On Targeted Entity Hardening Problem in Multi-layered Interdependent Networks

Joydeep Banerjee, Chenyang Zhou, and Arunabha Sen
School of Computing, Informatics and Decision System Engineering
Arizona State University
Email: {jbanerje, czhou24, asen}@asu.edu

Abstract—Critical infrastructures like power and communication networks are highly interconnected. Hence it is imperative to have an accurate model that captures these interdependencies. A number of models were proposed but each has their own limitations. Some limitations of the existing models were addressed by the Implicative Interdependency Model which uses Boolean Logic to represent these interdependencies. In this paper, we study the Targeted Entity Hardening problem. Some entities in an interdependent network might have a higher priority to be protected from failure. This can be achieved by hardening a set of entities. A hardened entity is assumed to have the capacity to remain operational on being attacked by any kind of adversary. But hardening an entity would usually entail a high cost. So it is essential to minimize the number of hardened entities which would protect all entities in the higher priority set from failure. We study this problem utilizing the Implicative Interdependency Model. We provide a polynomially solvable restricted case and prove that the problem is NP-complete. An Integer Linear program is provided to obtain the optimal solution. A heuristic is proposed whose efficacy is judged by comparing it with the optimal solution using real world data.

Keywords—Interdependent Network, Entity Hardening, Targeted Entity Hardening, Power Network, Communication Network

I. INTRODUCTION

A nation’s critical infrastructures (like power, communication, transportation networks) are heavily interdependent on each other for their functionality. As an example the power grid and communication network engage in a heavy symbiotic relationship among each other. To explain this dependency consider entities in power network such as Supervisory Control and Data Acquisition System (SCADA). The SCADA systems primarily control the electricity generation and flow in the power grid. These controls are essentially carried out by signals from the communication network. On the other way round every entity in the communication network require power to be operational. These dependencies causes failure in any of these two network to have its impact on the other which may eventually lead to cascade of failures. The initial failure of entities in either network are driven by their vulnerability to nature induced and man made (terrorist attack, cyber-attack) failure. Failures in power or communication network have disastrous effects (as seen in power blackouts which occurred in New York (2003) and India (2012)

This topic is important in communication network perspective in the same way it is for power grid. Owing to the dependencies stated above, the working of the communication network can get affected due to failures in power network. Previous work on this topic has also been accepted in communication conference (GLOBECOM). Hence it can be claimed that modeling and analysis of interdependent power-communication network is relevant among communication network research community.

Modeling these complex interdependencies and analysis of failure in these infrastructures are considered to be highly important. A number of models have been proposed that capture these interdependencies. However each of these models have their own shortcomings in bringing out the complex nature of the interdependencies that might exist. Authors in [12] brought out the need to address the complex interdependency which can explained through the following example. Let \( a_x \) (which can be a generator, substation, transmission line etc.) be a power network entity and \( b_w, b_y, b_z \) (which can be a router, end system etc.) a set of communication network entities. Consider the dependency where the entity \( a_x \) is operational if (i) entities \( b_w \) and (logical AND) \( b_y \) are operational, or (logical OR) (ii) entity \( b_z \) is operational. Models in [3], [5], [4], [6], [7], [8], [9], [10] fails to capture this kind of interdependency. Owing to the above nature of dependencies, graph based models might lack the capacity to represent the same. Motivated by these findings and limitations of the existing models, the authors in [12] proposed a Boolean logic based dependency model termed as Implicative Interdependency Model (IIM). For the example stated above the dependency of \( a_x \) on \( b_w, b_y, b_z \) can be represented as \( a_x \leftarrow b_w b_y + b_z \). This equations representing the dependency of an entity is termed as Interdependency Relation (IDR). Using this model a number of problems were studied on interdependent power and communication infrastructure system [12], [13], [14], and [15]. The Targeted Entity Hardening problem discussed in this article is a restricted version of the Entity Hardening Problem [14]. We use IIM to study this problem with respect to interdependent power and communication network.

An entity \( x_i \) when hardened is resistant to both initial and induced (failing of entities in the cascading process) failures. In physical world an entity can be hardened with respect to cyber attacks (say) by having strong firewall. Similarly some entities can be hardened by strengthening their physical structures for protection from natural disaster. There exist multiple such ways to harden an entity from different kind of failures. Even though there may be circumstances under which an entity cannot be hardened, in this paper we relax such possibilities and assume that there always exist a way to harden a given entity.

For a positive integer \( K \) consider the most vulnerable set of \( K \) entities [12] are known. Initial failure of these vulnerable entities would maximize the total number of failed entities (through induced failure) in the interdependent network. The Entity Hardening Problem [14] takes as input an interdependent network, the set of \( K \) vulnerable entities and a budget \( H \) on the number of entities that can be hardened. With these \( K \) vulnerable entities failing initially, the problem finds a set of \( H \) entities which when hardened minimizes the cardinality of the final failure set.

For an interdependent power and communication infrastructure certain entities might have higher priority to be
protected. There might exist entities whose non-functionality poses higher economic or societal damage as compared to other entities. For example, power and communication network entities corresponding to office buildings running global stock exchanges, transportation sectors like airports etc. presumably are important to have higher protection. Let $F$ denote the failed set of entities (including initial and induced failure) when the $K$ most vulnerable entities fail initially. We define a set $P$ (with $P \subseteq F$) of entities which have a higher priority to be protected. $P$ contains all those entities which have a higher priority to be protected. The Targeted Entity Hardening problem finds the minimum set of entities which when hardened would ensure that none of the entities in set $P$ fail. In our initial attempt to solve this problem we consider a restricted class of IDRs. For this setting the problem can be solved optimally in polynomial time and an algorithm solving the same is provided. However the problem is found to be NP-complete for IDRs in general form. Owing to the hardness we provide an Integer Linear Program that solves the problem optimally and a non optimal heuristic with the optimal solution.

II. IMPLICATIVE INTERDEPENDENCY MODEL AND PROBLEM FORMULATION

In this section we describe the IIM model [12]. An inter-dependent network is represented as $I(A, B, \mathcal{F}(A, B))$ with $A$ being the set of entities in power network, $B$ representing the set of entities in communication network and the function $\mathcal{F}(A, B)$ consisting of the IDRs that capture the dependencies between these two networks. Consider an example where the set $A$ and $B$ consist of entities $\{a_1, a_2, a_3\}$ and $\{b_1, b_2, b_3, b_4\}$ respectively. The function $\mathcal{F}(A, B)$ giving the set of dependency equations are provided in Table I. In the given example, an IDR $b_3 \leftarrow a_2 + a_4 a_3$ implies that entity $b_3$ is operational if entity $a_2$ or entity $a_1$ and $a_3$ are operational. In the IDRs each conjunction term e.g. $a_4 a_3$ is referred to as minterms. It is also to be noted that the IDRs can have dependencies between entities in the same network.

| Power Network | Comm. Network |
|---------------|---------------|
| $a_1 \leftarrow b_2$ | $b_1 \leftarrow a_1 + a_2$ |
| $a_2 \leftarrow b_2$ | $b_2 \leftarrow a_1 a_2$ |
| $a_3 \leftarrow b_4$ | $b_3 \leftarrow a_2 + a_4 a_3$ |
| $a_4 \leftarrow b_4$ | $b_4 \leftarrow a_3$ |

TABLE I: IDRs for the constructed example

Initial failure of entities in $A \cup B$ would cause the failure to cascade until a steady state is reached. The event of an entity failing after the initial failure is termed as induced failure. The cascade is assumed to occur in time steps of unit length. Each time step captures the effect of entities killed in all previous time steps. We demonstrate the cascading failure for the interdependent network outlined in Table I through an example. Consider that the entity $a_2$ and $a_3$ fail at time step $t = 0$. Table I] represents the cascade of failure in each subsequent time steps. In Table I] for a given entity and time step, ’0’ represents the entity is operational and ’1’ non operational. In this example a steady state is reached at time step $t = 3$ when all entities are non operational. The IIM model also assumes that the dependent entities of all failed entities are killed immediately at the next time step. For example at time step $t = 1$ entities $a_2$, $a_3$, $b_2$, $b_3$ and $b_4$ are non operational. Due to the IDR $a_1 \leftarrow b_2$ entity $a_1$ is killed immediately at time step $t = 2$. At $t = 3$ the entity $b_1$ is killed due to the IDR $b_1 \leftarrow a_1 + a_2$ thus reaching the steady state. It can be followed that with $K = 2$, $\{a_2, a_3\}$ represents a set of 2 vulnerable entities.

| Entities | Time Steps (t) |
|----------|---------------|
| $a_1$    | 0 1 2 3 4 5   |
| $a_2$    | 0 0 1 1 1 1   |
| $a_3$    | 1 1 1 1 1 1   |
| $b_1$    | 0 0 0 0 1 1   |
| $b_2$    | 0 1 1 1 1 1   |
| $b_3$    | 0 1 1 1 1 1   |
| $b_4$    | 1 1 1 1 1 1   |

TABLE II: Failure cascade propagation when entities $\{a_2, a_3\}$ fail at time step $t = 0$. A value of 1 denotes entity failure, and 0 otherwise.

Before describing the problem in IIM setting we note some of the challenges in modeling the IDRs. The main challenge is accurate formulation of the IDRs. Two possible ways of doing this would be (i) careful analysis of the underlying infrastructures as in [10], (ii) consultation with domain experts. The formulation of IDRs from the interdependent network is an ongoing research and the problem is solved under the assumption that these IDRs can be developed.

With this example we develop the notion implied by the Targeted Entity Hardening (TEH) problem. As mentioned earlier, when an entity $x_i \in A \cup B$ is hardened then it is protected from both initial and induced failure. Consider the problem where we have to choose minimum number of entities to harden such that at least the entity $\{b_4\}$ is protected from failure. With $\{a_2, a_3\}$ being the two vulnerable entities, hardening entity $a_2$ (with $a_3$ failing) would prevent failure of entities $a_1, a_3, b_1, b_3$. Similarly hardening the entity $a_3$ (with $a_2$ failing) would prevent the failure of entity $b_4$. Even though hardening $a_2$ prevent failure of more entities than hardening $a_3$, owing to the problem description $a_3$ has to be hardened which is a solution to the TEH problem in this scenario. It is to be noted that other entities might also be protected from failure when a set of entities are hardened to protect a given set of entities.

The TEH problem is formally stated below accompanied with a descriptive diagram provided in Figure [1].

INSTANCE: Given:
(i) An interdependent network system $I(A, B, \mathcal{F}(A, B))$, where the sets $A$ and $B$ represent the entities of the two networks, and $\mathcal{F}(A, B)$ is the set of IDRs.
(ii) The set of $K$ most vulnerable entities of the system $A' \cup B'$, where $A' \subseteq A$ and $B' \subseteq B$. 
(iii) The set $F \subseteq A \cup B$ contains all the entities failed due to initial failure of $A' \cup B'$ entities.
(iv) A positive integer $k$ and $k < K$.
(v) A set $P \subseteq F$.

DECISION VERSION: Is there a set of entities $H = A'' \cup B''$, $A'' \subseteq A$, $B'' \subseteq B$, $|H| \leq k$, such that hardening $H$ entities would result in protecting all entities in the set $P$ after entities $A' \cup B'$ fails at the initial time step.

OPTIMIZATION VERSION: Find the minimum set of entities in $A \cup B$ to harden that would result in protecting all entities in the set $P$ after entities $A' \cup B'$ fails at the initial time step.

The TEH problem solutions are based on the following assumptions — (i) A hardened entity is always operational and at any given time step it does not fail, even if the entity belongs to the $K$ most vulnerable set of entities, (ii) the condition $k < K$ is assumed as with $k \geq K$ hardening the
Fig. 1: Figure describing the Targeted Entity Hardening problem

$K$ vulnerable entities would ensure that there are no induced and initial failure, (iii) The set of $K$ vulnerable entities for an interdependent network i.e. the attackers strategy is assumed to be provided. The necessity of this assumption can be described through the example provided in this section. For the interdependent network with IDRs table 1 both the set \{b₂,b₄\} and \{a₂,a₃\} represent the 2 vulnerable entities. If we worked with the former set of entities the solution obtained for the TEH problem with $P = \{b₂\}$ will be different. Hence for a given $K$ if the attacker has a choice of different set of $K$ vulnerable entities, with the current problem setting it is not possible to find the set of entities to harden. Solving the problem by relaxing the assumption (iii) is considered to be a potential future work.

III. COMPUTATIONAL COMPLEXITY ANALYSIS

In this section we provide (i) a polynomial time algorithm that solves the Targeted Entity Hardening Problem optimally with IDRs restricted to single minterm of size 1 and (ii) prove the problem is NP-complete with IDRs in general form.

A. Solution to the Targeted Entity Problem with IDRs having single minterm of size 1

With two entities $x_i$ and $y_i$ of network $A$ and $B$ respectively, IDRs of form $x_i \leftarrow y_i$ represents this special case. Additionally an entity can appear at most once on the left side of the IDR. Consider a simple interdependent network with the following two properties — (i) When an entity fails it has the capacity to make one or more entity non-operational, (ii) However each entity can be made non-operational by failure of at most one entity. Presence of this kind of dependency in the physical word encompass the IDRs of this special case. To develop the solution for this case consider an interdependent network $\mathcal{I}(A,B,\mathcal{F}(A,B))$. Let $A' \cup B'$ (with $A' \subseteq A$ and $B' \subseteq B$) the $K$ most vulnerable entities of this interdependent network. We first define Protection set in Definition 1. Using the result in Theorem 2 we design an algorithm (Algorithm 1) that solves the problem for this case optimally in polynomial time (proved in Theorem 3).

Definition 1. $PS(x_i|A' \cup B')$ denotes a set of entities which would not fail due to induced failure when the entity $x_i$ is hardened with entities in $A' \cup B'$ failing initially. $PS(x_i|A' \cup B')$ is termed as Protection Set of entity $x_i$.

Theorem 2. For any entity $x_i$ and $x_j$ with $x_i \neq x_j$ either (a) $PS(x_i|A' \cup B') \subseteq PS(x_j|A' \cup B')$, (b) $PS(x_i|A' \cup B') \subseteq PS(x_j|A' \cup B')$, or (c) $PS(x_i|A' \cup B') \cap PS(x_j|A' \cup B') = \emptyset$.

Proof: Consider a directed graph $G = (V,E)$. The vertex set $V$ consists of a vertex for each entity in $A \cup B$. For each IDR of form $y \leftarrow x$ there is a directed edge $(x,y) \in E$. In this proof the term vertex and entity is used interchangeably as an entity is essentially a vertex in $G$. It can be shown that $G$ is either (a) Directed Acyclic Graph (DAG) with maximum in-degree of at most 1 or, (b) contain at most one cycle with no incoming edge to any vertex in the cycle and maximum in-degree of at most 1, or (c) collection of graphs (a) and/or (b). Consider a vertex $x_i \in V$. Let $G' = (V',E')$ be a subgraph of $G$ with $V'$ consisting of $x_i$ and all the vertices that has a directed path from $x_i$. Moreover The edge set $E'$ consists of all edges $(x,y) \in E$ with $x,y \in V'$ except for any edge $(y,x_i)$ with $y_i \in V'$. Such a subgraph $G'$ would be a directed tree with (i) one or more entities in $V' \backslash \{x_i\}$ is in $A' \cup B'$. Let $X$ denote the set of such entities which satisfy this property, or (ii) no entities in $V' \backslash \{x_i\}$ is in $A' \cup B'$. If the entity $x_i$ hardened then for case (i) all the entities in $V'$ would be protected from failure except for entities in all such subtrees with roots in $X$. The set of entities in such subtrees are contained in a set $Z$ (say). For this condition if $x_j \in V' \backslash Z$ then $PS(x_j|A' \cup B') \subseteq PS(x_i|A' \cup B')$. Else if $x_j \in Z$ then $PS(x_j|A' \cup B') \cap PS(x_i|A' \cup B') = \emptyset$. For case (ii) for any entity $x_j \in V'$ the condition $PS(x_j|A' \cup B') \subseteq PS(x_i|A' \cup B')$ always holds (the equality holds for graphs of type (b) as stated above). This property holds for all entities in the entity set $A \cup B$. Hence proved.

Algorithm 1: Algorithm for TEH problem with IDRs of minterms with size 1

Data: An interdependent network $\mathcal{I}(A,B,\mathcal{F}(A,B))$, set of $K$ vulnerable entities and the set $P$ of entities to be protected from failure.

Result: A set of entities $H$ to be hardened.

1 begin
2 For each entity $x_i \in (A \cup B)$ compute the Protection Sets $PS(x_i|A' \cup B')$;
3 Initialize $H = \emptyset$;
4 while $P \neq \emptyset$ do
5 Choose the Protection Set with highest $|PS(x_i|A' \cup B') \cap P|$;
6 Update $H = H \cup \{x_i\}$;
7 Update $P = P \backslash PS(x_i|A' \cup B')$;
8 for all $x_i \in A \cup B$ do
9 $PS(x_i|A' \cup B') = PS(x_i|A' \cup B') \backslash PS(x_i|A' \cup B')$;
10 return $E$;

Theorem 3. Algorithm 1 solves the Targeted Entity Hardening problem with IDRs having single minterms of size 1 optimally in polynomial time.

Proof: The Protection Sets of the entities can be found in a similar way as that of computing Kill Sets defined in [12]. Due to lack of space we did not provide the algorithm to compute the Protection Sets. It can be shown that computing these sets for all entities in $A \cup B$ can be done in $O(n^3)$ where $n = |A| + |B|$. The while loop in Algorithm 1 iterates for a maximum of $n$ times. Step 5 can be computed in $O(n^2)$ time. The for loop in step 8 iterates for $n$ times. For any given $x_j$ and $x_i$, $PS(x_j|A' \cup B') = PS(x_j|A' \cup B') \cap PS(x_i|A' \cup B')$ can be computed in $O(n^3)$ time with the worst case being the condition when $|PS(x_j|A' \cup B')| = |PS(x_j|A' \cup B')| = n$. As step 9 is nested in a for loop within the while loop this accounts for the most expensive step in the algorithm. The time complexity of this step is $O(n^4)$. Thus Algorithm 1 runs polynomially in $n$ with time complexity being $O(n^4)$.

In Algorithm 1 the while loop iterates till all the entities in $P$ are protected from failure. In step 5 the entity $x_i$ with
protection set $PS(x_i|A^i \cup B^i)$ having most number of entities belonging to set $P$ is chosen to be hardened. Correspondingly the entity $x_i$ is added to the hardening set $H$. The set $P$ is updated by removing the entities in $PS(x_i|A^i \cup B^i)$. Similarly all the protection sets are updated by removing the entities in $PS(x_i|A^i \cup B^i)$.

We use the result from Theorem 2 to prove the optimality of Algorithm 1. An entity $x_i$ is selected to be hardened at any iteration of the while loop has maximum number of entities in $PS(x_i|A^i \cup B^i)$ $\cap P$. All entities $x_j$ with $PS(x_j|A^j \cup B^j) \subseteq PS(x_i|A^i \cup B^i)$ would have $PS(x_j|A^j \cup B^j) \cap P \subseteq PS(x_i|A^i \cup B^i) \cap P$. Moreover there exist no entity $x_k$ for which $PS(x_k|A^k \cup B^k) \subset PS(x_k|A^k \cup B^k)$ otherwise $x_k$ would have been hardened instead. Hence there exist no other entity that protect other entities in $P$ including $PS(x_i|A^i \cup B^i)$ $\cap P$.

So Algorithm 1 selects the minimum number of entities to harden that protects all entities in $P$.

**B. Computation Complexity of Targeted Entity Hardening with IDRs in general case**

In general case the IDRs can have arbitrary number of minterms of arbitrary size. With entities $x_i$ and $y_q$ belonging to network $A(B)$ and $B(A)$ respectively this case can be represented as $x_i \leftarrow \sum_{j=1}^{p} \gamma_{j,1} y_{j,2}$. The given example has $p$ minterms each of size $q_{j,1}$. We prove that the TEH problem is NP-complete (in Theorem 4) when the IDRs are logical disjunctions with minterms of size 1. With entities $x_i$ and $y_q$ belonging to network $A(B)$ and $B(A)$ respectively this case can be represented as $x_i \leftarrow \sum_{q=1}^{p} y_{q,1}$. The given example has $p$ minterms each of size 1. This class of IDRs is a subset of the general case and hence proves that TEH problem is NP-complete for the general case as well. In Theorem 5 we prove that the TEH problem is solvable with an approximation bound of $O(\log(|P|))$ when IDRs are logical disjunctions of minterms with size 1.

**Theorem 4. The TEH problem is NP-complete**

Proof: We prove that the Targeted Entity Hardening is NP complete by a reduction from Set Cover problem. An instance of the Set Cover problem consists of (i) a set of elements $U = \{x_1, x_2, \ldots, x_m\}$, (ii) a set of subsets $S = \{S_1, S_2, \ldots, S_m\}$ with $S_i \subseteq U \forall S_i \in S$, and (iii) a positive integer $M$. The problem asks the question whether there is a subset $S'$ of $S$ with $|S'| \leq M$ such that $\bigcup_{S_i \in S'} S_i = U$. From an instance of the Set Cover problem we create an instance of the Targeted Entity Hardening Problem as follows. For each element $x_j$ in $U$ we add an entity $a_i$ in set $A$. Similarly for each subset $S_i$ in set $S$ we add an entity $b_i$ in set $B$. For each element $x_j \in U$ which appears in subsets $S_m, S_n, S_p$ in $S$ (say) we add an IDR $a_i \leftarrow b_m + b_n + b_p$. There are no IDRs for entities in set $B$ which prevents any cascading failure. The value of $k$ is set to $|S|$. This ensures that all entities in set $B$ are killed initially for finalization of maximum number of entities. The maximum number of entities failed in this scenario are all entities in $A \cup B$. The set $P$ of entities to be protected is set to $U$ and $k$ is set to $M$.

Consider there exists a solution to the Set Cover problem. Then there exist a set $S'$ of cardinality $M$ such that $\bigcup_{S_i \in S'} S_k = U$. For each subsets $S_i \in S'$ we harden the entity $b_i \in B$. So in each IDR of the $A$ type entities there exist a $B$ type entity that is hardened. Hence all $A$ type entities will be protected from failure thus solving the Targeted Entity Hardening problem.

On the other way round consider there is a solution to the Targeted Entity Hardening problem. This ensures either that for each entity $a_j \in A$ (i) $a_j$ itself is hardened, or (ii) at least one entity from set $B$ in $a_j$’s IDR is hardened. For scenario (i) arbitrarily select an entity $b_j$ in $a_j$’s IDR and include it in set $C$. For scenario (ii) include the hardened entities in the IDR of $a_j$ into set $C$. This is done for each entity $a_j \in A$. For each entity in set $C$ select the corresponding subset in set $S$. The union of these set of subsets would result in the set $U$. Thus solving the set cover problem. Hence the theorem is proved.

**Theorem 5. The Targeted Entity Hardening Problem is $O(\log(|P|))$ approximate when IDRs are logical disjunctions of minterms with size 1.**

Proof: We first compute the protection set $PS(x_i|A^i \cup B^i)$ for all entities $x_i \in A \cup B$. Each protection set is pruned by removing entities that are not in set $P$. Now the Targeted Entity Hardening Problem can be directly transformed into Minimum Set Cover problem by setting $U = P$ and $S = \{PS(x_i|A^i \cup B^i), PS(x_2|A^i \cup B^i), \ldots, PS(x_p|A^i \cup B^i)\}$. Selecting the corresponding entities of the protection sets that solve the Minimum Set Cover problem would also solve the Targeted Entity Hardening problem. There exists an approximation ratio of order $O(\log(n))$ (where $n$ is the number of elements in set $U$) for the Set Cover problem. Hence the same ratio holds for the Targeted Entity Hardening problem with $n = |P|$. Hence proved.

**IV. SOLUTIONS TO THE ENTITY HARDENING PROBLEM**

In this section we provide optimal solution to the Targeted Entity Hardening problem using an Integer Linear program and a non optimal heuristic solution with polynomial time complexity.

**A. Optimal solution to the Targeted Entity Hardening problem**

We propose an Integer Linear Program (ILP) that solves the TEH problem optimally. Let $G = [g_1, g_2, \ldots, g_n]$ and $H = [h_1, h_2, \ldots, h_m]$ be two boolean arrays with $g_i = 0$ ($h_i = 0$) if entity $a_i \in A$ ($b_i \in B$) is in a failed state and $g_i = 1$ ($h_i = 1$) otherwise. Given an integer $K$ let $[G, H]$ be the solution to the $K$ most vulnerable node problem (with $g_i = 1$ ($h_i = 1$) if entity $a_i$ ($b_i$) belongs to the set of vulnerable entities). A set of variables $x_{id}$ and $y_{jd}$ are used in the ILP with $x_{id} = 1$ ($y_{jd} = 1$), when entity $a_i \in A$ ($b_i \in B$) is in a failed state at time step $d$, and 0 otherwise. It is to be noted that the maximum number of cascading steps is upper bounded by $|A| + |B| - 1 = m + n - 1$. The variables $g_{id}$ and $q_{id}$, are used to denote entity hardening. If an entity $a_i \in A$ ($b_i \in B$) is hardened then $q_{id} = 1$ ($q_{jd} = 1$) and 0 otherwise. The objective function can now be formulated as follows:

$$\min \left( \sum_{i=1}^{m} q_{id} + \sum_{j=1}^{n} q_{jd} \right)$$

(1)

The set of constraints are described below:

**Constraint Set 1:** $x_{id} \geq g_i - q_{id}$, and $y_{jd} \geq h_i - q_{jd}$. This constraint implies that only if an entity is not hardened and $g_i$ ($h_i$) is 1 then the entity will fail at the initial time step.

**Constraint Set 2:** $x_{id} \geq x_{i(d-1)}, \forall d, 1 \leq d \leq m + n - 1$, and $y_{jd} \geq y_{j(d-1)}, \forall d, 1 \leq d \leq m + n - 1$, in order to ensure that for an entity which falls in a particular time step would remain in failed state at all subsequent time steps.

**Constraint Set 3:** Modeling the constraints to capture...
the cascade propagation in IIM is similar to the constraints established in [12]. A brief presentation of this constraint is provided here. Consider an IDR \( a_i \leftarrow b_jb_kb_l + b_mb_n + b_q \) in general form. The following steps are enumerated to depict the cascade propagation:

Step 1: Replace all minterms of size greater than one with a variable. In the example provided we have the transformed minterm as \( a_i \leftarrow c_1 + c_2 + b_q \) with \( c_1 \leftarrow b_jb_kb_l \) and \( c_2 \leftarrow b_mb_n(b_1, b_2 \in \{0, 1\}) \) as the new IDRs.

Step 2: For each variable \( c_i \), constraints are added to capture the cascade propagation. Let \( N \) be the number of entities in the minterm on which \( c_i \) is dependent. In the example, for the variable \( c_1 \) with IDR \( c_1 \leftarrow b_jb_kb_l \), constraints \( c_{1d} \geq y_{j(d-1)} + y_{k(d-1)} + y_{l(d-1)} \) and \( c_{1d} \leq y_{j(d-1)} + y_{p(d-1)} + y_{l(d-1)} \forall d, 1 \leq d \leq m + n + 1 \) are introduced (with \( N = 3 \) in this case). If an IDR of an entity is already in form of a single minterm of arbitrary size, i.e., \( a_i \leftarrow b_jb_kb_l \) then constraints \( x_{id} \geq y_{j(d-1)} + y_{k(d-1)} + y_{l(d-1)} - q_{xi} \) and \( x_{id} \leq y_{j(d-1)} + y_{p(d-1)} + y_{l(d-1)} \forall d, 1 \leq d \leq m + n + 1 \) are introduced (with \( N = 3 \)). These constraints satisfies that if the entity \( x_i \) is hardened initially then it is not dead at any time step.

Step 3: Let \( M \) be the number of minterms in the transformed IDR as described in Step 1. In the given example with IDR \( a_i \leftarrow c_1 + c_2 + b_q \), constraints of form \( x_{id} \geq c_{1(d-1)} + c_{2(d-1)} + y_{q(d-1)} - (M - 1) - q_{x_i} \) and \( x_{id} \leq c_{1(d-1)} + c_{2(d-1)} + y_{q(d-1)} - (M - 1) - q_{x_i} \) are introduced. These constraints ensures that even if all the minterms of \( x_i \) has at least one entity in dead state then it will be alive if the entity is hardened initially.

Constraint Set 4: For all entities \( x_i, y_j \in P \), \( x_{i(m+n+1)} = 0 \) and \( y_{j(m+n+1)} = 0 \). This ensures that all the entities in set \( P \) are protected from failure at the final time step.

With these constraints the objective in (1) minimizes the number of hardened entities that results in protection of all entities in set \( P \).

B. Heuristic Solution of the Targeted Entity Hardening problem

A heuristic solution is provided in this subsection. Along with the definition of Protection Set, we introduce the notion of Cumulative Fractional Minterm Hit Value of an entity to design the heuristic. Before formal definition of Cumulative Fractional Minterm Hit Value (in Definition 7) we first define Fractional Minterm Hit Value of an entity in Definition 6.

Definition 6. The Fractional Minterm Hit Value for an entity \( x_j \in A \cup B \) in an interdependent network \( I(A, B, \mathcal{F}(A, B)) \) is denoted as \( FMHV(x_j, X) \). It is calculated as \( FMHV(x_j, X) = \sum_{i=1}^{m} \frac{x_i}{\Pi_i} \). In the formulation \( m \) are the minterms in which \( x_j \) appears over all IDRs except for the IDRs of entities in set \( X \). The parameter \( s_i \) denotes \( i^{th} \) such minterm. If an entity \( x_j \) is hardened (or protected from failure) the value computed provides an estimate impact on protection of other non operational entities.

Definition 7. The Cumulative Fractional Minterm Hit Value for an entity \( x_j \in A \cup B \) is denoted as \( CFMHV(x_j) \). It is computed as \( CFMHV(x_j) = \sum_{x_j, e \in PS(x_j | A \cup B)} FMHV(x_j, PS(x_j | A \cup B)) \). This gives a measure of impact on protecting non functional entities when the entity \( x_j \) is hardened.

Using these definitions a heuristic is formulated in Algorithm 2. For each iteration of the while loop in the algorithm, the entity having highest cardinality of the set \( PS(x_j | A \cup B) \) is hardened. This ensures that at each step the number of entities protected in set \( P \) is maximized. In case of a tie, the entity having highest Cumulative Fractional Minterm Hit Value among the set of tied entities is selected. This causes the selection of the entity that has the potential to protect maximum number of entities in subsequent iterations. Thus, the heuristic greedily minimizes the set of entities hardened which would cause protection of all entities in \( P \). The heuristic overestimates the cardinality of \( H \) from the optimal solution.

Algorithm 2: Heuristic solution to the TEH problem

Data: An interdependent network \( I(A, B, \mathcal{F}(A, B)) \), set of \( K \) vulnerable entities and the set \( P \) of entities to be protected from failure.

Result: A set of entities \( H \) to be hardened.

1 begin
2 Initialize \( D = \emptyset \) and \( H = \emptyset \);
3 while \( P \neq \emptyset \) do
4 For each entity \( x_d \in (A \cup B) \) compute the Protection Sets \( PS(x_d | A' \cup B') \);
5 For each entity \( x_d \in (A \cup B) \) compute \( CFMHV(x_d) \);
6 if there exists multiple entities having same value of the highest cardinality of the set \( PS(x_d | A' \cup B') \) then
7 Let \( x_p \) be an entity having highest \( CFMHV(x_p) \) among all \( x_p \)'s in the set of entities having highest cardinality of the set \( PS(x_p | A' \cup B') \);
8 If there is a tie choose arbitrarily;
9 Add \( x_d \) to set \( H \);
10 Update \( D = D \cup PS(x_p | A' \cup B') \);
11 Update \( P = P \setminus PS(x_p | A' \cup B') \);
12 Update \( \mathcal{F}(A, B) \) by removing entities in \( PS(x_p | A' \cup B') \) both in the left and right side of the IDRs;
13 else
14 Let \( x_p \) be an entity having highest cardinality of the set \( PS(x_p | A' \cup B') \);
15 Add \( x_p \) to set \( H \);
16 Update \( D = D \cup PS(x_p | A' \cup B') \);
17 Update \( P = P \setminus PS(x_p | A' \cup B') \);
18 Update \( \mathcal{F}(A, B) \) by removing entities in \( PS(x_p | A' \cup B') \) both in the left and right side of the IDRs;
19 return \( H \);

V. EXPERIMENTAL RESULTS

In this section we compared the heuristic solution with the optimal obtained from the Integer Linear program. The simulations were performed with power network data obtained from Platts (www.platts.com) and communication network data obtained from GeoTel (www.geo-tel.com). The power network consists of 70 power plants and 470 transmission lines and communication network constitutes 2,690 cell towers, 7, 100 fiber-bit buildings and 42, 723. All this data pertains to Maricopa County, Arizona, USA. Five non overlapping regions
of the county were identified (union of these five region does not span over the entire Maricopa county). The entities in the power and communication network for these regions were extracted and added to set $A$ (for power network entities) and set $B$ (for communication network entities). The cardinality of the entity sets $A$ and $B$ were 29 and 19 for Region 1, 29 and 20 for Region 2, 29 and 19 for Region 3, 33 and 20 for Region 4 and 29 and 20 for Region 5. For each of these regions an interdependent network $I(A, B, F(A, B))$ was constructed. The function $F(A, B)$ was computed for each interdependent network $I(A, B, F(A, B))$ using the IDR construction rules defined in [12].

IBM CPLEX optimizer was used to obtain the optimal solutions. The heuristic solutions were obtained using Python. The value of $K$ ($K$ most vulnerable entity) was set to 8 which resulted in failure of 28, 23, 28, 28 and 27 entities over the five regions. For each region an arbitrary set $P$ was constructed using 5, 10, 15, 20 entities from the respective failed set of entities. The set $P$ gives the entities to be protected from failure. The number of entities required to harden for a given region and set $P$ was obtained for the optimal and heuristic solution. The results are provided in Figure 2a - Figure 2c. For the given set of simulations the heuristic solution deviates by a maximum of 50% with the optimal when $|P| = 15$ for Region 5. This variance can be accounted for the greedy nature of Algorithm 2. On an average the heuristic solution varied by 18.31% from the optimal.

VI. CONCLUSION

In this paper we studied the Targeted Entity Hardening problem in multi-layer networks. We modeled the interdependencies shared between the networks using IIM, and formulated the Targeted Entity Hardening problem in this setting. We showed that the problem is solvable in polynomial time for a special case, whereas for IDR's in general form it is NP-complete. We evaluated the efficacy of our heuristic by comparing it with the optimal solution (obtained from an Integer Linear program) using power and communication network data of Maricopa County, Arizona.

REFERENCES

[1] G. Andersson, P. Donalek, R. Farmer, N. Hatzigiroyiou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca et al., “Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance,” Power Systems, IEEE Transactions on, vol. 20, no. 4, pp. 1922–1928, 2005.

[2] Y. Tang, G. Bu, and J. Yi, “Analysis and lessons of the blackout in indian power grid on july 30 and 31, 2012,” in Zhongguo Dianji Gongcheng Xuexiao (Proceedings of the Chinese Society of Electrical Engineering), vol. 32, no. 25. Chinese Society for Electrical Engineering, 2012, pp. 167–174.

[3] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” Nature, vol. 464, no. 7291, pp. 1025–1028, 2010.

[4] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, “Cascade of failures in coupled network systems with multiple support-dependence relations,” Physical Review E, vol. 83, no. 3, p. 036116, 2011.

[5] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, “Networks formed from interdependent networks,” Nature Physics, vol. 8, no. 1, pp. 40–48, 2011.

[6] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola, “Modelling interdependent infrastructures using interacting dynamical models,” International Journal of Critical Infrastructures, vol. 4, no. 1, pp. 63–79, 2008.

[7] P. Zhang, S. Peeta, and T. Friesz, “Dynamic game theoretic model of multi-layer infrastructure networks,” Networks and Spatial Economics, vol. 5, no. 2, pp. 147–178, 2005.

[8] M. Parandehgheibi and E. Modiano, “Robustness of interdependent networks: The case of communication networks and the power grid,” arXiv preprint arXiv:1304.0356, 2013.

[9] D. T. Nguyen, Y. Shen, and M. T. Thai, “Detecting critical nodes in interdependent power networks for vulnerability assessment,” 2013.

[10] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, “Power grid vulnerability to geographically correlated failures-analyses and control implications.,” arXiv preprint arXiv:1206.1099, 2012.

[11] J. Banerjee, A. Das, and A. Sen, “A survey of interdependency models for critical infrastructure networks,” NATO Science for Peace and Security Series -D: Information and Communication Security, vol. 37, pp. 1–16, 2014.

[12] A. Sen, A. Mazumder, J. Banerjee, A. Das, and R. Compton, “Identification of k most vulnerable nodes in multi-layered network using a new model of interdependency,” in Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on. IEEE, 2014, pp. 831–836.

[13] A. Das, J. Banerjee, and A. Sen, “Root cause analysis of failures in interdependent power-communication networks,” in Military Communications Conference (MILCOM), 2014 IEEE. IEEE, 2014, pp. 910–915.

[14] J. Banerjee, A. Das, C. Zhou, A. Mazumder, and A. Sen, “On the entity hardening problem in multi-layered interdependent networks,” in Computer Communications Workshops (INFOCOM WKSHPS), 2015 IEEE Conference on. IEEE, 2015, pp. 648–653.

[15] A. Das, C. Zhou, J. Banerjee, A. Sen, and L. Greenwald, “On the smallest pseudo target set identification problem for targeted attack on interdependent power-communication networks,” in Military Communications Conference, MILCOM 2015-2015 IEEE. IEEE, 2015, pp. 1015–1020.