRYPTO '93 (1994)
6. Li, S.Y., Yeung, R.W., Cai, N.: Linear network coding. IEEE Transactions on Information Theory 49(2), 371–381 (Feb 2003)
7. McEliece, R.J., Sarwate, D.V.: On Sharing Secrets and Reed-Solomon Codes. Commun. ACM 24(9), 583–584 (Sep 1981)
8. Rabin, M.O.: Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. Journal of the ACM 36(2), 335–348 (Apr 1989), http://doi.acm.org/10.1145/62044.62050
9. Resch, J.K., Plank, J.S.: AONT-RS: Blending Security and Performance in Dispersed Storage Systems. In: Proceedings of the 9th USENIX Conference on File and Stroage Technologies. pp. 14–14. FAST'11 (2011)
10. Shamir, A.: How to Share a Secret. Communications of the ACM 22(11), 612–613 (1979)
11. Zhang, S., Liew, S.C., Lam, P.P.: Hot topic: Physical-layer network coding. In: Proceedings of the 12th Annual International Conference on Mobile Computing and Networking. pp. 358–365. MobiCom '06 (2006)