Evaluation of Security Robustness Against Information Leakage in Gaussian Polytree Graphical Models

Ali Moharrer, Shuangqing Wei, George T. Amariucai, and Jing Deng

***Abstract*—Extensive works have been undertaken to develop efficient statistical inference algorithms based on graphical models. However, there still lacks sufficient understanding about how topological properties affect certain information related metrics for certain graphs. In this paper, we are particularly interested in finding out how topological properties of rooted polytrees for Gaussian random variables determine its security robustness, which is measured by our proposed max-min information (MaMI) metric. MaMI is defined as the maximin value of the conditional mutual information between any two random variables (nodes) in a given DAG, conditioned on the value of a third random variable, which is at full disposal of an eavesdropper, under a constraint of a given fixed joint entropy. We show some general topological properties which the desired max-min solutions satisfy. Under such properties, we prove the superior max-min feature of the linear topology for a simple but non-trivial case. The results not only help us understand the security strength of different rooted polytree type DAGs, which is critical when we evaluate the information leakage issues for various jointly Gaussian distributed measurements in networks, but also provide us another algebraic and analysis perspective in grasping some fundamental properties of such DAGs.**

I. Introduction

Graphical models have been extensively studied and employed for statistical inferences. Their applications span over a vast amount of fields and topics including biology, social networks, computer science (such as network tomography methods), *etc*., to characterize the dependency relationships among multiple random variables [1]. In order to facilitate the representation of such relationships among random variables, special types of graphical models such as *Directed Acyclic Graphs* (DAGs) (*Bayesian networks*), and *Markov Random Fields* (MRFs) have been widely used. These models are essentially reflecting conditional independence relationships using directed or undirected graphs [2]. In order to characterize such relationships, one should have the knowledge of joint behavior of the users. The joint density $P(\boldsymbol{x})$ can be used to characterize such joint behavior, where $\boldsymbol{x} = \{x_1, x_2, ..., x_n\}$ is a vector of size n consisting all random variables. Given a DAG $G = (V, E)$, where $V = \{x_1, x_2, \cdots, x_n\}$ denotes the set of variables, and E is a set of directed edges, we can therefore factorize the joint density $P(\boldsymbol{x})$. The presence or absence of edges indicates the statistical dependency relationship among the associated vertices (random variables). In particular, $E = (i, j)$ is a directed edge if x_i is a direct cause of x_j [3].

Recently, some fundamental properties of Gaussian graphical models have drawn more attention and have been tackled using algebraic methods [4], [5]. In [4] the author shows that when the underlying random variables are Gaussian, conditional independence statements can be interpreted as algebraic constraints on the parameter space of the global model.

In this paper, we also attempt to study some salient properties of certain classes of DAGs related to security or privacy metrics. More specifically, we would like to evaluate a specific security metric defined as the *maximin* value of the conditional mutual information between any two random variables (nodes) in a given DAG, conditioned on the value of a third random variable. We assume that the third node is at full disposal of a passive eavesdropper who can select this variable from the remaining ones in the DAG. We could coin this metric as *max-min information* (MaMI) metric. Our goal is to seek and find certain topological properties for *rooted polytree* DAGs, representing joint distribution of Gaussian random variables so that we could infer the security robustness of each DAG in terms of the resulting max-min values under a constraint of a given fixed joint entropy. Such constraint provides a common ground on which we could fairly compare different topologies. With MaMI metric, we essentially provide a binary relationship to establish partial ordering among the same sized Gaussian rooted polytree models sharing the same determinant, *i.e.*, fixed joint entropy.

We anticipate that our results will be specifically useful in wireless sensor networks (WSNs) applications, in which given a particular topology of sensors, we want to choose the most informative set of sensors [6]. Under the attack by an eavesdropper, this in turn results in choosing sensors that are the most *secure*. Also, using our approach one can select the most *secure* polytree structures: by dividing a given set of DAGs into *Partially Ordered Sets* (POSETs) so that each subset contains a particular structure that is most secure in comparison with other structures in the same subset.

Our main contributions can be summarized as follows. First, we formulate a new problem that captures the security and privacy characteristics of polytree DAGs using the MaMI metric. Also, we prove in Lemma 1 that in order to solve the max-min problem, the triplets consisting of two random variables and an eavesdropper should follow a special structure. Next, for a simple but not a trivial case we prove that linear topology is most favorable in terms of our MaMI metric, and further demonstrate its validity using numerical results. Lastly, we provide a general principle on ordering the polytree

[1] A. Moharrer, and S. Wei are with the school of Electrical Engineering and Computer Science, Louisiana State University, Baton Rouge, LA 70803, USA (Email: amohar2@lsu.edu, swei@lsu.edu).

G. T. Amariucai is with the department of Electrical and Computer Engineering, Iowa State University, Ames, IA, USA (Email: gamari@iastate.edu).

J. Deng is with the department of Computer Science, University of North Carolina at Greensboro, Greensboro, NC, USA (Email: jing.deng@uncg.edu).

This work is funded in part by the National Science Foundation (NSF) under contract CIF-1320543.

structures.

The paper is organized as follows. Section II presents the system model. The main results of the paper are provided in Section III. We analyze the performance of 4-node polytree models in section IV. Section V gives the concluding remarks, and possible future works.

II. System Model

In order to find a valid representation, the joint density P and the underlying DAG $G = (V, E)$ should satisfy the *Markov* and *faithfulness* conditions, whose definition can be found in many existing works, e.g., [7].

Before describing the system model we will provide a definition for *d-separation* between nodes in DAGs [2].

Definition 1. *In the DAG G, a path between the two nodes x and y is open(active), given the set of vertices $\mathbf{Z} \subseteq E \backslash \{x, y\}$, if:*

• Every non-collider node on the path is not in $\mathbf{Z}$

• Every collider node on the path is either in $\mathbf{Z}$ or it is an ancestor of the specific node that is the member of $\mathbf{Z}$.

Two nodes x and y are d-separated by $\mathbf{Z}$ if there are no active paths between them.

In the above definition, the node v is said to be *collider*, if it is the outcome of at least two distinct parents: $(\rightarrow v \leftarrow)$. Otherwise, v is a *non-collider* node: $(\rightarrow v \rightarrow)$ or $(\leftarrow v \rightarrow)$.

Note that there is a significant difference between the collider and non-collider nodes. In particular, suppose that c is a non-collider, which is on the path of the nodes a and b: $(a \rightarrow c \rightarrow b)$ or $(a \leftarrow c \rightarrow b)$. First, observe that a and b are jointly dependent through their path. Second, it can be seen that conditioning on c blocks the path between a and b. In other words, learning b has no effect on the probability of a, given c [2]. On the other hand, suppose that c is a collider node that is the common outcome of the nodes a and b: $(a \rightarrow c \leftarrow b)$. In this case, the nodes a and b are marginally independent. However, if we condition on the node c, then they become conditionally dependent. This is also the case, if we condition on one of the possible descendants of the node c.

DAGs are the general models, which represent any joint density that satisfies both Markov and faithfulness conditions. In this paper, we consider a subset of DAGs known as *rooted polytree* models. In a rooted polytree, we have a single node that is the ancestor for all other nodes(the root node). Moreover, the polytree structures do not contain any cycles (either directed or undirected). Hence, polytree model can be seen as a tree structure with directed edges. As a result, there is exactly one path between any two different nodes. Note that since we have a single root, our model does not contain any colliders.

We will observe in section III that the polytree models include some nice structural properties that can be easily translated to our primary security question. Here, we use the conditional mutual information metric to measure the connection security between any pair of users, which is similar to the metric used in [8]. In particular, we model our scenario as a specific max-min problem.

Definition 2. *suppose we have an active connection between the users Alice and Bob. Also, we have the node Eve, which plays the eavesdropper role. In this problem the endpoint users, i.e., a and b choose their connecting path first. The node z picks its favorite position second. The endpoint users want to choose a path based on the pessimistic assumption that the eavesdropper chooses the best possible node, in terms of security: $\max_{\{a,b\}} \min_z I(a; b|z)$. On the other hand, the eavesdropper wants to make the connection more insecure. The higher values for the conditional mutual information $I(a; b|z)$ increases the security.*

A. Joint probability of the nodes: The Gaussian model

In this study, we consider the Gaussian joint density define the joint probability of users in a network, *i.e.*, $P_{\boldsymbol{\zeta}}(\zeta_1, \zeta_2, ..., \zeta_n) \sim N(\mu, \Sigma)$, where μ is the mean vector and Σ is the symmetric, positive-definite covariance matrix of n random variables. We believe that analyzing the connections' privacy given the general joint density, is a complex problem to solve. However, for the Gaussian joint density the analysis becomes tractable. Also, the algebraic analysis of Gaussian graphical models is considered in several papers [4], [5], and [9], whose results could be leveraged to look into our problems.

B. Independence relationships reflected in the covariance matrix entries

Let a and b be distinct elements chosen from the set of all nodes $\{1, ..., n\}$ and Z be a subset of $\{1, ..., n\} \backslash \{a, b\}$, then we can easily show the following conclusions [9].

• The random variables ζ_a and ζ_b are independent (denoted by $\zeta_a \perp \zeta_b$ or $\zeta_a \perp \zeta_b | \emptyset$) if and only if the (a, b)-th element (and also b, a) of Σ is zero.

• The random variables ζ_a and ζ_b are conditionally independent given $\boldsymbol{\zeta}_Z$ (denoted by $\zeta_a \perp \zeta_b | \boldsymbol{\zeta}_Z$) if and only if both determinant values, $|\Sigma_{aZ,bZ}| = |\Sigma_{bZ,aZ}|$ equal to zero, where $|\Sigma_{aZ,bZ}|$ is the submatrix of the covariance matrix Σ whose rows and columns are chosen from the subsets $a \cup Z$ and $b \cup Z$, respectively.

The latter claim uses the fact that if $\zeta_a \perp \zeta_b | \boldsymbol{\zeta}_Z$ then $(\Sigma^{-1})_{a,b} = (\Sigma^{-1})_{b,a}$ equals to zero. In other words, the conditional independence relation $\zeta_a \perp \zeta_b | \boldsymbol{\zeta}_Z$ holds if and only if $(\Sigma^{-1})_{a,b} = (\Sigma^{-1})_{b,a}$ equals to zero.

In the next sections we directly apply the results obtained above to extract algebraic equalities of the conditional independence relationships between random variables.

From now on for the simplicity of notations, instead of writing random variables and vectors we use their index. Hence, instead of using ζ_Z, we simply write Z to indicate the subset random vectors.

In a general DAG, there are many possible situations that every set of three nodes can have relation with each other. However, In a rooted polytree model these numerous cases will be reduced to a few general cases. In a rooted polytree, there is exactly one path between any two nodes. Also, the colliders do not appear in the structure.

In addition, for Gaussian random variables the conditional mutual information $I(a; b|z)$ can be directly related to the *partial correlation coefficient*, which is defined as below [10],

$$\rho^2_{ab|Z} = \frac{(\sigma_{ab} - \Sigma_{aZ}\Sigma^{-1}_{ZZ}\Sigma_{bZ})^2}{(\sigma_{aa} - \Sigma_{aZ}\Sigma^{-1}_{ZZ}\Sigma_{aZ})(\sigma_{bb} - \Sigma_{bZ}\Sigma^{-1}_{ZZ}\Sigma_{bZ})} = 1 - e^{-2I(a;b|Z)} \tag{1}$$

where $\sigma_{ab} = E[(a - \mu_a)(b - \mu_b)]$, the (a, b)-th element of Σ, is the covariance value between variables a and b. Also, Σ_{aZ} denotes the $a \times Z$ submatrix of Σ and $\Sigma^{-1}_{ZZ} = (\Sigma_{ZZ})^{-1}$ is the inverse of the $Z \times Z$ submatrix of the covariance matrix. We can see that the conditional mutual information is a monotone increasing function of the partial correlation coefficient. As we are seeking ordering of $I(a;b|Z)$, some results from [10] could be leveraged.

III. Main Result

We provide a lemma that shows the structural correspondence of the triplet (a,b,z) with respect to each other in the max-min problem. Here, using the results shown in [10] we will find an answer for the *maximin* problem. In particular, first using the information theoretic inequalities we will simplify the possible cases for $\min_z I(a;b|z)$. Second, we suggest an idea to simplify the possible cases for $\max_{\{a,b\}} I(a;b|z)$.

Lemma 1. *For any rooted polytree model with nodes that have the joint Gaussian density, the answer for $\max_{\{a,b\}} \min_z I(a;b|z)$ is the set of triples that a and b are adjacent, and the eavesdropper is neighbor to either a or b.*

Proof: We will use the following theorems directly, whose proofs can be found in [10].

Theorem 1. *Suppose $b' \perp a|bZ$, then $\rho^2_{ab'|Z} \leq \rho^2_{ab|Z}$*

Theorem 2. *Suppose for some x, $a \perp b|x$ and $ab \perp z|x$. Then $\rho^2_{ab|Z} \leq \rho^2_{ab}$. In addition, if $ab \perp z'|z$, then $\rho^2_{ab|Z} \leq \rho^2_{ab|Z'} \leq \rho^2_{ab}$*

Theorem 1 is a conditional version of the well-known information inequality and holds in general for mutual information of any distribution [11]. Intuitively, for the polytree model the condition in Theorem 1 is satisfied when b lies on the path between a and b'. In other words, the longer path implies weaker dependence. On the other hand, Theorem 2 holds in general for the Gaussian joint density. The first part of Theorem 2 shows that if a, b, and z are pairwise separated given x, then conditioning always reduces the mutual information between a and b. For the polytree models, the second part of the theorem 2 shows that for the fixed correlates a and b, the eavesdropper z wants to be closer to the path between them.

Figure 1 shows all the possible cases that a particular eavesdropper can take, in a fixed path between the nodes a and b. Note that there might be several steps between any pair of nodes. Also, we don't show the arrows (cause and effect) in the figure. Any arrow head is valid for this model, as long as we do not produce any colliders.

From this figure we can see that there are totally four possible locations for z: When z is connected to the path p_{ab} through one of the nodes a or b; when z is connected to p_{ab} through the node x; and when z lies on the path between a and b.

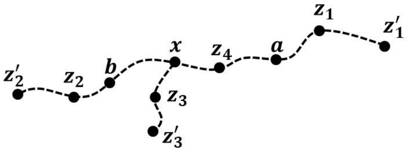


Fig. 1: All the possible locations for the eavesdropper given the fixed correlates

Recall that the objective is to find the value for z that minimizes the mutual information between a and b: $\min_z I(a;b|z)$.

Cases 1 and 2. When z is along the path p_{ab}, i.e., the case z_1 or z_2: First, consider the case z_1, the analysis for z_2 is exactly the same. From Theorem 1 we know that because $a \perp z'_1|z_1$ we have: $I(b;z_1) \geq I(b;z'_1)$. Now we want to compare two values for the mutual information. First, observe that $b \perp z_1|a$. In other words, b and z_1 are *d-separated* given a. Therefore, knowing z_1 does not change the probability for b, given a. So we can conclude that $I(b;a,z_1) = I(b;a)$. The same condition holds for z'_1: $I(b;a,z'_1) = I(b;a)$.

$$\begin{aligned}
&I(b;z_1) > I(b;z'_1) \rightarrow \\
&I(b;a) - I(b;z_1) < I(b;a) - I(b;z'_1) \rightarrow \\
&I(b;a,z_1) - I(b;z_1) < I(b;a,z'_1) - I(b;z'_1) \rightarrow \\
&I(b;a|z_1) < I(b;a|z'_1)
\end{aligned} \tag{2}$$

Eq. (2) shows that $I(a;b|z_1) \leq I(a;b|z'_1)$. In other words, the eavesdropper wants to be as close as possible to the path p_{ab}.

Case 3. Now consider the case when z is a branch node, i.e., it is connected to p_{ab} through the node x: It is obvious that by replacing z_3 with z and z'_3 with z' in the Theorem 2's conditions, we can satisfy all the constraints in this theorem. Hence, we can conclude that $I(a;b|z_3) \leq I(a;b|z'_3)$. Again, we conclude that z wants to be closer to the path p_{ab}.

Case 4. When z lies on the path p_{ab}: In this case it is obvious that $a \perp b|z_4$. In other words, z_4 *d-separates* a and b. As a result we have $I(a;b|z_4) = 0$.

Before moving on to the next part of the proof, consider the following remarks:

- In cases 1, 2 and 3, we concluded that the eavesdropper wants to be as close as possible to the p_{ab}.
- Obviously, the case 4, where z lies on the path p_{ab} is the worst case scenario, in which two endpoint nodes should prevent it from happening.

Next, we find possible cases that maximizes the mutual information between a and b, given the fixed node for z: $\max_{(a,b)} I(a;b|z)$. We want to show that to maximize the conditional mutual information, a and b should be closer to each other. Consider the case where $a \perp b'|bZ$, *i.e.*, given the subset of nodes bZ, a is independent of b'. Using the data processing inequality [11], we have $I(a;b|Z) \geq I(a;b'|Z)$.

For the polytree models, we can develop an intuition for this result. In a polytree model, if the node c is in the path between a and c', then conditioned on any subset of variables, we have $I(a;c|Z) \geq I(a;c'|Z)$. Hence, we can immediately pick the pair of nodes that are adjacent. Also, it can be argued that if a and b are not adjacent, then the eavesdropper wants to pick the best node: z picks any node on the path p_{ab}. As a result $I(a;b|z)$ becomes zero. ■

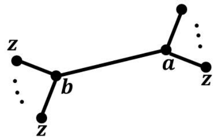


Fig. 2: The Final Set of Triplets in a Maximin Scenario

Figure 2 shows the final set of candidates for any maximin scenario in a rooted polytee models. The edges in the figure can have any direction, as long as they don't produce any colliders.

While the result stated in Lemma 1 might seem intuitive, we will provide an example to show that this result does not hold in structures that have colliders.

Example 1. *Consider the structure shown in figure 3. Note that in this structure, the node a is the only collider. We want to compare the cases that eavesdropper picks either z_1 or z_2. From the figure, we have $z_2 \perp b|z_1a$. Hence, from Theorem 1 we conclude that $I(b;z_2|a) < I(b;z_1|a)$. We simply have $I(b;a,z_2) < I(b;a,z_1)$. Since the node a is collider, we have $I(b;z_1) = I(b;z_2) = 0$. As a result $I(b;a,z_2) - I(b;z_2) < I(b;a,z_1) - I(b;z_1)$. Finally, we can attain the result $I(b;a|z_2) < I(b;a|z_1)$. In other words, in this case the eavesdropper picks a farther node to reduce the mutual information between a and b.*

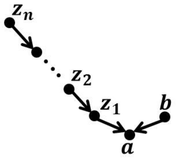


Fig. 3: Counter Intuitive Example: The Collider Case

We can simply, generalize this result and show that $I(a;b|z_1) > I(a;b|z_2) > ... > I(a;b|z_n)$. Hence, the eavesdropper picks the farthest node to the path p_{ab}.

Obviously, since the rooted polytrees do not contain the colliders, the situations like the case shown in Example 1 do not happen in our model of interest.

IV. Security Comparison: 4-Node Case

Recall that our goal is to find certain topological properties for rooted polytree structures, representing joint distribution of Gaussian random variables so that we could infer the strength of each topology in terms of the resulting max-min values under a constraint of a given fixed determinant. Determinant of Σ affects the entropy of the users. In particular, for a model with joint Gaussian density we have $H = 1/2 \log |2\pi e \Sigma|$. Roughly speaking, this condition makes the users in both models to have the same joint randomness.

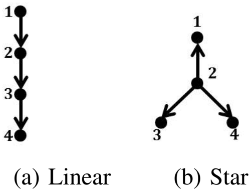
Definition 3. *Suppose we are given two rooted polytrees T_n and T'_n, with the same joint entropy for their variables. Given the same covariance values between all the adjacent nodes on both structures, we say that T_n is more secure than T'_n shown by a binary relationship $T_n \succeq T'_n$, whenever the resulting max-min value for T_n is always larger (or equal) than the max-min value for the polytree T'_n.*

The problem of comparing the security of any general polytree model is computationally complex. In particular, the number of variables involving in a covariance matrix of T_n is $n(n+1)/2$. In other words we have $n(n+1)/2$ degrees of freedom (DoF) for this graph. As n grows, the number of DoF becomes very large, and makes the analysis complicated. Hence, we will provide the analysis for simpler case, i.e., the polytrees consisting of 4 nodes. The analysis for the independence models that are Gaussian representable is done in [9]. Even for a four node tree, the covariance matrix consists of $4(4+1)/2 = 10$ variables. To better understand the impact of correlations between users and also observing the influence of tree structure on security, we would rather decrease the number of DoFs by introducing more constraints on the covariance matrix. Similar to [9], by normalizing the diagonal entries in the covariance matrix we will obtain $10 - 4 = 6$ variables. As we will see, the security analysis for this special case is not trivial. In contrast, it has some nice intuitions behind it, which becomes the basis for the performance analysis of more general cases. Moreover, the normalization of diagonal entries does not change the dependency relations in graph. We can always change the diagonal entries by multiplying the covariance matrix Σ, with the diagonal matrix J: $\Sigma' = J\Sigma J$. The diagonal entries of J are $1/\sqrt{\sigma_{vv}}$, $\forall v \in V$, where V is the set of users. Note that because Σ is positive definite, all the off-diagonal elements in the covariance matrix are in the range $(-1, 1)$. The corresponding covariance matrix follows the form below,

$$\Sigma = \begin{pmatrix} 1 & a & b & c \\ a & 1 & d & e \\ b & d & 1 & f \\ c & e & f & 1 \end{pmatrix} \tag{3}$$

We used [5] to find all the possible isomorphism classes of rooted polytree models on 4 nodes. The results are shown in figure 4. Note that in a rooted polytree model we are not allowed to use colliders.

In [5], the authors show that the two models $A \rightarrow B \rightarrow C$ and $B \leftarrow A \rightarrow C$ are *isomorphic*. In other words, after some appropriate relabeling of the nodes, both models describe the same collection of joint distributions $P(A, B, C)$. As a result, if we change the direction of the edge between nodes 1 and 2 in any structure shown in figure 4, we will obtain the same set of (conditional) independence relationships as before. Thus, we are facing two possible structures for the polytree models including 4 nodes: the *linear* (string) and *star* structures.



(a) Linear (b) Star

Fig. 4: The isomorphism classes of rooted polytrees on four nodes

In order to make a fair comparison between these two models, we fix the determinant of Σ. In other words, for both structures we have: $|\Sigma| = k$.

Next, we can compute σ_{ij}, *i.e.*, the covariance between the users i and j. We will simplify the Eq. (1) for the triplet a, b and the eavesdropper z:

$$\rho^2_{ab|z} = \frac{\sigma^2_{ab}(1 - \sigma^2_{bz})}{1 - \sigma^2_{ab}\sigma^2_{bz}} \tag{4}$$

A. Linear structure: The max-min table

Consider the linear topology on 4 nodes. Through the analysis of conditional independences between different nodes in this network, we know that $1 \perp 3|2$, $1 \perp 4|2$, and $2 \perp 4|3$. These conditions make the covariance matrix Σ to have some

TABLE I: Maximin table for the string model

$\{a;b\}$	z	$\rho^2_{ab\|z}$
$\{1;2\}$	3	$\frac{A(1-D)}{1-AD}$
$\{2;3\}$	1 or 4	$\frac{D(1-A)}{1-AD}$ or $\frac{D(1-F)}{1-DF}$
$\{3;4\}$	2	$\frac{F(1-D)}{1-DF}$

TABLE II: Maximin values and their corresponding regions in linear model

$\rho^2_{ab\|z}$	Boundries	Region Number
$\rho^2_{12\|3}$	$A > D,\ A > F$	R_1
$\rho^2_{23\|1}$	$D > A > F$	R_2
$\rho^2_{23\|4}$	$D > F > A$	R_3
$\rho^2_{34\|2}$	$F > A,\ F > D$	R_4

restrictions on its elements. In particular, we have $a \times d = b$, $a \times e = c$, and $d \times f = e$. Using these constraints, we can conclude the expression for $|\Sigma|$:

$$|\Sigma| = -(a^2-1)(d^2-1)(f^2-1) = k \qquad (5)$$

where, using Eq. (3) we conclude that $\sigma_{12} = a$, $\sigma_{23} = d$, and $\sigma_{34} = f$.

Using Lemma 1, we can conclude Table I for the max-min table of the linear structure. The last column shows the expressions for different partial correlation coefficients.

Next, we want to consider all the possible relations between a, d, and f to find the *maximin* value.

Let us define $A = a^2$, $D = d^2$, and $F = f^2$. Note that $F = 1 - k/(1-A)(1-D)$, where $k = |\Sigma|$. Let's Consider the following case:

Region 1. *$A > D$ and $A > F$: Then using table I it is easy to show that $\rho^2_{23|1} < \rho^2_{23|4}$. Hence, we can simplify the corresponding row. Now, we should find the maximin value. As a result we want to find the maximum value for the partial correlation coefficient. Again, it is straightforward to show that $\rho^2_{12|3} > \rho^2_{23|1}$ and $\rho^2_{12|3} > \rho^2_{34|2}$. Hence, the maximin value in this case is $\rho^2_{12|3}$.*

Similarly using Table I we can find the regions for all the maximin values. Table II shows these results.

B. Star structure: The max-min table

Consider the star topology on 4 nodes. For the conditional independence relations we have: $1 \perp 3|2$, $1 \perp 4|2$, and $3 \perp 4|2$. As a result we conclude that $a \times d = b$, $a \times e = c$, and $e \times d = f$. Similarly, in this case the determinant expression becomes as follows:

$$|\Sigma| = -(a^2-1)(d^2-1)(e^2-1) = k \qquad (6)$$

Similarly, using the results for the previous section, we can conclude table III for the max-min table of star structure.

Next, we want to consider all the possible relations between a, d, and e to find the *maximin* value of table III. Again, let us define $A = a^2$, $D = d^2$, and $E = e^2$. Here, E in the star structure has the same value as the F in the linear structure. Similar to the linear case, we can obtain Table IV for this case.

TABLE III: Maximin table for the star model

$\{a;b\}$	z	$\rho^2_{ab\|z}$
$\{1;2\}$	3 or 4	$\frac{A(1-D)}{1-AD}$ or $\frac{A(1-E)}{1-AE}$
$\{2;3\}$	1 or 4	$\frac{D(1-A)}{1-(AD}$ or $\frac{D(1-E)}{1-DE}$
$\{2;4\}$	1 or 3	$\frac{E(1-A)}{1-AE}$ or $\frac{E(1-D)}{1-ED}$

TABLE IV: Maximin values and their corresponding regions in star model

$\rho^2_{ab\|z}$	Boundries	Region Number
$\rho^2_{12\|3}$	$A > D > E$	R_1
$\rho^2_{12\|4}$	$A > E > D$	R_2
$\rho^2_{23\|1}$	$D > A > E$	R_3
$\rho^2_{23\|4}$	$D > E > A$	R_4
$\rho^2_{24\|1}$	$E > A > D$	R_5
$\rho^2_{24\|3}$	$E > D > A$	R_6

C. Plotting the max-min values for both structures

Here, we want to plot the answers for all of the cases above, for both linear and star structures. Recall that in both models we have two degrees of freedom. Let us choose A and D as DoFs. We want to compute $\rho^2_{ab|z}$ for all the values of A and D. Note that both A and D are in the interval $(0, 1-k)$, where $k = |\Sigma|$. Also, we have the Eqs. (5) and (6) as the constraints. Figure 5 shows the heatmap for both models. From this model we can observe that in some regions the string structure have larger values for the mutual information. We prove this observation in the next lemma.

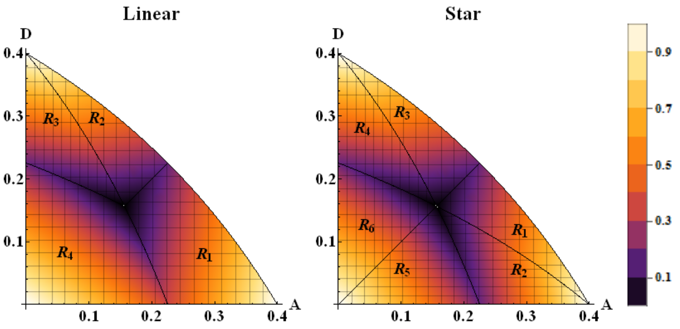


Fig. 5: The heatmap for different values of correlation coefficient $\rho^2_{ab|z}$ in both structures ($k = 0.6$)

Lemma 2. *We always have Linear $\succeq$ Star: the linear structure always produces larger maximin values than the star structure. Therefore, the linear model is more secure than the star model.*

Proof: By considering tables I and III it is easy to observe that in several regions the partial correlation is exactly the same in both models, *i.e.*, in regions R_1, R_3, R_4, and R_6 of the star model and their corresponding areas in the linear model heatmap. In two regions the linear structure outperforms the star structure. We will prove this conclusion for one of the regions. The proof for the other case is exactly the same.

Case 1. *In region R_5 ($E > A > D$) the maximin value for* *the star model is computed using the triplet* $(2,4,1)$. *Hence, the maximin value is computed using* $\rho^2_{24|1}$. *We can see from the figures that* R_4 *is the only region in linear model that has an intersection with* R_5 *in the star model. The intersection happens in* $F > A > D$ *region. The maximin value for the linear model is computed using* $\rho^2_{34|2}$. *Thus, We need to show that* $\dfrac{E(1-A)}{1-EA} < \dfrac{F(1-D)}{1-FD}$. *Observe that* $E = F$. *Since* $A > D$, *the result follows.*

The proof for the other case is similar. ■

D. Ordering rooted polytrees: the general principle

Next, using the insight we obtained from the 4-node polytree models, we want to prove the similar results for more general cases. By comparing linear and star structures on 4 nodes, we can see that the only difference between two structures is that in linear case the node 2 is adjacent to nodes 1 and 3; However in the star model the node 2 is adjacent to nodes 1, 3, and 4. Loosely speaking, in linear model by moving node 4 and connecting it to node 2 we obtain the star model. In the following lemma, we show that this operation always reduces the security of the polytree models. In particular, we consider two polytrees T_n and T'_n. The polytree T_n might have any structure with n vertices. On the other hand, T'_n is obtained from T_n by cutting a special edge and connecting it to its grandparent. The following lemma shows the result.

Lemma 3. *Consider a general rooted polytree model* T_n *having* n *nodes. Let's assume that* T_n *has at least one leaf node* (v) *that has a parent with no other child, i.e.,* v *has no siblings. Now, if we remove* v *and connect it to its grandparent (the parent of the parent of* v*), we obtain the polytree* T'_n. *We always obtain* $T_n \succeq T'_n$.

Proof: Because of the space limit we only provide an outline of the proof.

First, by induction we show that the number of DoFs is the same for any polytree structure with n nodes. For any general model with n nodes, and given a fixed value for the determinant of covariance matrix, the number of DoFs is $n-2$.

Second, by induction we prove that for any rooted polytree model, the determinant of the covariance matrix with normalized diagonal entries has the following form: $|\Sigma_{n\times n}| = \prod_{i=1}^{n-1}(1-\sigma^2_{e_i}) = k$. Here, σ_{e_i} is the covariance value between two adjacent nodes that are connected by e_i. Using this part of the proof we can conclude that if we cut a single leaf node and connect it to any other node, the covariance between this node, and its new parent remains the same as before.

Finally, we should write the max-min table for both polytrees. Both tables have the same entries in most parts. The only differences happen around the rows that relate to the old and new parents. In other words, under the same values for DoFs of both structures, we can show that the operation changes the local elements in the covariance matrix, and also in the max-min tables. The idea is to compare these special cases and show that if the maximin value occurs in these parts, we can always show that $T_n \succ T'_n$. Otherwise the max-min value for both structures is equal. ■

V. Conclusion

In this paper, we have studied the impact of changing the topology of DAGs on connections' security. We have used rooted polytree structures to model the network topology. under the joint Gaussian density we have proposed the max-min strategy over all the possible triplets (a, b, z) to measure the security of connections. The analysis has shown that in the final set of triplets the nodes a and b should be neighbors, and the eavesdropper is adjacent to one of them. We have used this general criterion to find the best possible structure in a rooted polytree model with 4 nodes, where we have proved that the linear polytree always dominates the star structure. Finally, we have introduced an operation that can be applied to any rooted polytree structure. We have shown in Lemma 3 that this operation always decreases the maximin value of the resulting polytree. Using this operation, we can also fully order all rooted polytrees with 5 nodes for those identified equivalent isomorphic classes in [5], and further show that linear topology is still the most favorable one using the MaMI metric, as in the case of 4 nodes in this paper. Also, by using this operation repeatedly, we can construct all equivalence classes of rooted polytrees that are partially ordered using the binary operation introduced in this paper, which further helps us to compare different topologies in terms of security robustness. The results will be presented in our future works [12].

References

[1] M. J. Wainwright and M. I. Jordan, "Graphical models, exponential families, and variational inference," *Foundations and Trends® in Machine Learning*, vol. 1, no. 1-2, pp. 1–305, 2008.

[2] J. Pearl, "Causality. 2000," *Cambridge University, New York.*

[3] T. S. Verma and J. Pearl, "Causal networks: Semantics and expressiveness," *arXiv preprint arXiv:1304.2379*, 2013.

[4] S. Sullivant, "Algebraic geometry of Gaussian Bayesian networks," *Advances in Applied Mathematics*, vol. 40, no. 4, pp. 482–513, 2008.

[5] H. Roozbehani and Y. Polyanskiy, "Algebraic methods of classifying directed graphical models," *arXiv preprint arXiv:1401.5551*, 2014.

[6] A. Krause and C. E. Guestrin, "Near-optimal nonmyopic value of information in graphical models," *arXiv preprint arXiv:1207.1394*, 2012.

[7] P. Spirtes, C. N. Glymour, and R. Scheines, *Causation, prediction, and search.* MIT press, 2000, vol. 81.

[8] U. M. Maurer, "Secret key agreement by public discussion from common information," *Information Theory, IEEE Transactions on*, vol. 39, no. 3, pp. 733–742, 1993.

[9] P. Šimecek, "Gaussian representation of independence models over four random variables," in *COMPSTAT conference*, 2006.

[10] S. Chaudhuri, "Qualitative inequalities for squared partial correlations of a Gaussian random vector," *Annals of the Institute of Statistical Mathematics*, vol. 66, no. 2, pp. 345–367, 2014.

[11] T. M. Cover and J. A. Thomas, *Elements of information theory.* John Wiley & Sons, 2012.

[12] A. Moharrer, S. Wei, G. Amariucai, and J. Deng, "Relationships between topological properties and algebraic structures for Gaussian rooted polytrees under maxmin information metric," *under preparation.*