

Detecting Byzantine Attacks Without Clean Reference

Ruohan Cao, Tan F. Wong, Tiejun Lv, Hui Gao and Shaoshi Yang

Abstract—We consider an amplify-and-forward relay network composed of a source, two relays, and a destination. In this network, the two relays are untrusted in the sense that they may perform Byzantine attacks by forwarding altered symbols to the destination. Note that every symbol received by the destination may be altered, and hence no clean reference observation is available to the destination. For this network, we identify a large family of Byzantine attacks that can be detected in the physical layer. We further investigate how the channel conditions impact the detection against this family of attacks. In particular, we prove that all Byzantine attacks in this family can be detected with asymptotically small miss detection and false alarm probabilities by using a sufficiently large number of channel observations *if and only if* the network satisfies a non-manipulability condition. No pre-shared secret or secret transmission is needed for the detection of these attacks, demonstrating the value of this physical-layer security technique for counteracting Byzantine attacks.

I. INTRODUCTION

In many communication networks, no direct physical link exists between source and destination nodes. As a result, the information that is to be delivered from a source to a destination has to be relayed by intermediate relay nodes. This gives the potentially malicious relay nodes the chances to perform Byzantine attacks by altering the information intended for the destination. Such attacks degrade the security of the network, and may diminish the potential benefits of relaying in practice [1], [2].

Under the risk of Byzantine attacks, one major challenge in achieving secure communications is to determine the existence of malicious relays. Conventionally, cryptographic keys or

Manuscript received February 1, 2016; revised June 21, 2016; Accepted July 8, 2016. The associate editor coordinating the review of the manuscript and approving it for publication was Prof. Lifeng Lai.

The financial support of the National Natural Science Foundation of China (NSFC) (Grant No. 61271188, 61401041 and 61501046), of the Project funded by China Postdoctoral Science Foundation, and of the National Science Foundation (NSF) under Grant CCF-1320086 is gratefully acknowledged.

Copyright (c) 2016 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

R. Cao is with the Institute of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications (BUPT), Beijing 100876, China (e-mail: caoruohan@bupt.edu.cn). She is also with the School of Information and Communication Engineering, BUPT.

T. F. Wong is with the Department of Electrical and Computer Engineering, University of Florida, FL 32611, U.S. (e-mail: twong@ufl.edu).

T. Lv and H. Gao are with the School of Information and Communication Engineering, BUPT, Beijing 100876, China (e-mail: {lvtiejun, huigao}@bupt.edu.cn).

S. Yang is with the School of Electronics and Computer Science, University of Southampton, SO17 1BJ Southampton, U.K. (e-mail: sy7g09@ecs.soton.ac.uk).

tracing symbols are often added to the information in or above the physical layer for making Byzantine attacks detectable. More specifically, in [3], [4], cryptographic keys are applied at the source to encrypt the data above the physical layer. Relying on the *a priori* shared knowledge of cryptographic keys, the destination performs attack detection by checking whether or not its received data obeys the constraints imposed by the cryptographic keys. In [5]–[8], tracing symbols are inserted into the transmitted signal in the physical layer. Using these tracing symbols, the intended destination is capable of determining whether an attack has occurred or not by comparing the known and observed tracing symbols. These cryptography-based and tracing-symbol-based schemes require the cryptographic information and tracing symbols, to which the relays are not privy, to be shared between the source and destination before the communication takes place.

It is also possible to detect Byzantine attacks without assuming any prior shared secret in certain network scenarios, where a “clean” reference is available for attack detection. For instance, in [9]–[11], special symbols are carefully generated and inserted into network-coded packets. By comparing the network-coded packets received from different relays, the destination can infer whether the relay network is malicious or not. However, the detection methods employed by [9]–[11] require at least one guaranteed “safe packet” be delivered to the destination so that this safe packet can serve as a clean reference to enable attack detection. This requirement is often satisfied by assuming that at least one relay or link is absolutely trustworthy. This assumption can be eliminated in a two-way relay (TWR) or one-way relay network by the schemes in [12]–[16]. Benefiting from the network topology of a TWR network, each source (destination) node can utilize its own transmitted symbols as the clean reference to carry out attack detection [12]–[15]. To further elaborate, in [12], each node’s own lattice-coded transmitted symbols are employed to simultaneously support secret transmission and construct an algebraic manipulation detection (AMD) code to detect Byzantine attacks in TWR networks with Gaussian channels. However, it is difficult to extend this scheme to non-Gaussian channels. In our previous work [13]–[15], we show that for TWR networks with discrete memoryless channels (DMCs), it is possible to detect potential Byzantine attacks without any AMD code or cryptographic keys. The basic idea is that each node utilizes its own transmitted symbols as a clean reference for statistically checking against the other node’s symbols forwarded by the relay. In [16], a two-hop, one-way relay network is considered. It is assumed that a safe direct link from the source to the destination exists. Since the direct

link is not attacked, observations made through the direct link can be utilized as the clean reference to check against attacks imposed by the possibly malicious relay.

In many relay networks, the clean reference assumed in [12]–[16] does not exist. Schemes have been proposed in [17]–[19] to detect Byzantine attacks without using any prior shared secret in some relay networks where no clean reference is available to the destination. These schemes assume that each malicious relay garbles its received symbols according to independent and identically distributed (i.i.d.) stochastic distributions. This model of i.i.d. attacks may not always be valid in practice, although it makes analysis simple. The Byzantine attack detection methods presented in [17]–[19] may no longer be provably unbreakable for non-i.i.d. attacks.

Against this background, we consider in this paper the Byzantine attack detection problem in a one-way, two-hop network consisting of a source node, two potentially malicious relay nodes and a destination node, where clean reference is unavailable. There are two independent transmission paths from the source node to the destination node, each via a relay node that may perform Byzantine attacks. For this network, we propose an attack detection approach employing only the physical-layer signals that the destination receives. No AMD codes or cryptographic keys are needed. Our treatment is considerably different from existing contributions [17]–[19] in that a more generalized attack model is considered. In particular, this model allows the two relays to conduct non-i.i.d. attacks. It is worth noting that considering non-i.i.d. attacks significantly complicates the analysis presented in this paper. Moreover, since all symbols observed by the destination node are prone to Byzantine attacks, no clean reference is available at the destination. Under these more general assumptions, the major contributions of this paper are summarized as follows:

- 1) We identify a large family of Byzantine attacks that physically correspond to the case in which the two relays do not collude in attack. For a Byzantine attack in this family, the attack can be sufficiently characterized by two stochastic matrices, each containing the empirical transition probabilities between a relay's input symbols and output symbols. This result is summarized in Proposition 1 of Section III.
- 2) We prove that under a non-manipulable channel condition, all Byzantine attacks in the aforementioned family are asymptotically detectable by simply comparing proper statistics generated from the destination's observations to known values of the statistics when there is no attack. This result is summarized in Theorem 1 of Section III.
- 3) Additionally, we also find a non-i.i.d. attack strategy, not belonging to the aforementioned family of Byzantine attacks, which is always capable of fooling the destination in this network with no clean reference. This result is summarized in Proposition 2 of Section III.

In short, we investigate in this paper both the feasibility and vulnerability of detecting Byzantine attacks in the physical layer of networks without clean references. The rest of this

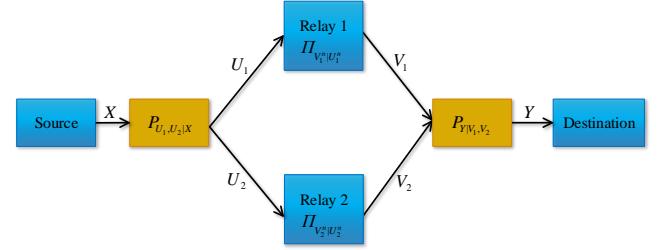


Fig. 1: A relay network with two unsafe links from the source to the destination.

paper is organized follows. In Section II, the problem to be addressed is formalized. In Section III, we provide our main results as described above. In Section IV, we discuss how to check for the above-mentioned non-manipulability condition numerically. Numerical simulation results are given in Section V, and finally the conclusions are drawn in Section VI. In Appendices A and B, we detail the proofs of the propositions and Theorem 1, respectively.

II. SYSTEM MODEL

A. Notation

Let \mathbf{a} be an $m \times 1$ column vector and A be an $m \times n$ matrix. For $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, n$, $[\mathbf{a}]_i$ denotes the i th element of \mathbf{a} , and $[A]_{i,j}$ denotes the (i, j) th entry of A . Whenever there is no ambiguity, we will employ the notation with no brackets for simplicity. The transpose of A is denoted by A^T . The Euclidean norm of \mathbf{a} is $\|\mathbf{a}\|_2$, and $\|A\|_2$ is the Frobenius norm of A . $|\mathbf{a}|$ and $|A|$ denote the L_1 -norm of \mathbf{a} and A , respectively. The Kronecker product of matrices A and B is represented by $A \otimes B$. The identity and zero matrices of any dimension are denoted by the generic symbols I and 0 , respectively.

For the random variables, we use upper-case script letters and serif-font letters to denote the corresponding discrete alphabets and elements in the alphabets, respectively. For instance, suppose that we denote a finite alphabet by $\mathcal{X} = \{x_1, x_2, \dots, x_{|\mathcal{X}|}\}$, where $|\mathcal{X}|$ is the cardinality of \mathcal{X} . Then X is a generic random variable over \mathcal{X} , and x is a generic element in \mathcal{X} . For a pair of random variables X and Y , we use $P_X(x)$ and $P_{X|Y}(x|y)$ to denote the marginal distribution of X and the conditional distribution of X given Y , respectively. Whenever needed, we will treat $P_{X|Y}$ as a stochastic matrix whose entries are specified by $P_{X|Y}(x|y)$ with x and y indexing the rows and columns, respectively. Similarly, P_X is also treated as an $1 \times |\mathcal{X}|$ vector whose entries are specified by $P_X(x)$ with x indexing the columns.

We employ x^n to denote a sequence of n symbols drawn from \mathcal{X} , and x_i to denote the i th symbol in x^n . We also employ X^n to denote a sequence of n random variables defined over \mathcal{X} , and X_i to denote the i th random variable in X^n . The counting function $N(x|x^n)$ records the number of occurrences of the element x in the sequence x^n . The indicator function $1_i(x|x^n)$ tells whether x_i is x . We may also use $1_i(x)$ instead of $1_i(x|x^n)$ for simplicity, whenever the meaning is clear from the context. It is clear that $N(x|x^n) = \sum_{i=1}^n 1_i(x|x^n)$.

We may trivially extend the aforementioned notations to a tuple of symbols drawn from the corresponding alphabets. The empirical distribution of the sequence x^n is denoted by $\Pi_{x^n}(x) \triangleq \frac{1}{n}N(x|x^n)$, while the empirical conditional distribution of x^n given y^n is $\Pi_{x^n|y^n}(x|y) \triangleq \frac{N(x,y|x^n,y^n)}{N(y|y^n)}$, provided that $N(y|y^n) > 0$. Similar to the notation of $P_{X|Y}$ and $P_{X|Y}(x|y)$, we also treat $\Pi_{x^n|y^n}$ as a stochastic matrix, whose entries are specified by $\Pi_{x^n|y^n}(x|y)$ with x and y indexing the rows and columns, respectively. Moreover, since X^n and Y^n denote random sequences, if the subscript of $\Pi_{x^n|y^n}$ is written in uppercase as $\Pi_{X^n|Y^n}$, then $\Pi_{X^n|Y^n}$ will be viewed as a random matrix denoting the empirical conditional distribution of X^n given Y^n .

Throughout this paper, Greek letters are exclusively used to represent constants and functions that have arbitrarily small yet positive value. In particular, $\varepsilon(\sigma) \rightarrow 0$ as $\sigma \rightarrow 0$. Unless otherwise stated, any convergence involving random variables should be interpreted as convergence in probability. For example, if $\{X^n\}$ and $\{Y^n\}$ are two sequences of random variables (matrices) over the same alphabet, $X^n \rightarrow Y^n$ means $|X^n - Y^n| \rightarrow 0$ (or $\|X^n - Y^n\|_2 \rightarrow 0$) in probability as n approaches infinity. For easy reference, the main quantities defined and employed in the rest of the paper are listed in Table I.

B. Channel Model

Consider the relay network shown in Fig. 1. The source sends symbols to the destination through two distinct paths. Along each path, the source symbols are forwarded by a potentially malicious relay to the destination. A malicious relay may forward symbols that are different from the ones received from the source. Our goal is to detect malicious actions of the two relays by observing the received symbols. The channels from the source to the relays, and from the relays to the destination are assumed to be memoryless with discrete inputs and outputs.

Let X be a discrete random variable, with probability mass function (PMF) P_X , that specifies a generic symbol transmitted by the source. During the period spanning the time instants $1, 2, \dots, n$, the source transmits X^n . We assume X^n is an i.i.d. sequence whose symbols are all independently drawn from \mathcal{X} according to P_X . For description convenience, the two relays are referred to as “relay 1” and “relay 2”. Correspondingly, their generic received symbols are denoted by U_1 and U_2 . Hence, the channel from the source to the relays is characterized by the conditional PMF $P_{U_1, U_2|X}$. We also write the joint PMF of (U_1, U_2) in the form of the $1 \times |\mathcal{U}_1||\mathcal{U}_2|$ vector P_{U_1, U_2} , whose elements are defined as:

$$[P_{U_1, U_2}]_j \triangleq P_{U_1, U_2}(u_{1,k}, u_{2,t}) \quad (1)$$

for $j = (k-1)|\mathcal{U}_2| + t$, where $k = 1, 2, \dots, |\mathcal{U}_1|$ and $t = 1, 2, \dots, |\mathcal{U}_2|$.

After the relays receive symbols from the source during time instants $1, 2, \dots, n$, the relays simultaneously forward the symbols, possibly manipulated, to the destination during the period covering the time instants $n+1, n+2, \dots, 2n$. More precisely, relay 1 sends the sequence V_1^n while relay

2 sends the sequence V_2^n . We may assume with no loss of generality that $\mathcal{V}_1 = \mathcal{U}_1$ and $\mathcal{V}_2 = \mathcal{U}_2$. Let us use Y to denote the generic symbol observed by the destination. The multiple-access channel from the two relays to the destination is characterized by the conditional PMF $P_{Y|V_1 V_2}$. Like before, we may interpret $P_{Y|V_1, V_2}$ as a $|\mathcal{Y}| \times |\mathcal{U}_1||\mathcal{U}_2|$ matrix, whose entries are defined as:

$$[P_{Y|V_1, V_2}]_{i,j} \triangleq P_{Y|V_1, V_2}(y_i | v_{1,k}, v_{2,t}), \quad (2)$$

for $j = (k-1)|\mathcal{U}_2| + t$, where $k = 1, 2, \dots, |\mathcal{U}_1|$ and $t = 1, 2, \dots, |\mathcal{U}_2|$. The PMF pair $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ will be referred to as *observation channel*. The knowledge of $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ is assumed to be available to the destination for facilitating maliciousness detection.

During the period spanning the time instants $n+1, n+2, \dots, 2n$, the destination observes the sequence Y^n . The destination needs to determine whether the relays have manipulated their received sequences or not by processing and analyzing Y^n . In particular, we will employ the empirical distribution Π_{Y^n} of Y^n to construct decision statistics for detecting potential malicious manipulations by the relays. Note that we may again write Π_{Y^n} as a $1 \times |\mathcal{Y}|$ vector, whose j th element is defined as

$$[\Pi_{Y^n}]_j \triangleq \frac{N(y_j | Y^n)}{n}, \quad (3)$$

for $j = 1, 2, \dots, |\mathcal{Y}|$.

C. Malicious Relays

For $m = 1, 2$, let U_m^n denote the sequence of n symbols observed by the m th relay during time instants $1, 2, \dots, n$, and V_m^n denote the sequence of n symbols transmitted by the relay during time instants $n+1, n+2, \dots, 2n$. Then the actions of the relays are specified by the mapping from (U_1^n, U_2^n, X^n) to (V_1^n, V_2^n) . We allow this mapping to be stochastic in general, described by the conditional PMF $P_{V_1^n, V_2^n | U_1^n, U_2^n, X^n}$, as long as it satisfies the following Markovity constraints:

$$\begin{aligned} P_{V_1^n | U_1^n, U_2^n, X^n}(v_1^n | u_1^n, u_2^n, x^n) &= P_{V_1^n | U_1^n}(v_1^n | u_1^n) \\ P_{V_2^n | U_1^n, U_2^n, X^n}(v_2^n | u_1^n, u_2^n, x^n) &= P_{V_2^n | U_2^n}(v_2^n | u_2^n). \end{aligned} \quad (4)$$

Physically these constraints impose the restriction that each relay can only formulate its attack (modification from U_m^n to V_m^n) based solely on the symbol sequence that it has received from the source.

We note that the knowledge of $(P_{V_1^n | U_1^n}, P_{V_2^n | U_2^n})$ is usually not available to the destination for attack detection. Thus we seek alternative non-parametric characterizations of the relay actions that do not require such knowledge. In particular, we will employ the empirical conditional PMFs (conditional types) $\Pi_{V_1^n, V_2^n | U_1^n, U_2^n}$, $\Pi_{V_1^n | U_1^n}$ and $\Pi_{V_2^n | U_2^n}$ to characterize the actions of relays 1 and 2. As before, for $m = 1, 2$, the conditional type $\Pi_{V_m^n | U_m^n}$ may be treated as a $|\mathcal{U}_m| \times |\mathcal{U}_m|$ matrix whose (i, j) th entry is defined by

$$[\Pi_{V_m^n | U_m^n}]_{i,j} \triangleq \frac{N(v_{m,i}, u_{m,j} | V_m^n, U_m^n)}{N(u_{m,j} | U_m^n)}. \quad (5)$$

TABLE I: Notation Table

X	Source symbol
U_m	Symbol received by relay m ($m = 1, 2$)
V_m	Symbol forwarded by relay m ($m = 1, 2$)
Y	Symbol observed by the destination
$\mathcal{X}, \mathcal{U}_m, \mathcal{V}_m, \mathcal{Y}$	Alphabets of X, U_m, V_m and Y , respectively
$P_{U_1, U_2 X}$	Conditional PMF of (U_1, U_2) given X
P_{U_1, U_2}	Joint PMF of (U_1, U_2)
$P_{Y V_1, V_2}$	Conditional PMF of Y given (V_1, V_2)
$(P_{U_1, U_2}, P_{Y V_1, V_2})$	Observation channel
U_m^n	Symbol sequence received by relay m ($m = 1, 2$)
V_m^n	Symbol sequence forwarded by relay m ($m = 1, 2$)
Y^n	Symbol sequence observed by the destination
$U_{m,i}, V_{m,i}$	The i th symbols in U_m^n and V_m^n , respectively
$\mathbf{u}_m, \mathbf{v}_m$	Generic elements in \mathcal{U}_m and \mathcal{V}_m , respectively
$1_i(\mathbf{u}_m U_m^n)$	Indicator of whether $U_{m,i} = \mathbf{u}_m$
$1_i(\mathbf{u}_1, \mathbf{u}_2 U_1^n, U_2^n)$	Indicator of whether $U_{1,i} = \mathbf{u}_1$ and $U_{2,i} = \mathbf{u}_2$
$1_i(\mathbf{u}_m, \mathbf{v}_m U_m^n, V_m^n)$	Indicator of whether $U_{m,i} = \mathbf{u}_m$ and $V_{m,i} = \mathbf{v}_m$
$N(\mathbf{u}_m U_m^n)$	$\sum_i^n 1_i(\mathbf{u}_m U_m^n)$
$N(\mathbf{u}_1, \mathbf{u}_2 U_1^n, U_2^n)$	$\sum_i^n 1_i(\mathbf{u}_1, \mathbf{u}_2 U_1^n, U_2^n)$
$N(\mathbf{u}_m, \mathbf{v}_m U_m^n, V_m^n)$	$\sum_i^n 1_i(\mathbf{u}_m, \mathbf{v}_m U_m^n, V_m^n)$
$\Pi_{V_1^n U_1^n}(\mathbf{v}_1 \mathbf{u}_1)$	$N(\mathbf{u}_1, \mathbf{v}_1 U_1^n, V_1^n)$
$\Pi_{V_2^n U_2^n}(\mathbf{v}_2 \mathbf{u}_2)$	$\frac{N(\mathbf{u}_1 U_1^n)}{N(\mathbf{u}_2 U_2^n)}$
$\Pi_{V_1^n, V_2^n U_1^n, U_2^n}(\mathbf{v}_1, \mathbf{v}_2 \mathbf{u}_1, \mathbf{u}_2)$	$\frac{N(\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}_1, \mathbf{v}_2 U_1^n, U_2^n)}{N(\mathbf{u}_1, \mathbf{u}_2 U_1^n, U_2^n)}$
$\mathbf{x}_i, \mathbf{u}_{m,i}, \mathbf{v}_{m,i}, \mathbf{y}_i$	The i th elements in alphabets $\mathcal{X}, \mathcal{U}_m, \mathcal{V}_m$, and \mathcal{Y} , respectively
$\left[\Pi_{V_m^n U_m^n} \right]_{i,j}$	$\Pi_{V_m^n U_m^n}(\mathbf{v}_{m,i} \mathbf{u}_{m,j})$
$\left[\Pi_{V_1^n, V_2^n U_1^n, U_2^n} \right]_{i,j}$	$\Pi_{V_1^n, V_2^n U_1^n, U_2^n}(\mathbf{v}_{1,t_1}, \mathbf{v}_{2,t_2} \mathbf{u}_{1,k_1}, \mathbf{u}_{2,k_2}), j = (k_1 - 1) \mathcal{U}_2 + k_2, i = (t_1 - 1) \mathcal{U}_2 + t_2$
$[P_{U_1, U_2}]_j$	$\Pr\{U_1 = \mathbf{u}_{1,k}, U_2 = \mathbf{u}_{2,t}\}, j = (k - 1) \mathcal{U}_2 + t$
$[P_{Y V_1, V_2}]_{i,j}$	$\Pr\{Y = \mathbf{y}_i V_1 = \mathbf{v}_{1,k}, V_2 = \mathbf{v}_{2,t}\}, j = (k - 1) \mathcal{U}_2 + t$
$D(Y^n)$	Decision statistic as a function of Y^n
I	Identity matrix with any dimension
\otimes	Kronecker operator

Similarly, we also treat $\Pi_{V_1^n, V_2^n | U_1^n, U_2^n}$ as a $|\mathcal{U}_1| |\mathcal{U}_2| \times |\mathcal{U}_1| |\mathcal{U}_2|$ matrix whose (i, j) th entry is defined by

$$\left[\Pi_{V_1^n, V_2^n | U_1^n, U_2^n} \right]_{i,j} = \frac{N(\mathbf{u}_{1,k_1}, \mathbf{u}_{2,k_2}, \mathbf{v}_{1,t_1}, \mathbf{v}_{2,t_2} | U_1^n, U_2^n, V_1^n, V_2^n)}{N(\mathbf{u}_{1,k_1}, \mathbf{u}_{2,k_2} | U_1^n, U_2^n)}, \quad (6)$$

for $i = (t_1 - 1) |\mathcal{U}_2| + t_2$ and $j = (k_1 - 1) |\mathcal{U}_2| + k_2$, where $k_1, t_1 = 1, 2, \dots, |\mathcal{U}_1|$ and $k_2, t_2 = 1, 2, \dots, |\mathcal{U}_2|$. We will restrict ourselves to consider the family of relay actions that satisfy the following constraint:

$$\Pi_{V_1^n, V_2^n | U_1^n, U_2^n}(\mathbf{v}_1, \mathbf{v}_2 | \mathbf{u}_1, \mathbf{u}_2) \rightarrow \Pi_{V_1^n | U_1^n}(\mathbf{v}_1 | \mathbf{u}_1) \Pi_{V_2^n | U_2^n}(\mathbf{v}_2 | \mathbf{u}_2), \quad (7)$$

for all $(\mathbf{u}_1, \mathbf{v}_1) \in \mathcal{U}_1^2$ and $(\mathbf{u}_2, \mathbf{v}_2) \in \mathcal{U}_2^2$. This constraint can be interpreted as the relays cannot decide their own actions by colluding with each other, either beforehand or during the transmission process.

We will see from Theorem 1 of Section III that for the purpose of attack detection, the conditional types $\Pi_{V_1^n | U_1^n}$ and $\Pi_{V_2^n | U_2^n}$ are sufficient for characterizing the maliciousness of any non-colluding relay actions that satisfy (7). In addition, it is clear that $\Pi_{V_1^n | U_1^n}$ and $\Pi_{V_2^n | U_2^n}$ describe the maliciousness of individual actions of relays 1 and 2, respectively. When $\Pi_{V_m^n | U_m^n} = I$ (i.e., $V_m^n = U_m^n$), relay m is intuitively non-malicious in the sense that it faithfully forwards its received sequence to the destination. This motivates us to adopt the following more formal definition of maliciousness of the relays based on $\Pi_{V_1^n | U_1^n}$ and $\Pi_{V_2^n | U_2^n}$:

Definition 1. (Non-malicious relay) For $m = 1, 2$, relay m is said to be non-malicious if $\Pi_{V_m^n | U_m^n} \rightarrow I$ as n approaches infinity. Otherwise, relay m is considered to be malicious. In addition, the relay network is considered to be safe if both relays are non-malicious, i.e., $\Pi_{V_1^n | U_1^n} \rightarrow I$ and $\Pi_{V_2^n | U_2^n} \rightarrow I$.

Note that the above definition of non-maliciousness of relay m is more relaxed than the strict requirement of $\Pi_{V_m^n | U_m^n} = I$, since it allows relay m to alter a negligible portion of its received symbols. Although we adopt this relaxation for mathematical convenience, it has minimal practical implications, because the negligible altered symbols can be corrected by using channel coding/decoding in practice.

For the family of relay actions that satisfy (7), we will show in Lemma 2 that

$$P_{U_1, U_2}(\Pi_{V_1^n | U_1^n}^T \otimes \Pi_{V_2^n | U_2^n}^T) P_{Y | V_1, V_2}^T \rightarrow \Pi_{Y^n} \quad \text{as } n \rightarrow \infty. \quad (8)$$

Since the destination is capable of calculating Π_{Y^n} directly from its observation Y^n , the above convergence allows the destination to estimate $\Pi_{V_1^n | U_1^n}$ and $\Pi_{V_2^n | U_2^n}$ from Y^n obtained in the physical layer. Then, the attack detection can be achieved by comparing the estimate of $(\Pi_{V_1^n | U_1^n}, \Pi_{V_2^n | U_2^n})$ to (I, I) . The particular detection method and its performance analysis will be detailed in Appendix B. Furthermore, it is clear from the convergence characterized by (8) that the observation channel $(P_{U_1, U_2}, P_{Y | V_1, V_2})$ is essential for determining the detectability of the attacks. We will investigate in more

depth how $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ affects the detection of such attacks in Section III.

Note that the restriction imposed by (7) excludes some possible attacks. Nevertheless, Proposition 1 in Section III shows that the family of possible attacks that satisfy (7) is in fact rather large. In particular, it allows one relay to conduct *any* deterministic or random attack, provided that the other relay can only conduct certain stationary attacks, e.g., i.i.d. attacks. Compared with the existing schemes which restrict both relays to make i.i.d. attacks, our results in Section III extend the family of attacks that can be detected at the destination based only on its observations.

III. MAIN RESULTS

From (8), we see that the observation channel $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ plays a critical role in determining whether an attack from the family satisfying (7) can be detected by the destination solely using its own observation Y^n . Specifically, this detectability is determined by the number of stochastic matrix pairs (Υ_1, Υ_2) , which are solutions to the matrix equation:

$$P_{U_1, U_2} P_{Y|V_1, V_2}^T = P_{U_1, U_2} (\Upsilon_1 \otimes \Upsilon_2) P_{Y|V_1, V_2}^T, \quad (9)$$

where Υ_1 and Υ_2 are of dimensions $|\mathcal{U}_1| \times |\mathcal{U}_1|$ and $|\mathcal{U}_2| \times |\mathcal{U}_2|$, respectively. Recall from Definition 1 that relay m is non-malicious if $\Pi_{V_m^n|U_m^n} \rightarrow I$ for $m = 1, 2$. Thus, it is intuitive that if the observation channel $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ constitutes such a pair of distributions that make (I, I) the unique solution to (9), then comparing Π_{Y^n} with $P_{U_1, U_2} P_{Y|V_1, V_2}^T$ can tell us whether malicious attacks have been carried out by the relays. On the other hand, if (9) has multiple solutions, then there exist attacks that cannot be detected by simply comparing Π_{Y^n} with $P_{U_1, U_2} P_{Y|V_1, V_2}^T$. This intuitive argument leads to the dichotomy of all observation channels into the following two classes:

Definition 2. (Non-manipulable observation channel) The observation channel $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ is said to be non-manipulable if (I, I) is the unique stochastic matrix pair that solves (9). Otherwise, the observation channel is said to be manipulable.

With this dichotomy of observation channels, we can now present the main results of this paper, which formally establish the detectability of malicious attacks from the family that satisfies (7) at the destination:

Theorem 1. (Maliciousness detectability) For all malicious actions that satisfy (7), the observation channel $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ is non-manipulable constitutes the necessary and sufficient condition for the existence of a decision statistic $D(Y^n)$ which simultaneously has the following two properties:

For any fixed sufficiently small $\delta > 0$ and $\epsilon > 0$, and for all sufficiently large n , we have

$$1) \Pr \left\{ D(Y^n) > \delta \mid \sum_{m=1}^2 \|\Pi_{V_m^n|U_m^n} - I\|_2 > \delta \right\} \geq 1 - \epsilon, \text{ whenever } \Pr \left\{ \sum_{m=1}^2 \|\Pi_{V_m^n|U_m^n} - I\|_2 > \delta \right\} > 0,$$

$$2) \Pr \left\{ D(Y^n) > \varepsilon(\delta) \mid \sum_{m=1}^2 \|\Pi_{V_m^n|U_m^n} - I\|_2 \leq \delta \right\} \leq \epsilon, \text{ whenever } \Pr \left\{ \sum_{m=1}^2 \|\Pi_{V_m^n|U_m^n} - I\|_2 \leq \delta \right\} > 0, \text{ where } \varepsilon(\delta) \rightarrow 0 \text{ as } \delta \rightarrow 0.$$

Note that for a non-manipulable observation channel, properties 1) and 2) of Theorem 1 together imply that $D(Y^n) \rightarrow 0$ if and only if the relay network is safe (see Definition 1). This means that the destination may detect an attack by simply comparing the decision statistic $D(Y^n)$ to the threshold 0. Then property 1 guarantees a small miss detection probability when an attack has occurred, while property 2 guarantees a small false alarm probability when no attack has been carried out by the relays. On the other hand, no such decision statistic exists for a manipulable observation channel, and thus over this type of channels malicious attacks imposed by the relays cannot be accurately detected based only on Y^n at the destination.

We see that Theorem 1 provides a definite answer to the detectability of attacks in the family (7). Its usefulness and contribution depend on whether the family (7) contains many common attacks beyond i.i.d attacks, whose detectability has been previously investigated. To this end, the following proposition shows that (7) does include a very large class of attacks including many common non-i.i.d. attacks.

Proposition 1. Let $(V_1^n, V_2^n, U_1^n, U_2^n)$ be jointly distributed according to

$$P_{V_1^n, V_2^n, U_1^n, U_2^n}(v_1^n, v_2^n, u_1^n, u_2^n) = P_{V_1^n|U_1^n}(v_1^n|u_1^n) P_{V_2^n|U_2^n}(v_2^n|u_2^n) \prod_{i=1}^n P_{U_1^n, U_2^n}(u_{1,i}, u_{2,i}). \quad (10)$$

Suppose that there exists a constant $c_{v_2|u_2}$ satisfying $E\{1_{i(v_2|V_2^n)}|U_2^n = u_2^n\} = c_{v_2|u_2}$ for all i such that $u_{2,i} = u_2$. Then, $\Pr\{\Pi_{V_1^n|U_1^n}(v_1|u_1) > 0\} \rightarrow 1$ and $P_{U_1, U_2}(u_1, u_2) > 0$ imply

$$I_{V_1^n, V_2^n|U_1^n, U_2^n}(v_1, v_2|u_1, u_2) \rightarrow \Pi_{V_1^n|U_1^n}(v_1|u_1) \Pi_{V_2^n|U_2^n}(v_2|u_2).$$

Note that Proposition 1 only restricts one relay's (relay 2) malicious action, and the other relay's (relay 1) attack can be arbitrary without any restriction. The condition $E\{1_{i(v_2|V_2^n)}|U_2^n = u_2^n\} = c_{v_2|u_2}$ for relay 2 is a first-order stationarity requirement on the attack mapping from U_2^n to V_2^n . It is easy to check that this condition is satisfied by i.i.d. attacks as well as any attack that can be modeled by a Markov chain with a unique stationary distribution.

The example illustrated by Fig. 2 describes an attack scenario that can be modeled by a stationary Markov chain, and hence by Proposition 1 satisfying (7). More specifically, in Fig. 2 a jammer inserts malicious sequence J^n into the data flowing to relay 2. We assume that the symbols of J^n , V_2^n and U_2^n take values from the same finite field \mathbb{F}_q . The i th output symbol of relay 2 is given by $V_{2,i} = (J_i + U_{2,i})_q$, where $(\cdot)_q$ is the modulo value of its argument with base q , and q is a prime number. This assumption approximately models the case that the symbols of J^n and U_2^n superimpose before they arrive at relay 2, which simply forwards its received symbols to the destination. We assume that the jammer sequence J^n is

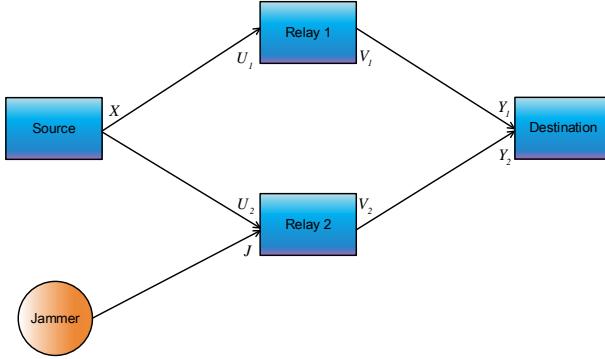


Fig. 2: A relay network with a jammer, which transmits J^n obeying a stationary Markov stochastic process.

a stationary Markov sequence satisfying $P_{J_i} = P_{J_i} P_{J_{i+1}|J_i}$, $i = 1, \dots, n$, where P_{J_i} is the distribution of J_i , and $P_{J_{i+1}|J_i}$ specifies the transfer probability from J_i to J_{i+1} . In addition, J^n is also independent of all other random variables. Note that the action of relay 1 specified by the mapping from U_1^n to V_1^n is arbitrary. It is easy to check that for all i such that $u_{2,i} = u_2$, $E\{1_i(v_2|V_2^n)|U_2^n = u_2^n\} = P_{J_i}((v_2 - u_2)_q)$. Therefore, Proposition 1 applies, showing that this attack scenario is within the family (7). Theorem 1 is thus applicable to this attack scenario as well.

In summary, Theorem 1 and Proposition 1 together show that non-manipulability of the observation channel $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ is necessary and sufficient for the detectability of a very large family of attacks by solely using the sequence received at the destination. This family of attacks is specified by (7) and includes attacks in which the action of one relay can be modeled by a first-order stationary mapping, while the action of the other relay can be completely arbitrary. This contribution distinguishes our work from the existing literature that either focuses on i.i.d. attacks conducted by both relays, or imposes the requirement of utilizing reliable observations.

We note that while the family (7) contains a very large class of attacks that can be detected at the destination by Theorem 1, Proposition 2 below shows that there are attacks that cannot be detected based on observing only Y^n .

Proposition 2. *Let $(V_1^n, V_2^n, U_1^n, U_2^n)$ be distributed according to (10). Consider the attack in which the two relays permute their received symbols according to the same predetermined order. This means that V_1^n and V_2^n are respective rearrangements of U_1^n and U_2^n , and for any $k, t = 1, \dots, n$, if $V_{1,k} = U_{1,t}$ and $V_{1,t} = U_{1,k}$, we must have $V_{2,k} = U_{2,t}$ and $V_{2,t} = U_{2,k}$. For this attack, there does not exist any decision statistic $D(Y^n)$ that satisfies the two properties given in Theorem 1.*

Note that the permutation attack described in Proposition 2 does not belong to the family (7). Intuitively, the two relays collude in agreeing to permute their respective received symbols in the same order. We see that the lack of a clean reference at the destination prevents it from detecting this kind of attacks in which the two relays collude.

To summarize, we have briefly discussed some practical implications of the theoretical detectability results provided by Theorem 1, Proposition 1 and Proposition 2. These results show that it is possible to perform Byzantine attack detection when no clean reference is available at the destination for a large family of non-colluding attacks. The lack of a clean reference is rather commonplace in many peer-to-peer or ad hoc networks, where we may not be able to guarantee the trustworthiness of all relay nodes. The Byzantine attack detectability results in Theorem 1 and Proposition 1 suggest us to form the network in a more judicious manner so that it is less likely to select relay nodes that may collude in attack. By doing so, malicious attacks by the relay nodes can be detected. Moreover, since the proposed Byzantine attack detection techniques do not require any cryptographic aid, the usual overheads incurred in the implementation of cryptographic systems, such as key management and distribution, can be avoided.

IV. CHECKING THE NON-MANIPULABILITY CONDITION

As shown in Theorem 1, the detectability of attacks in the family (7) is determined by whether the condition of non-manipulability holds for the observation channel $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ or not. Recall that $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ is non-manipulable if (I, I) is the unique stochastic solution to (9). This condition is sometimes difficult to check. In this section, we discuss a numerically efficient method to check the non-manipulability condition. The main idea is to transform the task of checking the condition of non-manipulability into an optimization problem that can be solved by standard methods. To this end, we first rewrite the solution of (9) as that of an optimization problem (see (11) below). The non-manipulability condition is equivalent to the solution to the optimization problem taking an extremal value in the possible range. This optimization problem is non-convex as its feasible set is non-convex. In order to find numerically efficient methods to solve this optimization problem, we further relax the feasible set to a convex set, which results a convex optimization problem (see (16) below) that can be solved efficiently.

More specifically, we first consider the optimization below:

$$\min_{\Upsilon_1, \Upsilon_2} \sum_{k=1}^{|\mathcal{U}_1|} [\Upsilon_1]_{k,k} + \sum_{k=2}^{|\mathcal{U}_2|} [\Upsilon_2]_{k,k} \quad (11a)$$

$$s.t. P_{U_1, U_2}(\Upsilon_1^T \otimes \Upsilon_2^T) P_{Y|V_1, V_2}^T = P_{U_1, U_2} P_{Y|V_1, V_2}^T, \quad (11b)$$

$$0 \leq [\Upsilon_1]_{i,j} \leq 1, \quad 1 \leq i \leq |\mathcal{U}_1|, 1 \leq j \leq |\mathcal{U}_1|, \quad (11c)$$

$$0 \leq [\Upsilon_2]_{i,j} \leq 1, \quad 1 \leq i \leq |\mathcal{U}_2|, 1 \leq j \leq |\mathcal{U}_2|, \quad (11d)$$

$$\sum_{i=1}^{|\mathcal{U}_1|} [\Upsilon_1]_{i,j} = 1, \quad j = 1, 2, \dots, |\mathcal{U}_1|, \quad (11e)$$

$$\sum_{i=1}^{|\mathcal{U}_2|} [\Upsilon_2]_{i,j} = 1, \quad j = 1, 2, \dots, |\mathcal{U}_2|. \quad (11f)$$

It is clear that the minimum value of the problem (11) lies inside the interval $[0, |\mathcal{U}_1| + |\mathcal{U}_2|]$. Moreover, under the

constraints (11b)–(11f), the value of the objective function in (11) can be equal to $|\mathcal{U}_1| + |\mathcal{U}_2|$ if and only if $\Upsilon_1 = I$ and $\Upsilon_2 = I$. For any other choice of (Υ_1, Υ_2) , the value of the objective function in (11) is strictly smaller than $|\mathcal{U}_1| + |\mathcal{U}_2|$. From this observation, we can conclude that $(\Upsilon_1, \Upsilon_2) = (I, I)$ is the unique solution to (9), and hence $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ is non-manipulable, if and only if the minimum value of the problem (11) is $|\mathcal{U}_1| + |\mathcal{U}_2|$. Thus we may determine whether the observation channel is non-manipulable by solving the optimization problem (11) and checking whether the minimum value attained is $|\mathcal{U}_1| + |\mathcal{U}_2|$. Because the constraint (11b) is not convex, the optimization problem (11) is non-convex. Hence, it is challenging to solve the problem in a computationally efficient manner.

To check the non-manipulability condition efficiently, we relax the feasible set specified by (11b)–(11f) into a convex set in order to obtain convexity. Note that the non-convexity of (11) is caused by the Kronecker product appearing in (11b). In order to get a convex feasible set, we replace $\Upsilon_1 \otimes \Upsilon_2$ with a $|\mathcal{U}_1| |\mathcal{U}_2| \times |\mathcal{U}_1| |\mathcal{U}_2|$ matrix Υ in (11b). Then from the constraint that Υ_1 and Υ_2 are stochastic matrices, W must satisfy the following linear constraints:

$$\sum_{i=1}^{|\mathcal{U}_1| |\mathcal{U}_2|} [\Upsilon]_{i,j} = 1, \quad j = 1, 2, \dots, |\mathcal{U}_1| |\mathcal{U}_2|, \quad (12)$$

$$\sum_{i=1}^{|\mathcal{U}_1|} [\Upsilon_1]_{i,j} = 1, \quad j = 1, 2, \dots, |\mathcal{U}_1|, \quad (13)$$

$$\begin{aligned} \sum_{i=(t-1)|\mathcal{U}_2|+1}^{t|\mathcal{U}_2|} [\Upsilon]_{i,(k-1)|\mathcal{U}_2|+1} &= \sum_{i=(t-1)|\mathcal{U}_2|+1}^{t|\mathcal{U}_2|} [\Upsilon]_{i,(k-1)|\mathcal{U}_2|+2} \\ &= \dots = \sum_{i=(t-1)|\mathcal{U}_2|+1}^{t|\mathcal{U}_2|} [\Upsilon]_{i,k|\mathcal{U}_2|} = [\Upsilon_1]_{t,k}, \quad t, k = 1, 2, \dots, |\mathcal{U}_1|, \end{aligned} \quad (14)$$

$$\begin{aligned} \sum_{i=0}^{|\mathcal{U}_1|-1} [\Upsilon]_{i|\mathcal{U}_2|+t,k} &= \sum_{i=0}^{|\mathcal{U}_1|-1} [\Upsilon]_{i|\mathcal{U}_2|+t,k+|\mathcal{U}_2|} \\ &= \dots = \sum_{i=0}^{|\mathcal{U}_1|-1} [\Upsilon]_{i|\mathcal{U}_2|+t,k+(|\mathcal{U}_1|-1)|\mathcal{U}_2|} = [\Upsilon_2]_{t,k}, \\ &\quad t, k = 1, 2, \dots, |\mathcal{U}_2|. \end{aligned} \quad (15)$$

Adding these four linear constraints back, the feasible set specified by (11b)–(11f) can be relaxed, and correspondingly we obtain the following linear optimization problem which is a relaxation of (11):

$$\min_{\Upsilon_1, \Upsilon_2} \sum_{k=1}^{|\mathcal{U}_1|} [\Upsilon_1]_{k,k} + \sum_{k=2}^{|\mathcal{U}_2|} [\Upsilon_2]_{k,k} \quad (16a)$$

$$\text{s.t. } P_{U_1, U_2} \Upsilon^T P_{Y|V_1, V_2}^T = P_{U_1, U_2} P_{Y|V_1, V_2}^T, \quad (16b)$$

$$0 \leq [\Upsilon_1]_{i,j} \leq 1, \quad 1 \leq i \leq |\mathcal{U}_1|, 1 \leq j \leq |\mathcal{U}_1|, \quad (16c)$$

$$0 \leq [\Upsilon_2]_{i,j} \leq 1, \quad 1 \leq i \leq |\mathcal{U}_2|, 1 \leq j \leq |\mathcal{U}_2|, \quad (16d)$$

$$(12), (13), (14), \text{ and } (15). \quad (16e)$$

We note that this linear program can be solved efficiently using standard linear programming techniques. Comparing the optimization problems (11) and (16), it is clear that both have the same objective function. Furthermore, since the feasible set of (11) is a subset of that of (16), the minimum value of

(16) must be no greater than the minimum value of (11). As a result, if the minimum value of (16) is $|\mathcal{U}_1| + |\mathcal{U}_2|$, then the minimum value of (11) must also be $|\mathcal{U}_1| + |\mathcal{U}_2|$, and hence the observation channel $(P_{U_1, U_2}, P_{Y|V_1, V_2})$ is non-manipulable. Although the converse is not true for the linear program (16), we may still use it to check for non-manipulability of the observation channel first before opting to solve the non-convex problem (11).

V. NUMERICAL EXAMPLES

We give three numerical examples in this section to illustrate the detectability results of Theorem 1, Propositions 1 and 2. In all the examples, we assume that the source alphabet is binary (i.e., $|\mathcal{X}| = 2$) and all the other alphabets are ternary (i.e., $|\mathcal{U}_1| = |\mathcal{U}_2| = |\mathcal{V}_1| = |\mathcal{V}_2| = 3$). For simplicity, we also assume $P_{Y|V_1, V_2} = I$ and $P_{U_1, U_2|X} = P_{U_1|X} \otimes P_{U_2|X}$. In addition, we note that the decision statistic used in the proof of Theorem 1 (see Appendix B-A) is too complicated for practical implementation. Therefore, we employ the simple heuristic decision statistic

$$D(Y^n) = \left\| \Pi_{Y^n} - P_{U_1, U_2} P_{Y|V_1, V_2}^T \right\|_2 \quad (17)$$

for Byzantine attack detection in the examples.

A. A Non-manipulable Observation Channel Example for Demonstrating the Sufficiency in Theorem 1

We first choose the source symbol distribution $P_X = [.4999 .5001]$. Then, we consider a relay network in which the channels from the source to the two relays are specified by the PMF matrices $P_{U_1|X} = P_{U_2|X} = \begin{bmatrix} .9 & 0 \\ .1 & .1 \\ 0 & .9 \end{bmatrix}$, while the channels from the two relays to the destination are assumed to be perfect, i.e., $P_{Y|V_1, V_2} = I$. By solving the linear program (16), it is easy to check that the observation channel (P_{U_1, U_2}, I) in this example is non-manipulable.

Two different attacks are considered. In the first attack, referred to as Attack 1, relay 2 performs an i.i.d. attack by randomly and independently switching its received symbols according to the conditional distribution specified by $P_{V_2|U_2} = \begin{bmatrix} .995 & .0025 & .0025 \\ .0025 & .995 & .0025 \\ .0025 & .0025 & .995 \end{bmatrix}$, while relay 1 conducts a non-i.i.d. attack by randomly and independently switching its i th input symbol $U_{1,i}$ according to the conditional distribution $P_{V_1|U_1} = \begin{bmatrix} .995 & .0025 & .0025 \\ .0025 & .995 & .0025 \\ .0025 & .0025 & .995 \end{bmatrix}$ when i is odd, and $\tilde{P}_{V_1|U_1} = \begin{bmatrix} .95 & .025 & 0 \\ .05 & .95 & .05 \\ 0 & .025 & .95 \end{bmatrix}$ when i is even.

Since relay 2 performs an i.i.d. attack, Attack 1 is in the family (7) according to Proposition 1. By Theorem 1, Attack 1 can be detected in the non-manipulable observation channel (P_{U_1, U_2}, I) .

In the second attack considered, referred to as Attack 2, relay 1 switches its input in the same manner as it does in

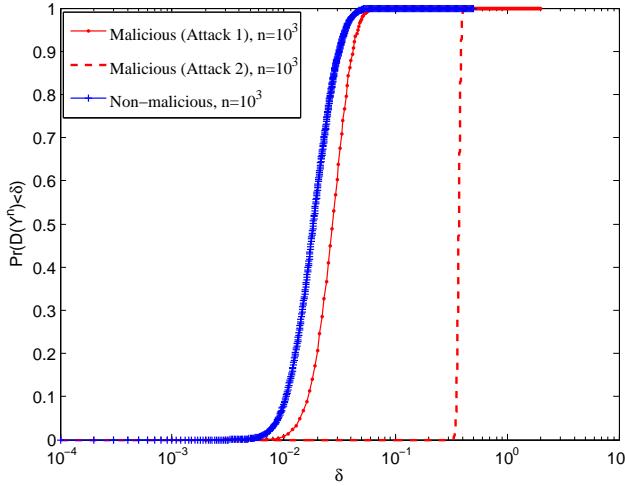


Fig. 3: Empirical CDFs of $D(Y^n)$, i.e., $\Pr(D(Y^n) \leq \delta)$, in the non-manipulable observation channel example considered in Section V-A. For $n = 10^3$, three different cases are compared, namely, the “non-malicious” case as well as the malicious cases of Attack 1 and Attack 2.

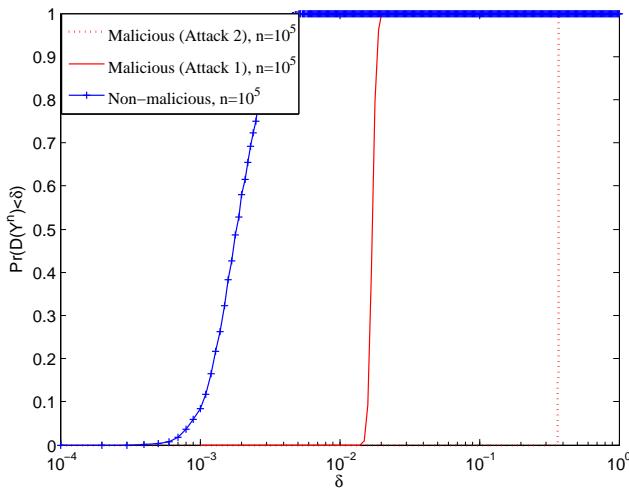


Fig. 4: Empirical CDFs of $D(Y^n)$, i.e., $\Pr(D(Y^n) \leq \delta)$, in the non-manipulable observation channel example considered in Section V-A. For $n = 10^5$, three different cases are compared, namely, the “non-malicious” case as well as the malicious cases of Attack 1 and Attack 2.

Attack 1. Meanwhile, relay 2 conducts the stationary Markov attack as illustrated in Fig. 2, with $P_{J_1} = \begin{bmatrix} \frac{6}{25} & \frac{2}{5} & \frac{9}{25} \end{bmatrix}$ and $P_{J_{i+1}|J_i} = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{6} & \frac{1}{3} & \frac{1}{2} \end{bmatrix}$, $i = 1, 2, \dots, n$. As explained before (see the description of Fig. 2 in Section III), Proposition 1 gives that Attack 2 belongs to the family (7). Thus by Theorem 1, Attack 2 can also be detected in the non-manipulable observation channel.

We conduct computer simulations to illustrate the detectability of both attacks using the heuristic decision statistic $D(Y^n)$ in (17). The empirical cumulative distribution functions (CDFs) of $D(Y^n)$ obtained from the simulation are

plotted in Figs. 3 and 4 for the cases of $n = 10^3$ and $n = 10^5$, respectively. From Fig. 4, it is observed that there are clear separations between the empirical CDFs of $D(Y^n)$ for the non-malicious case and the malicious cases of Attack 1 and Attack 2 when $n = 10^5$. For instance, as seen in Fig. 4, using the decision threshold $\delta = 0.01$ for $D(Y^n)$, one may differentiate between the non-malicious (both relays faithfully forward their respective received sequences to the destination) and malicious cases with negligible miss detection and false alarm probabilities. This observation verifies sufficiency of non-manipulability for the detectability of Byzantine attacks in the family (7) promised by Theorem 1.

B. A Manipulable Observation Channel Example for Demonstrating the Necessity in Theorem 1

We again consider the same relay network used in the previous example, except that the source symbol distribution is now $P_X = \begin{bmatrix} .5 & .5 \end{bmatrix}$ and hence giving $P_{U_1, U_2} = \begin{bmatrix} .125 & .125 & 0 \\ .125 & .25 & .125 \\ 0 & .125 & .125 \end{bmatrix}$. It is straightforward to check that the

choice of $\Upsilon_1 = \Upsilon_2 = \begin{bmatrix} -1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & -1 \end{bmatrix}$ makes this observation channel (P_{U_1, U_2}, I) manipulable. Therefore, according to Theorem 1, we know that the attacks in the family (7) are not detectable in this network. In order to verify this, a simulation is carried out for an i.i.d. attack, referred to as Attack 3, where each relay randomly and independently switches its input symbols according to the conditional distributions

$P_{V_1|U_1} = P_{V_2|U_2} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$. Attack 3 corresponds to the scenario where each relay flips the first and third symbols in their alphabet. The empirical CDFs of $D(Y^n)$ for the “non-malicious” case and this malicious case obtained from the simulation are plotted in Fig. 5. It is clearly seen from Fig. 5 that the CDFs are indistinguishable, regardless of the value of n . As a result, from $D(Y^n)$, we cannot differentiate between the non-malicious and malicious cases. This observation indicates that the two properties of Theorem 1 cannot be simultaneously satisfied in this manipulable observation channel.

C. An Example for Demonstrating Proposition 2

In order to verify the assertion of Proposition 2, we consider the permutation attack in which each relay permutes the symbols in its input sequences according to $v_{m,i} = u_{m,(i+\frac{n}{2})_n}$, where $m = 1, 2$, and $(\cdot)_n$ is the modulo value of its argument with base n . Simulations are conducted for the permutation attack in both the non-manipulable observation channel and the manipulable observation channel considered previously in Sections V-A and V-B, respectively. The empirical CDFs of $D(Y^n)$ for the non-malicious case and the malicious case of the permutation attack obtained from the simulations are plotted in Fig. 6 and Fig. 7 for the non-manipulable and manipulable observation channels, respectively. We can clearly see from Figs. 6 and 7 that the CDFs for the malicious and

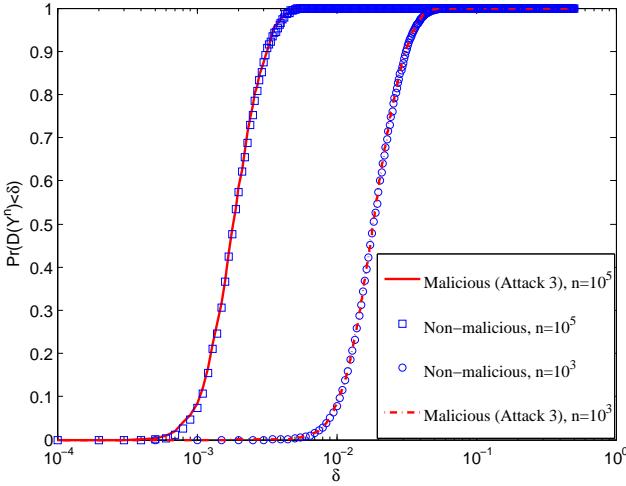


Fig. 5: Empirical CDFs of $D(Y^n)$, i.e., $\Pr(D(Y^n) \leq \delta)$, in the manipulable observation channel example considered in Section V-B.

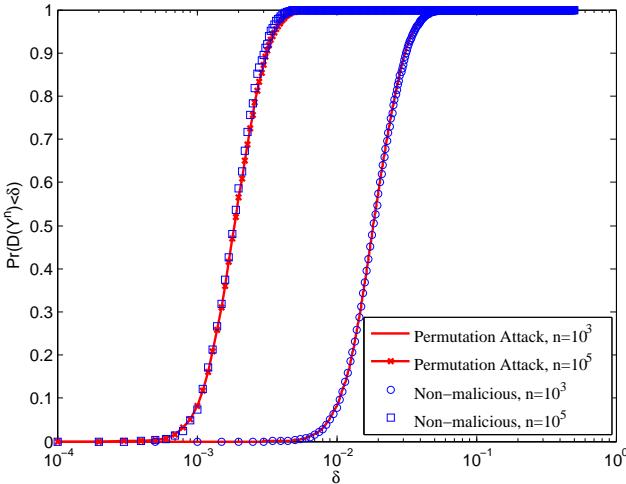


Fig. 6: Empirical CDFs of $D(Y^n)$, i.e., $\Pr(D(Y^n) < \delta)$, for the non-malicious case and the malicious case of the permutation attack in the non-manipulable observation channel of Section V-A.

non-malicious cases are indistinguishable, regardless of the value of n and whether the observation channel is manipulable or not. In other words, the permutation attack is not detectable. This is consistent with the assertion of Proposition 2.

VI. CONCLUSIONS

We have considered the detectability of Byzantine attacks conducted by two non-colluding relay nodes in a relay network, where there are two independent paths, each via one relay node, from the source to the destination. No clean reference is assumed available to the destination to detect whether Byzantine attacks have been carried out by the relay nodes. The destination is allowed to employ only the symbol sequence that it has received from the relays to perform attack detection. We have identified a family of attacks that can be detected with asymptotically small miss detection and false

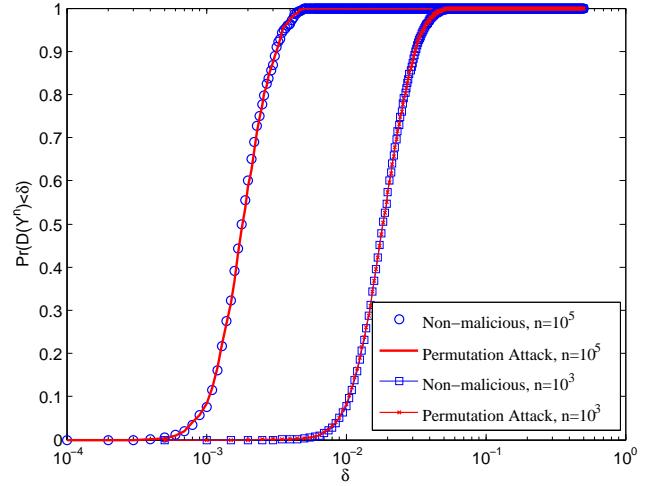


Fig. 7: Empirical CDFs of $D(Y^n)$, i.e., $\Pr(D(Y^n) \leq \delta)$ for the non-malicious case and the malicious case of the permutation attack in the manipulable observation channel of Section V-B.

alarm probabilities if and only if the channels that make up the relay network satisfies a non-manipulability condition. This family of attacks physically correspond to ones in which the two relays do not collude in attack. In addition, we have also shown that there are attacks, which do not belong to this family, that are not detectable by the destination due to the lack of a clean reference. These results provide the practical insight that we should choose relay nodes judiciously in order to reduce the possibility that they may collude in attack.

APPENDIX A

PROOF OF PROPOSITION 1 AND PROPOSITION 2

A. Proof of Proposition 1

In order to prove Proposition 1, we first give the following lemma.

Lemma 1. Let \tilde{V}^n, V^n, U^n and W^n be jointly distributed random sequences satisfying:

- 1) $\Pr\{\Pi_{U^n, V^n}(u, v) > 0\} \rightarrow 1$,
- 2) (\tilde{V}^n, V^n) and W^n are conditionally independent given U^n , and
- 3) there exists a constant $c_{w|u}$ such that $E\{1_i(w|W^n)|U^n = u^n\} = c_{w|u}$ for all $u_i = u$.

Then, we have $\Pi_{W^n|U^n, V^n}(w|u, v) \rightarrow \Pi_{W^n|U^n}(w|u)$ for all w . Furthermore, if

- 4) $\Pr\{\Pi_{W^n|U^n}(w|u) > 0\} \rightarrow 1$ is also satisfied, then $\Pi_{\tilde{V}^n, V^n|U^n, W^n}(\tilde{v}|u, v, w) \rightarrow \Pi_{\tilde{V}^n|U^n, V^n}(\tilde{v}|u, v)$ for all \tilde{v} .

Proof: Condition 1) guarantees that $\Pr\{\Pi_{U^n}(u) > 0\} \rightarrow 1$. Hence $\Pi_{V^n|U^n}(v|u)$ and $\Pi_{\tilde{V}^n, V^n|U^n}(\tilde{v}, v|u)$ are well-defined with high probabilities for all sufficiently large n . Define

$$S_n \triangleq \sum_{i=1}^n \{1_i(w|W^n) - c_{w|u}\} 1_i(u|U^n) \{1_i(\tilde{v}, v|\tilde{V}^n, V^n)$$

$$- \Pi_{\tilde{V}^n, V^n | U^n}(\tilde{v}, v | u) \}. \quad (18)$$

For any (u^n, v^n, \tilde{v}^n) conditioned on the event $\{U^n = u^n, V^n = v^n, \tilde{V}^n = \tilde{v}^n\}$, conditions 2) and 3) guarantee that the sequence $\{S_n\}$ is a martingale. According to Hoeffding's inequality [20, Theorem 2], we have

$$\Pr \left\{ \left| \frac{S_n}{n} \right| \geq \mu \middle| U^n = u^n, V^n = v^n, \tilde{V}^n = \tilde{v}^n \right\} \leq 2e^{-\frac{n\mu^2}{2}} \quad (19)$$

for any $\mu > 0$.

Furthermore, we have the equality

$$\sum_{i=1}^n 1_i(u | U^n) \{1_i(\tilde{v}, v | \tilde{V}^n, V^n) - \Pi_{\tilde{V}^n, V^n | U^n}(\tilde{v}, v | u)\} = 0, \quad (20)$$

which implies that

$$\begin{aligned} S_n &= \Pi_{\tilde{V}^n, V^n, U^n, W^n}(\tilde{v}, v, u, w) \\ &\quad - \Pi_{\tilde{V}^n, V^n | U^n}(\tilde{v}, v | u) \Pi_{U^n, W^n}(u, w). \end{aligned}$$

The above equation together with (19) gives

$$\Pr \left\{ \left| \Pi_{\tilde{V}^n, V^n, U^n, W^n}(\tilde{v}, v, u, w) - \Pi_{\tilde{V}^n, V^n | U^n}(\tilde{v}, v | u) \Pi_{U^n, W^n}(u, w) \right| \geq \mu \right\} \leq 2e^{-\frac{n\mu^2}{2}}. \quad (21)$$

Thus, we have

$$\Pi_{\tilde{V}^n, V^n, U^n, W^n}(\tilde{v}, v, u, w) \rightarrow \Pi_{\tilde{V}^n, V^n | U^n}(\tilde{v}, v | u) \Pi_{U^n, W^n}(u, w) \quad (22)$$

and

$$\begin{aligned} \Pi_{U^n, W^n}(u, v, w) &\rightarrow \Pi_{V^n | U^n}(v | u) \Pi_{U^n, W^n}(u, w) \\ &= \Pi_{U^n, V^n}(u, v) \Pi_{W^n | U^n}(w | u). \end{aligned} \quad (23)$$

Immediately, (23) implies $\Pi_{W^n | U^n}(w | u, v) \rightarrow \Pi_{W^n | U^n}(w | u)$. Furthermore, note that if condition 4) holds, (23) also implies that $\Pr\{\Pi_{U^n, V^n, W^n}(u, v, w) > 0\} \rightarrow 1$, and hence $\Pi_{\tilde{V}^n | U^n, V^n, W^n}(\tilde{v} | u, v, w)$ is well-defined. Dividing (22) by (23) gives $\Pi_{\tilde{V}^n | U^n, V^n, W^n}(\tilde{v} | u, v, w) \rightarrow \Pi_{\tilde{V}^n | U^n, V^n}(\tilde{v} | u, v)$. ■

Let us now turn our attention to the proof of Proposition 1. Note that

$$\begin{aligned} \Pi_{V_1^n, V_2^n | U_1^n, U_2^n}(v_1, v_2 | u_1, u_2) \\ = \Pi_{V_1^n | U_1^n, U_2^n}(v_1 | u_1, u_2) \Pi_{V_2^n | V_1^n, U_1^n, U_2^n}(v_2 | v_1, u_1, u_2). \end{aligned} \quad (24)$$

Since $P_{U_1, U_2}(u_1, u_2) > 0$, we have $\Pr\{\Pi_{U_1^n, U_2^n}(u_1, u_2) > 0\} \rightarrow 1$. As a result, relying on Lemma 1, we obtain $\Pi_{V_1^n | U_1^n, U_2^n}(v_1 | u_1, u_2) \rightarrow \Pi_{V_1^n | U_1^n}(v_1 | u_1)$. This result, together with the assumption $\Pr\{\Pi_{V_1^n | U_1^n}(v_1 | u_1) > 0\} \rightarrow 1$, gives $\Pr\{\Pi_{V_1^n, U_1^n, U_2^n}(v_1, u_1, u_2) > 0\} \rightarrow 1$, and thus $\Pi_{V_2^n | V_1^n, U_1^n, U_2^n}(v_2 | v_1, u_1, u_2)$ is well-defined. Then, the proof of Proposition 1 is equivalent to proving

$$\Pi_{V_2^n | V_1^n, U_1^n, U_2^n}(v_2 | v_1, u_1, u_2) \rightarrow \Pi_{V_2^n | U_2^n}(v_2 | u_2) \quad (25)$$

as long as the conditions stated in Proposition 1 are satisfied. To this end, we notice that Proposition 1 essentially assumes

- 1) (V_1^n, U_1^n) and V_2^n are conditionally independent given U_2^n .

2) There exists a constant $c_{v_2 | u_2}$ such that $E\{1_i(v_2 | V_2^n) | U_2^n = u_2^n\} = c_{v_2 | u_2}$ for all $u_{2,i} = u_2$.

Substituting these conditions into Lemma 1, it is straightforward to arrive at (25). Therefore, Proposition 1 is proved.

B. Proof of Proposition 2

The proof of Proposition 2 is presented as follows.

Proof: Let us consider the following two cases:

- i) The relays attack their received signals by rearranging the sequences in the time domain. For any $k, t = 1, \dots, n$, if $V_{1,k} = U_{1,t}$ and $V_{1,t} = U_{1,k}$, there must be $V_{2,k} = U_{2,t}$ and $V_{2,t} = U_{2,k}$. In such case, we obtain $\Pi'_{V_m^n | U_m^n} \neq I$ for $m = 1, 2$.
- ii) Both relays are non-malicious, i.e., $\Pi_{V_m^n | U_m^n} = I$ for $m = 1, 2$.

Let us stack U_1 and U_2 into a vector denoted as \mathbf{U} , i.e., $\mathbf{U} = [U_1; U_2]$. Similarly, we also stack V_1 and V_2 into a vector denoted as \mathbf{V} , i.e., $\mathbf{V} = [V_1; V_2]$. The matrices $\mathbf{U}^n = [U_1^n; U_2^n]$ and $\mathbf{V}^n = [V_1^n; V_2^n]$, of dimension $2 \times n$, represent the input and output random sequences of the relays, respectively. The i th column in \mathbf{U}^n and \mathbf{V}^n is denoted as \mathbf{U}_i and \mathbf{V}_i , respectively. In the case i), from $V_{1,k} = U_{1,t}, V_{1,t} = U_{1,k}$ and $V_{2,k} = U_{2,t}, V_{2,t} = U_{2,k}$, we have $\mathbf{V}_k = \mathbf{U}_t$ and $\mathbf{V}_t = \mathbf{U}_k$, which indicates that \mathbf{V}^n is actually equivalent to the rearrangement of \mathbf{U}^n in the time domain. Since \mathbf{U}^n is an i.i.d sequence, the PMF of \mathbf{U}^n only depends on the PMFs of its elements. Rearranging \mathbf{U}^n does not change the PMFs of its elements, and hence the PMF of \mathbf{U}^n remains unchanged. In other words, \mathbf{V}^n and \mathbf{U}^n have the same PMF in the case i). Therefore, the distribution of Y^n in both cases is exactly the same. Thus, any decision statistic $D(Y^n)$ also has the same distribution in both cases. Furthermore, in case ii), since we have $\sum_{m=1}^2 \|\Pi_{V_m^n | U_m^n} - I\|_2 = 0$, Property 2) of Theorem 1 requires the probability of the event $\{D(Y^n) > \delta\}$ be arbitrarily small as long as δ is sufficiently small and n is sufficiently large. On the other hand, in the case i), by choosing $\delta < \sum_{m=1}^2 \|\Pi'_{V_m^n | U_m^n} - I\|_2$, Property 1) requires that the probability of the same event $\{D(Y^n) > \delta\}$ is arbitrarily close to 1 as long as n is large enough. Hence, these two requirements contradict. Therefore, Proposition 2 is proved. ■

APPENDIX B PROOF OF THEOREM 1

A. Proof of Sufficiency of Theorem 1

To prove the sufficiency of Theorem 1, we need the following Lemma 2 which characterizes the convergence property of Π_{Y^n} . Note that the lemma holds for any arbitrary attack in the family (7).

Lemma 2. *If $\Pi_{V_1^n, V_2^n | U_1^n, U_2^n}(v_1, v_2 | u_1, u_2) \rightarrow \Pi_{V_1^n | U_1^n}(v_1 | u_1) \Pi_{V_2^n | U_2^n}(v_2 | u_2)$, we have $\|\Pi_{Y^n} - P_{U_1, U_2}(\Pi_{V_1^n | U_1^n}^T \otimes \Pi_{V_2^n | U_2^n}^T) P_{Y | V_1, V_2}^T\|_2 \rightarrow 0$ in probability as $n \rightarrow \infty$.*

Proof: According to the definitions of $\Pi_{V_1^n, V_2^n | U_1^n, U_2^n}$, $\Pi_{V_1^n | U_1^n}$ and $\Pi_{V_2^n | U_2^n}$, the convergence $\Pi_{V_1^n, V_2^n | U_1^n, U_2^n} (v_1, v_2 | u_1, u_2) \rightarrow \Pi_{V_1^n | U_1^n} (v_1 | u_1) \Pi_{V_2^n | U_2^n} (v_2 | u_2)$ indicates

$$\left[\Pi_{V_1^n, V_2^n | U_1^n, U_2^n} \right]_{i,j} \rightarrow \left[\Pi_{V_1^n | U_1^n} \right]_{t_1, k_1} \left[\Pi_{V_2^n | U_2^n} \right]_{t_2, k_2},$$

$$j = (k_1 - 1) |\mathcal{U}_2| + k_2, i = (t_1 - 1) |\mathcal{U}_2| + t_2.$$

Then, applying the definition of Kronecker product, we obtain $\left[\Pi_{V_1^n, V_2^n | U_1^n, U_2^n} \right]_{i,j} \rightarrow \left[\Pi_{V_1^n | U_1^n} \otimes \Pi_{V_2^n | U_2^n} \right]_{i,j}$, which yields $\Pi_{V_1^n, V_2^n | U_1^n, U_2^n} \rightarrow \Pi_{V_1^n | U_1^n} \otimes \Pi_{V_2^n | U_2^n}$.

For any $\mu_1 > 0$, it is clear that (26) holds true, which is given in the next page. The second probability after the last “ \leq ” of (26) approaches zero according to the above-obtained assertion that $\Pi_{V_1^n, V_2^n | U_1^n, U_2^n} \rightarrow \Pi_{V_1^n | U_1^n} \otimes \Pi_{V_2^n | U_2^n}$. The first probability after the last “ \leq ” of (26) also approaches zero, as shown by the following proof. For ease of description, we employ the vector notation in the following proof. For instance, the pair of random variables $\{U_1, U_2\}$ is denoted as $\mathbf{U} = [U_1; U_2]$, whose alphabet \mathcal{U} is the Cartesian product of \mathcal{U}_1 and \mathcal{U}_2 . For ease of description, we also employ \mathbf{u}_i to denote the i th element in \mathcal{U} , where i is an integer taking value from 1 to $|\mathcal{U}|$. Similarly, we also stack V_1 and V_2 into a vector denoted as \mathbf{V} , i.e., $\mathbf{V} = [V_1; V_2]$, whose alphabet \mathcal{V} is the Cartesian product of \mathcal{V}_1 and \mathcal{V}_2 . For convenience of exposition, we employ \mathbf{v}_i to denote the i th element in \mathcal{V} , where i is an integer taking value from 1 to $|\mathcal{V}|$. Again, $\mathbf{U}^n = [U_1^n; U_2^n]$ and $\mathbf{V}^n = [V_1^n; V_2^n]$ denote the input and output random sequences of the relays, respectively. Correspondingly, $\mathbf{u}^n = [u_1^n; u_2^n]$ and $\mathbf{v}^n = [v_1^n; v_2^n]$ denote the generic value of the input and output sequences of the relays, respectively. In other words, \mathbf{U}^n and \mathbf{V}^n are sequences of random variables, while \mathbf{u}^n and \mathbf{v}^n denote the possible value of \mathbf{U}^n and \mathbf{V}^n , respectively. Then, we have

$$|P_U \Pi_{V^n | U^n}^T P_{Y|V}^T - \Pi_{Y^n}| = \sum_{i=1}^{|\mathcal{Y}|} |[P_U \Pi_{V^n | U^n}^T P_{Y|V}^T]_i - [\Pi_{Y^n}]_i|$$

$$\leq \sum_{i=1}^{|\mathcal{Y}|} \sum_{j=1}^{|\mathcal{U}|} \sum_{k=1}^{|\mathcal{V}|} |H_{i,j,k}|, \quad (27)$$

where

$$H_{i,j,k} = P_U(\mathbf{u}_j) \frac{N(\mathbf{u}_j, \mathbf{v}_k | \mathbf{U}^n, \mathbf{V}^n)}{N(\mathbf{u}_j | \mathbf{U}^n)} P_{Y|V}(y_i | \mathbf{v}_k)$$

$$- \frac{N(\mathbf{u}_j, \mathbf{v}_k, y_i | \mathbf{U}^n, \mathbf{V}^n, Y^n)}{n}. \quad (28)$$

This implies that

$$\Pr \left\{ |P_U \Pi_{V^n | U^n}^T P_{Y|V}^T - \Pi_{Y^n}| > \frac{\mu_1}{2} \right\}$$

$$\leq \sum_{i=1}^{|\mathcal{Y}|} \sum_{j=1}^{|\mathcal{U}|} \sum_{k=1}^{|\mathcal{V}|} \Pr \left\{ |H_{i,j,k}| \geq \frac{\mu_1}{2 |\mathcal{Y}| |\mathcal{U}| |\mathcal{V}|} \right\}. \quad (29)$$

In order to bound $\Pr \left\{ |H_{i,j,k}| \geq \frac{\mu_1}{2 |\mathcal{Y}| |\mathcal{U}| |\mathcal{V}|} \right\}$, we first consider to bound

$$\Pr \left\{ |\tilde{H}_{i,j,k}| \geq \frac{\mu_1}{2 |\mathcal{Y}| |\mathcal{U}| |\mathcal{V}|} \right\}, \quad (30)$$

where

$$\tilde{H}_{i,j,k} = \frac{N(\mathbf{u}_j | \mathbf{U}^n)}{n} \frac{N(\mathbf{u}_j, \mathbf{v}_k | \mathbf{U}^n, \mathbf{V}^n)}{N(\mathbf{u}_j | \mathbf{U}^n)} P_{Y|V}(y_i | \mathbf{v}_k)$$

$$- \frac{N(\mathbf{u}_j, \mathbf{v}_k, y_i | \mathbf{U}^n, \mathbf{V}^n, Y^n)}{n}$$

$$= \frac{N(\mathbf{u}_j, \mathbf{v}_k | \mathbf{U}^n, \mathbf{V}^n)}{n} P_{Y|V}(y_i | \mathbf{v}_k)$$

$$- \frac{N(\mathbf{u}_j, \mathbf{v}_k, y_i | \mathbf{U}^n, \mathbf{V}^n, Y^n)}{n}. \quad (31)$$

For any i, j and k ,

$$\Pr \left\{ |\tilde{H}_{i,j,k}| \geq \frac{\mu_1}{2 |\mathcal{Y}| |\mathcal{U}| |\mathcal{V}|} \right\} \leq \frac{4 |\mathcal{Y}|^2 |\mathcal{U}|^2 |\mathcal{V}|^2}{\mu_1^2} E\{|\tilde{H}_{i,j,k}|^2\}. \quad (32)$$

Furthermore, we have (33), as given on the next page, where the inequality (b) is obtained based on the fact that the elements of Y^n are conditionally independent given $\mathbf{V}^n = \mathbf{v}^n$. Again relying on this fact, the inequality (a) is obtained as follows. Firstly, we have (34), as given on the next page. Furthermore, for each $(\mathbf{u}^n, \mathbf{v}^n)$ and (t, t') with $1_t(\mathbf{u}_j, \mathbf{v}_k) 1_{t'}(\mathbf{u}_j, \mathbf{v}_k) = 1$, we have (35) shown on the next page, where the equation (a) is obtained relying on $P_{Y|V}(y_i | \mathbf{v}_k) = P_{Y|V, U}(y_i | \mathbf{v}_k, \mathbf{u}_j)$. Substituting (33) into (32), we get $\Pr\{|\tilde{H}_{i,j,k}| \geq \frac{\mu_1}{2 |\mathcal{Y}| |\mathcal{U}| |\mathcal{V}|}\} \rightarrow 0$ as $n \rightarrow \infty$. Comparing $\tilde{H}_{i,j,k}$ with $H_{i,j,k}$, we see that $\tilde{H}_{i,j,k} \rightarrow H_{i,j,k}$ as $n \rightarrow \infty$, then we arrive at $\Pr\{|H_{i,j,k}| \geq \frac{\mu_1}{2 |\mathcal{Y}| |\mathcal{U}| |\mathcal{V}|}\} \rightarrow 0$ as $n \rightarrow \infty$. Using (29), we further obtain $\Pr\{|P_U \Pi_{V^n | U^n}^T P_{Y|V}^T - \Pi_{Y^n}| > \frac{\mu_1}{2}\} \rightarrow 0$ as $n \rightarrow \infty$. Thus, this lemma has been proved, because we have shown that the two probabilities after the last “ \leq ” of (26) converge to 0 as n approaches infinity. ■

Applying Lemma 2, the sufficiency proof of Theorem 1 originally outlined in [17] for dealing with i.i.d attacks can be readily extended to the case of non-i.i.d attacks considered here. We provide the details of proof below for completeness.

To establish the proof of sufficiency, we construct the estimators $\hat{\Pi}_{V_1^n | U_1^n}$ and $\hat{\Pi}_{V_2^n | U_2^n}$ from Π_{Y^n} according to the following arrangement:

For $\mu > 0$, let $\mathcal{G}_\mu(\Pi_{Y^n})$ be the set of all pairs of the two stochastic matrices P_1 and P_2 (their dimensions are $|\mathcal{U}_1| \times |\mathcal{U}_1|$ and $|\mathcal{U}_2| \times |\mathcal{U}_2|$, respectively), which satisfy

$$\left\| P_{U_1, U_2} (P_1^T \otimes P_2^T) P_{Y|V_1, V_2}^T - \Pi_{Y^n} \right\|_2 \leq \mu; \quad (36)$$

if $\mathcal{G}_\mu(\Pi_{Y^n})$ is non-empty, we set

$$(\hat{\Pi}_{V_1^n | U_1^n}, \hat{\Pi}_{V_2^n | U_2^n}) = \arg \max_{(P_1, P_2) \in \mathcal{G}_\mu(\Pi_{Y^n})} \sum_{i=1}^2 \|P_i - I\|_2; \quad (37)$$

otherwise, set $(\hat{\Pi}_{V_1^n | U_1^n}, \hat{\Pi}_{V_2^n | U_2^n}) = (I, I)$. Relying on $(\hat{\Pi}_{V_1^n | U_1^n}, \hat{\Pi}_{V_2^n | U_2^n})$, in what follows we employ the decision statistic $D(Y^n) = \sum_{i=1}^2 \|\hat{\Pi}_{V_i^n | U_i^n} - I\|_2$.

1) *The Proof of Property 1) of Theorem 1:* To show that this decision statistic satisfies Property 1) of Theorem 1, note that (38) holds, where the equality in the third line is obtained relying on $\hat{\Pi}_{V_1^n | U_1^n}$ and $\hat{\Pi}_{V_2^n | U_2^n}$ given by (37), and on the fact that $\Pr\{(\hat{\Pi}_{V_1^n | U_1^n}, \hat{\Pi}_{V_2^n | U_2^n}) \in \mathcal{G}_\mu(\Pi_{Y^n})\} \rightarrow 1$ as $n \rightarrow \infty$, as implied by Lemma 2. Hence, it is plausible that Property 1) of Theorem 1 is a direct consequence of this latter fact and (38).

$$\begin{aligned}
& \Pr \left\{ \left\| P_{U_1, U_2} (\Pi_{V_1^n|U_1^n}^T \otimes \Pi_{V_2^n|U_2^n}^T) P_{Y|V_1, V_2}^T - \Pi_{Y^n} \right\|_2 > \mu_1 \right\} < \Pr \left\{ |P_{U_1, U_2} (\Pi_{V_1^n|U_1^n}^T \otimes \Pi_{V_2^n|U_2^n}^T) P_{Y|V_1, V_2}^T - \Pi_{Y^n}| > \mu_1 \right\} \\
& \leq \Pr \left\{ |P_{U_1, U_2} \Pi_{V_1^n, V_2^n|U_1^n, U_2^n}^T P_{Y|V_1, V_2}^T - \Pi_{Y^n}| > \frac{\mu_1}{2} \right\} + \\
& \quad \Pr \left\{ |P_{U_1, U_2} (\Pi_{V_1^n|U_1^n}^T \otimes \Pi_{V_2^n|U_2^n}^T) P_{Y|V_1, V_2}^T - P_{U_1, U_2} (\Pi_{V_1^n|U_1^n}^T \otimes \Pi_{V_2^n|U_2^n}^T) P_{Y|V_1, V_2}^T| > \frac{\mu_1}{2} \right\}. \tag{26}
\end{aligned}$$

$$\begin{aligned}
E\{|\tilde{H}_{i,j,k}|^2\} &= E\left\{ \left| \frac{N(\mathbf{u}_j, \mathbf{v}_k | \mathbf{U}^n, \mathbf{V}^n)}{n} P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - \frac{N(\mathbf{u}_j, \mathbf{v}_k, \mathbf{y}_i | \mathbf{U}^n, \mathbf{V}^n, Y^n)}{n} \right|^2 \right\} \\
&\leq \frac{E\{(\sum_{t=1}^n (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) 1_t(\mathbf{u}_j, \mathbf{v}_k) - 1_t(\mathbf{u}_j, \mathbf{v}_k, \mathbf{y}_i)))^2\}}{n^2} \\
&= \frac{E\{(\sum_{t=1}^n 1_t(\mathbf{u}_j, \mathbf{v}_k) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i)))^2\}}{n^2} \\
&= \frac{E\{\sum_{t,t'=1}^n 1_t(\mathbf{u}_j, \mathbf{v}_k) 1_{t'}(\mathbf{u}_j, \mathbf{v}_k) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i)) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_{t'}(\mathbf{y}_i))\}}{n^2} \\
&\leq \frac{E\{\sum_{t=1}^n 1_t(\mathbf{u}_j, \mathbf{v}_k) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i))^2\}}{n^2} \\
&\quad + \frac{E\{\sum_{t,t'=1, t \neq t'}^n 1_t(\mathbf{u}_j, \mathbf{v}_k) 1_{t'}(\mathbf{u}_j, \mathbf{v}_k) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i)) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_{t'}(\mathbf{y}_i))\}}{n^2} \\
&\stackrel{(a)}{\leq} \frac{E_{\mathbf{U}^n, \mathbf{V}^n} \left\{ \sum_{t=1}^n E\left\{ 1_t(\mathbf{u}_j, \mathbf{v}_k) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i))^2 | \mathbf{u}^n, \mathbf{v}^n \right\} \right\}}{n^2} \\
&\stackrel{(b)}{\leq} \frac{\sum_{t=1}^n E\left\{ (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i))^2 | \mathbf{u}_j, \mathbf{v}_k \right\}}{n^2} \\
&\leq \frac{P_{Y|\mathbf{V}}^2(\mathbf{y}_i | \mathbf{v}_k)}{n}, \tag{33}
\end{aligned}$$

$$\begin{aligned}
& E \left\{ \sum_{t,t'=1, t \neq t'}^n 1_t(\mathbf{u}_j, \mathbf{v}_k) 1_{t'}(\mathbf{u}_j, \mathbf{v}_k) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i)) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_{t'}(\mathbf{y}_i)) \right\} \\
&= E_{\mathbf{U}^n, \mathbf{V}^n} \left\{ \sum_{t,t'=1, t \neq t'}^n E\left\{ 1_t(\mathbf{u}_j, \mathbf{v}_k) 1_{t'}(\mathbf{u}_j, \mathbf{v}_k) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i)) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_{t'}(\mathbf{y}_i)) | \mathbf{u}^n, \mathbf{v}^n \right\} \right\}. \tag{34}
\end{aligned}$$

$$\begin{aligned}
& E\left\{ 1_t(\mathbf{u}_j, \mathbf{v}_k) 1_{t'}(\mathbf{u}_j, \mathbf{v}_k) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i)) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_{t'}(\mathbf{y}_i)) | \mathbf{u}^n, \mathbf{v}^n \right\} \\
&= E\left\{ (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i)) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_{t'}(\mathbf{y}_i)) | 1_t(\mathbf{u}_j, \mathbf{v}_k) 1_{t'}(\mathbf{u}_j, \mathbf{v}_k) = 1 \right\} \\
&= E\left\{ (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_t(\mathbf{y}_i)) [\mathbf{u}_j, \mathbf{v}_k] E\left[(P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - 1_{t'}(\mathbf{y}_i)) | \mathbf{u}_j, \mathbf{v}_k \right] \right\} \\
&\stackrel{(a)}{=} (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k)) (P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k) - P_{Y|\mathbf{V}}(\mathbf{y}_i | \mathbf{v}_k)) \\
&= 0, \tag{35}
\end{aligned}$$

2) *The Proof of Property 2) of Theorem 1:* To prove a stochastic matrix, W_i can be expressed as Property 2) of Theorem 1, we define the function

$$F(\mathbf{w}) \triangleq \left\| P_{U_1, U_2} (W_1^T \otimes W_2^T) P_{Y|V_1, V_2}^T - P_{U_1, U_2} P_{Y|V_1, V_2}^T \right\|_2^2,$$

where we use W_i , of dimension $|\mathcal{U}_i| \times |\mathcal{U}_i|$, to denote all possible values of $\Pi_{V_i^n|U_i^n}$ for $i = 1, 2$. Since $\Pi_{V_i^n|U_i^n}$ is

$$W_i = \begin{bmatrix} 1 - \sum_{k=2}^{|\mathcal{U}_i|} [W_i]_{k,1} & \cdots & \cdots & [W_i]_{1,|\mathcal{U}_i|} \\ [W_i]_{2,1} & \ddots & & [W_i]_{2,|\mathcal{U}_i|} \\ \vdots & & \ddots & \vdots \\ [W_i]_{|\mathcal{U}_i|,1} & \cdots & \cdots & 1 - \sum_{k=1}^{|\mathcal{U}_i|-1} [W_i]_{k,|\mathcal{U}_i|} \end{bmatrix},$$

$$\begin{aligned}
& \Pr \left\{ D(Y^n) > \delta \cap \sum_{i=1}^2 \|\Pi_{V_i^n|U_i^n} - I\|_2 > \delta \right\} \\
& \geq \Pr \left\{ (\Pi_{V_1^n|U_1^n}, \Pi_{V_2^n|U_2^n}) \in \mathcal{G}_\mu(\Pi_{Y^n}) \cap D(Y^n) > \delta \cap \sum_{i=1}^2 \|\Pi_{V_i^n|U_i^n} - I\|_2 > \delta \right\} \\
& = \Pr \left\{ (\Pi_{V_1^n|U_1^n}, \Pi_{V_2^n|U_2^n}) \in \mathcal{G}_\mu(\Pi_{Y^n}) \cap \sum_{i=1}^2 \|\Pi_{V_i^n|U_i^n} - I\|_2 > \delta \right\} \\
& \geq \Pr \left\{ \sum_{i=1}^2 \|\Pi_{V_i^n|U_i^n} - I\|_2 > \delta \right\} - \Pr \left\{ (\Pi_{V_1^n|U_1^n}, \Pi_{V_2^n|U_2^n}) \notin \mathcal{G}_\mu(\Pi_{Y^n}) \right\}, \tag{38}
\end{aligned}$$

where each entry of W_i takes value from the interval $[0, 1]$. Then, except the diagonal entries, stacking all entries of both W_1 and W_2 column by column, we obtain the vector \mathbf{w} . More precisely, $\mathbf{w} = [[W_1]_{2,1}, \dots, [W_1]_{|\mathcal{U}_1|,1}, \dots, [W_1]_{|\mathcal{U}_1|-1,|\mathcal{U}_1|}, \dots, [W_2]_{|\mathcal{U}_2|-1,|\mathcal{U}_2|}]$. It is straightforward to check that \mathbf{w} and $F(\mathbf{w})$ have the following properties:

- 1) All possible \mathbf{w} 's belong to $\mathcal{D} = \{\mathbf{w} | 0 \leq [W_i]_{k,j} \leq 1, \sum_{k=1, k \neq j}^{|\mathcal{U}_i|} [W_i]_{k,j} \leq 1, i = 1, 2, k \neq j, k, j = 1, 2, \dots, |\mathcal{U}_i|\}$. \mathcal{D} is a bounded convex and continuous set. Obviously, it includes $\mathbf{w}_0 \triangleq [0, 0, \dots, 0]$.
- 2) $F(\mathbf{w})$ is twice continuously differentiable in \mathcal{D} .
- 3) Since the non-manipulable condition is satisfied, \mathbf{w}_0 , which corresponds to $W_1 = I$ and $W_2 = I$, is the unique solution to $F(\mathbf{w}) = 0$ in \mathcal{D} . Moreover, $\nabla F = 0$ at \mathbf{w}_0 .

These properties can be used for proving the following Lemma 3:

Lemma 3. *There exists an $r_1 > 0$, depending only on $F(\mathbf{w})$, such that the closed subset $\mathcal{D}_1 \triangleq \{\mathbf{w} | \|\mathbf{w} - \mathbf{w}_0\|_2 \leq r_1\} \cap \mathcal{D}$ of \mathcal{D} has the following property:*

For each radial line L emanating from \mathbf{w}_0 to a point on the boundary of \mathcal{D}_1 (i.e., $\{\mathbf{w} | \|\mathbf{w} - \mathbf{w}_0\|_2 = r_1\} \cap \mathcal{D}$), we have $\nabla_L F(\mathbf{w}) > 0$ for all $\mathbf{w} \neq \mathbf{w}_0$ on L , where $\nabla_L F$ is the orientational derivative of F along L .

Proof: Let us choose an arbitrary orientation from \mathbf{w}_0 , denoted as $L = [l_1, l_2, \dots, l_{|\mathcal{U}_1|}]$, $\|L\|_2^2 = 1$. Each point \mathbf{w} along the orientation L can be expressed as $\mathbf{w} = lL$, where $l = \|\mathbf{w} - \mathbf{w}_0\|_2$ is positive and continuous-valued. Then, relying on the orientation L , l could be used to represent \mathbf{w} . We thus rewrite \mathbf{w} as \mathbf{w}_l . Correspondingly, we define a function $f(l) \triangleq F(\mathbf{w}_l)$ and its derivative function (i.e., $f'(l) \triangleq \nabla_L F(\mathbf{w})$) along the orientation L . According to the third property of $F(\mathbf{w})$, $l = 0$ is the only solution to $f(l) = 0$, and we also have $f'(0) = 0$. To complete the proof, let us prove that there exists a positive r_L such that for any arbitrary $l \in (0, r_L]$, we always have $f'(l) > 0$. To this end, let us discuss two possible cases in the following. In the first case where $f'(l) \neq 0$ holds true for all $l \in (0, \infty)$, there must exist at least one positive r_L that renders $f'(l) > 0$ true for all $l \in (0, r_L]$. Otherwise, the contrary statement that $f'(l) < 0$ for all $l \in (0, r_L]$ will result in the fact that $f(l)$ is a decreasing function in the domain $(0, r_L]$. As a

consequence, we will have $f(l) < f(0) = 0$ for $l \in (0, r_L]$, which contradicts the fact that $f(0) = 0$ is the minimum value. In addition, if $f'(l) < 0$ holds true for some values of l and $f'(l) > 0$ for another set of values of l , we can deduce that there is at least one point making $f'(l) = 0$, since $f'(l)$ is a continuous function according to the second property that $F(\mathbf{w})$ is twice continuously differentiable. This in turn contradicts the basic assumption of this case, namely $f'(l) \neq 0$.

Second, if $f'(l)$ can be equal to 0, among all the points making $f'(l) = 0$, let us choose the one nearest to $l = 0$, denoted as s . Then, r_L can be chosen from the interval $(0, s)$, such that for $l \in (0, r_L]$, we have $f'(l) \neq 0$. Hence, there must be $f'(l) > 0$ for $l \in (0, r_L]$. The explanation is similar to that of the first case.

Finally, we choose r_1 according to $r_1 = \min_{L=\frac{\mathbf{w}-\mathbf{w}_0}{\|\mathbf{w}-\mathbf{w}_0\|_2}, \mathbf{w} \in \mathcal{D}} r_L$. Hence, for each radial line L emanating from \mathbf{w}_0 to the boundary of $\mathcal{D}_1 = \{\mathbf{w} | \|\mathbf{w} - \mathbf{w}_0\|_2 \leq r_1\} \cap \mathcal{D}$, we have $\nabla_L F(\mathbf{w}) > 0$ for all $\mathbf{w} \neq \mathbf{w}_0$ on L . \blacksquare

Relying on Lemma 3, the function $F_{\min}(r) \triangleq \min_{\mathbf{w}: \|\mathbf{w} - \mathbf{w}_0\|_2 = r, \mathbf{w} \in \mathcal{D}} F(\mathbf{w})$ is a strictly increasing and bounded function over $0 \leq r \leq r_1$. Hence, an inverse of F_{\min} (denoted by F_{\min}^{-1}) exists, which is also increasing and bounded. This property can be used to prove the following Lemma 4:

Lemma 4. *Let us use \mathbf{m} to denote $\min_{\mathbf{w} \in \mathcal{D} - \mathcal{D}_1} F(\mathbf{w})$. For all $\mathbf{m}' \in (0, \mathbf{m}]$, if $\mathbf{w} \in \mathcal{D}$ and $F(\mathbf{w}) < \mathbf{m}'$, then there must exist*

$$\|\mathbf{w} - \mathbf{w}_0\|_2 < F_{\min}^{-1}(\mathbf{m}'). \tag{39}$$

Proof: Since \mathbf{w}_0 is not in $\mathcal{D} - \mathcal{D}_1$ and \mathbf{w}_0 is the only point satisfying $F(\mathbf{w}_0) = 0$, \mathbf{m} is a strictly positive number. Furthermore, noticing that $\{\mathbf{w} | \|\mathbf{w} - \mathbf{w}_0\|_2 = r_1, \mathbf{w} \in \mathcal{D}\}$ is a part of the boundary of $\mathcal{D} - \mathcal{D}_1$, we have $\mathbf{m} \leq F_{\min}(r_1) = \min_{\mathbf{w}: \|\mathbf{w} - \mathbf{w}_0\|_2 = r_1, \mathbf{w} \in \mathcal{D}} F(\mathbf{w})$. Then, for any arbitrary \mathbf{m}' smaller than \mathbf{m} , according to the monotonically increasing property of $F_{\min}^{-1}(\cdot)$, we have $F_{\min}^{-1}(\mathbf{m}') < F_{\min}^{-1}(\mathbf{m}) \leq r_1$. Based on this observation, we obtain $\mathcal{D}' \subset \mathcal{D}_1$, where \mathcal{D}' denotes $\{\mathbf{w} | \|\mathbf{w} - \mathbf{w}_0\|_2 < F_{\min}^{-1}(\mathbf{m}')\} \cap \mathcal{D}$. As a result, $\mathcal{D} - \mathcal{D}' = \{\mathcal{D} - \mathcal{D}_1\} \cup \{\mathcal{D}_1 - \mathcal{D}'\}$ holds true, from which the minimum value of $F(\mathbf{w})$ over $\mathcal{D} - \mathcal{D}'$ can be deduced as follows. Firstly, relying on the monotonically increasing property of $F_{\min}(\cdot)$, the minimum value of $F(\mathbf{w})$ over $\mathcal{D}_1 - \mathcal{D}'$ is \mathbf{m}' .

Secondly, recalling that m is the minimum value of $F(\mathbf{w})$ over $\mathcal{D} - \mathcal{D}_1$ and $m' < m$, then the minimum value of $F(\mathbf{w})$ over $\mathcal{D} - \mathcal{D}'$ is m' . Therefore, if $F(\mathbf{w}) < m' < m$, \mathbf{w} must be in $\mathcal{D}' = \{\mathbf{w} \mid \|\mathbf{w} - \mathbf{w}_0\|_2 < F_{\min}^{-1}(m')\} \cap \mathcal{D}$. Otherwise, if a point \mathbf{w}_t satisfying $F(\mathbf{w}_t) < m'$ were in $\mathcal{D} - \mathcal{D}'$, $F(\mathbf{w}_t)$ would be less than the minimum value of $F(\mathbf{w})$ over $\mathcal{D} - \mathcal{D}'$, which is a self-contradiction. Lemma 4 has been proved. ■

Furthermore, since $F_{\min}(r)$ is continuous at $r = 0$, the distance given by the left-hand side of (39) can be made arbitrarily small by selecting a sufficiently small m' .

Now, let us continue proving Property 2) of Theorem 1. First, note that if $\|\Pi_{Y^n} - P_{U_1, U_2}(\Pi_{V_1^n|U_1^n}^T \otimes \Pi_{V_2^n|U_2^n}^T)P_{Y|V_1, V_2}^T\|_2 \leq \mu_1$, with the aid of triangular inequality, we obtain (40), as given on the next page. Based on $\sum_{m=1}^2 \|\Pi_{V_m^n|U_m^n} - I\|_2 \leq \delta$, (40) implies that

$$\begin{aligned} & \|P_{U_1, U_2}(\hat{\Pi}_{V_1^n|U_1^n}^T \otimes \hat{\Pi}_{V_2^n|U_2^n}^T)P_{Y|V_1, V_2}^T - P_{U_1, U_2}P_{Y|V_1, V_2}^T\|_2 \\ & \leq \mu + \mu_1 + \delta^2 |\mathcal{U}_1|^3 |\mathcal{U}_2|^3. \end{aligned} \quad (41)$$

The bound on the right-hand side of (41) can be made smaller than m of Lemma 4, provided that δ , μ_1 and μ are all sufficiently small. Thus, applying Lemma 4, we arrive at

$$D(Y^n) \leq (|\mathcal{U}_1|^2 + |\mathcal{U}_2|^2) \cdot F_{\min}^{-1} \left(\mu + \mu_1 + \delta^2 |\mathcal{U}_1|^3 |\mathcal{U}_2|^3 \right). \quad (42)$$

Finally, setting both μ_1 and μ to δ , (42) proves Property 2) of Theorem 1, where we have

$$\varepsilon(\delta) \triangleq (|\mathcal{U}_1|^2 + |\mathcal{U}_2|^2) F_{\min}^{-1} (2\delta + \delta^2 |\mathcal{U}_1|^3 |\mathcal{U}_2|^3),$$

which vanishes as δ decreases to 0.

B. Proof of Necessity of Theorem 1

We assume that the observation channel is manipulable, i.e., there exist Υ_1 and Υ_2 satisfying

- 1) $\sum_{m=1}^2 \|\Upsilon_m - I\|_2^2 > 0$,
- 2) For an arbitrary value of $m \in \{1, 2\}$, Υ_m is a stochastic matrix, and
- 3) $P_{U_1, U_2} \left(\bigotimes_{m=1}^2 \Upsilon_m \right)^T P_{Y|V_1, V_2}^T = P_{U_1, U_2} P_{Y|V_1, V_2}^T$.

Now, let us consider the following two cases:

- i) The relay m modifies its input symbols according to $P_{V_m|U_m} = \Upsilon_m$, where $m = 1, 2$, in an i.i.d manner. In order to avoid confusion, we use $\Pi'_{V_m^n|U_m^n}$ to represent the value of $\Pi_{V_m^n|U_m^n}$ obtained in such case, i.e., $\Pi_{V_m^n|U_m^n} = \Pi'_{V_m^n|U_m^n}$. Due to the i.i.d attack, we get $\Pi'_{V_m^n|U_m^n} \rightarrow P_{V_m|U_m}$ for $m = 1, 2$ according to the law of large numbers. Recall that $P_{V_m|U_m} = \Upsilon_m$, we get $\sum_{m=1}^2 \|\Pi'_{V_m^n|U_m^n} - I\|_2 > 0$ and

$$P_{U_1, U_2} \left(\bigotimes_{m=1}^2 P_{V_m|U_m} \right)^T P_{Y|V_1, V_2}^T = P_{U_1, U_2} P_{Y|V_1, V_2}^T. \quad (43)$$

- ii) Neither of the relays is malicious, i.e., $\Pi_{V_m^n|U_m^n} = I$ for $m = 1, 2$.

In both cases, Y^n is an i.i.d sequence, whose distribution only depends on the distribution of Y . In the case i), the distribution

of Y is $P_{U_1, U_2} \left(\bigotimes_{m=1}^2 P_{V_m|U_m} \right)^T P_{Y|V_1, V_2}^T$. In the case ii), the distribution of Y is $P_{U_1, U_2} P_{Y|V_1, V_2}^T$. From (43), we can see that the distributions of Y^n in both cases are exactly the same. Thus, any decision statistic $D(Y^n)$ has the same (conditional) distribution in the above-mentioned two cases. Nevertheless, in the case ii), since $\sum_{m=1}^2 \|\Pi'_{V_m^n|U_m^n} - I\|_2 = 0$, Property 2) of Theorem 1 requires that the probability of the event $\{D(Y^n) > \delta\}$ is arbitrarily small as long as δ is sufficiently small and n is sufficiently large. On the other hand, in the case i), by choosing δ that satisfies $\delta < \sum_{m=1}^2 \|\Pi'_{V_m^n|U_m^n} - I\|_2$, Property 1) of Theorem 1 requires that the probability of the same event $\{D(Y^n) > \delta\}$ is arbitrarily close to 1 as long as n is large enough. Hence, these two requirements lead to contradiction. Therefore, the necessity of Theorem 1 has been proved.

REFERENCES

- [1] L. Butyan and J.-P. Hubaux, *Security and Cooperation in Wireless Networks*, Cambridge University Press, 2007.
- [2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.
- [3] P. Papadimitratos and Z. J. Haas, “Secure data communication in mobile ad hoc networks,” *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 343–356, Feb. 2006.
- [4] Y. C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,” *Wirel. Netw.*, vol. 11, no. 1-2, pp. 21–38, Jan. 2005.
- [5] Y. Mao and M. Wu, “Tracing malicious relays in cooperative wireless communications,” *IEEE Trans. Inf. Forens. Security*, vol. 2, no. 2, pp. 198–212, Jun. 2007.
- [6] T. Khalaf, S. Kim, and A. Abdel-Hakim, “Tradeoff between reliability and security in multiple access relay networks under falsified data injection attack,” *IEEE Trans. Inf. Forens. Security*, vol. 9, no. 3, pp. 386–396, Mar. 2014.
- [7] L.-C. Lo, Z.-J. Wang, and W. J. Huang, “Noncoherent misbehavior detection in space-time coded cooperative networks,” in *Proc. IEEE Intl. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, Kyoto, Mar. 2012, pp. 3061–3064.
- [8] L.-C. Lo, W. J. Huang, R. Y. Chang, and W.-H. Chung, “Noncoherent detection of misbehaving relays in decode-and-forward cooperative networks,” *IEEE Comm. Letters*, vol. 19, no. 9, pp. 1536–1539, Sept. 2015.
- [9] T. Ho, B. Leong, R. Koetter, M. Médard, M. Effros, and D. R. Karger, “Byzantine modification detection in multicast networks with random network coding,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2798–2803, Jun. 2008.
- [10] O. Kosut, L. Tong, and D. Tse, “Nonlinear network coding is necessary to combat general Byzantine attacks,” in *Proc. 47th Annu. Allerton Conf. on Commun., Control, and Compu.*, Monticello, IL, Oct. 2009, pp. 593–599.
- [11] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Médard and M. Effros, “Resilient network coding in the presence of Byzantine adversaries,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2596–2603, Jun. 2008.
- [12] X. He, and A. Yener, “Strong secrecy and reliable Byzantine detection in the presence of an untrusted relay,” *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 177–192, Jan. 2013.
- [13] E. Graves and T. F. Wong, “Detection of channel degradation attack by intermediary node in linear networks,” in *Proc. IEEE Intl. Conf. Comput. Commun. (INFOCOM)*, Orlando, FL, Mar. 2012, pp. 747–755.
- [14] E. Graves and T. F. Wong, “Detectability of symbol manipulation by an amplify-and-forward relay,” in *arXiv preprint arXiv:1205.2681*, 2012.
- [15] E. Graves and T. F. Wong, “A coding approach to guarantee information integrity against a Byzantine relay,” in *Proc. IEEE Intl. Symp. Inf. Theory (ISIT)*, Istanbul, Jul. 2013, pp. 2780–2784.
- [16] S. W. Kim, “Physical integrity check in cooperative relay communications,” *IEEE Trans. on Wirel. Commun.*, vol. 14, no. 11, pp. 6401–6413, Nov. 2015.

$$\begin{aligned}
& \left\| P_{U_1, U_2} (\hat{\Pi}_{V_1^n | U_1^n}^T \otimes \hat{\Pi}_{V_2^n | U_2^n}^T) P_{Y|V_1, V_2}^T - P_{U_1, U_2} P_{Y|V_1, V_2}^T \right\|_2 - \left\| P_{U_1, U_2} (\Pi_{V_1^n | U_1^n}^T \otimes \Pi_{V_2^n | U_2^n}^T) P_{Y|V_1, V_2}^T - P_{U_1, U_2} P_{Y|V_1, V_2}^T \right\|_2 \\
& \leq \left\| P_{U_1, U_2} (\hat{\Pi}_{V_1^n | U_1^n}^T \otimes \hat{\Pi}_{V_2^n | U_2^n}^T) P_{Y|V_1, V_2}^T - P_{U_1, U_2} (\Pi_{V_1^n | U_1^n}^T \otimes \Pi_{V_2^n | U_2^n}^T) P_{Y|V_1, V_2}^T \right\|_2 \\
& \leq \left\| P_{U_1, U_2} (\hat{\Pi}_{V_1^n | U_1^n}^T \otimes \hat{\Pi}_{V_2^n | U_2^n}^T) P_{Y|V_1, V_2}^T - \Pi_{Y^n} \right\|_2 + \left\| P_{U_1, U_2} (\Pi_{V_1^n | U_1^n}^T \otimes \Pi_{V_2^n | U_2^n}^T) P_{Y|V_1, V_2}^T - \Pi_{Y^n} \right\|_2 \\
& \leq \mu_1 + \mu.
\end{aligned} \tag{40}$$

[17] R. Cao, E. Graves, T. F. Wong, and T. Lv, "Detecting substitution attacks against non-colluding relays," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Atlanta, GA, Dec. 2013, pp. 1856–1861.

[18] S. Dehnie, H. T. Sencar, and N. Memon, "Detecting malicious behavior in cooperative diversity," in *Proc. Conf. Inf. Science and Systems (CISS)*, Baltimore, MD, Mar. 2007, pp. 895–899.

[19] W. Hou, X. Wang, and A. Refaei, "Misbehavior detection in amplify-and-forward cooperative OFDM systems," in *Proc. IEEE Intl. Conf. Commun. (ICC)*, Budapest, 2013, Jun. 2013, pp. 5345–5349.

[20] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963.



Tiejun Lv (M'08-SM'12) received the M.S. and Ph.D. degrees in electronic engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 1997 and 2000, respectively. From January 2001 to January 2003, he was a Postdoctoral Fellow with Tsinghua University, Beijing, China. In 2005, he became a Full Professor with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications (BUPT). From September 2008 to March 2009, he was a Visiting Professor

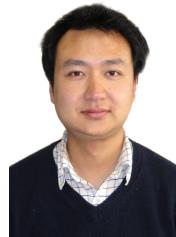
with the Department of Electrical Engineering, Stanford University, Stanford, CA, USA. He is the author of more than 200 published technical papers on the physical layer of wireless mobile communications. His current research interests include signal processing, communications theory and networking. Dr. Lv is also a Senior Member of the Chinese Electronics Association. He was the recipient of the Program for New Century Excellent Talents in University Award from the Ministry of Education, China, in 2006. He received the Nature Science Award in the Ministry of Education of China for the hierarchical cooperative communication theory and technologies in 2015.



Ruohan Cao received her B.Eng. degree in 2009 from Shandong University of Science and Technology (SDUST), Qingdao, China. She received the Ph.D. degree in 2014 from Beijing University of Posts and Telecommunications (BUPT), Beijing, China. From November 2012 to August 2014, she also served as a research assistant for the Department of Electrical and Computer Engineering at University of Florida, supported by the China Scholarship Council. She is now with the Institute of Information Photonics and Optical Communications, BUPT, as a Postdoc. Her research interests include physical-layer network coding, multiuser multiple-input-multiple-output systems and physical-layer security.



Tan F. Wong received the B.Sc. degree (first class honors) in electronic engineering from the Chinese University of Hong Kong in 1991 and the M.S.E.E. and Ph.D. degrees in electrical engineering from Purdue University in 1992 and 1997, respectively. He was a Research Engineer at the Department of Electronics, Macquarie University, Sydney, Australia. He also served as a Postdoctoral Research Associate at the School of Electrical and Computer Engineering, Purdue University. Since August 1998, he has been with the University of Florida, where he is currently a Professor of Electrical and Computer Engineering. Dr. Wong was the Editor for Wideband and Multiple Access Wireless Systems for the IEEE TRANSACTIONS ON COMMUNICATIONS and was the Editor-in-Chief for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He also served as an Associate Editor for the IEEE SIGNAL PROCESSING LETTERS.



Hui Gao S'10-M'13-SM'16) received his B. Eng. degree in Information Engineering and Ph.D. degree in Signal and Information Processing from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in July 2007 and July 2012, respectively. From May 2009 to June 2012, he also served as a research assistant for the Wireless and Mobile Communications Technology R&D Center, Tsinghua University, Beijing, China. From Apr. 2012 to June 2012, he visited Singapore University of Technology and Design (SUTD), Singapore, as a research assistant. From July 2012 to Feb. 2014, he was a Postdoc Researcher with SUTD. He is now with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications (BUPT), as an assistant professor. His research interests include massive MIMO systems, cooperative communications, ultra-wideband wireless communications.



Shaoshi Yang (S'09-M'13) received his B.Eng. degree in Information Engineering from Beijing University of Posts and Telecommunications (BUPT), Beijing, China in Jul. 2006, his first Ph.D. degree in Electronics and Electrical Engineering from University of Southampton, U.K. in Dec. 2013, and his second Ph.D. degree in Signal and Information Processing from BUPT in Mar. 2014. He is now working as a Postdoctoral Research Fellow in University of Southampton, U.K. From November 2008 to February 2009, he was an Intern Research

Fellow with the Communications Technology Lab (CTL), Intel Labs, Beijing, China, where he focused on Channel Quality Indicator Channel (CQICH) design for mobile WiMAX (802.16m) standard. His research interests include MIMO signal processing, green radio, heterogeneous networks, cross-layer interference management, convex optimization and its applications. He has published in excess of 30 research papers on IEEE journals.

Shaoshi has received a number of academic and research awards, including the prestigious Dean's Award for Early Career Research Excellence at University of Southampton, the PMC-Sierra Telecommunications Technology Paper Award at BUPT, the Electronics and Computer Science (ECS) Scholarship of University of Southampton, and the Best PhD Thesis Award of BUPT. He is a member of IEEE/IET, and a junior member of Isaac Newton Institute for Mathematical Sciences, Cambridge University, U.K. He also serves as a TPC member of several major IEEE conferences, including *IEEE ICC*, *GLOBECOM*, *VTC*, *WCNC*, *PIMRC*, *ICCVE*, *HPCC*, and as a Guest Associate Editor of *IEEE Journal on Selected Areas in Communications*. (<http://sites.google.com/site/shaoshiyang/>)