Joint Scheduling & Jamming for Data Secrecy in Wireless Networks

Siddhartha Sarma, Samta Shukla and Joy Kuri
Department of Electronic Systems Engineering
Indian Institute of Science
Bangalore, India
Email: {siddharth,samta,kuri}@dese.iisc.ernet.in

***Abstract*—The broadcast nature of the wireless medium jeopardizes secure transmissions. Cryptographic measures fail to ensure security when eavesdroppers have superior computational capability; however, it can be assured from *information theoretic security* approaches. We use *physical layer security* to guarantee non-zero secrecy rate in single source, single destination multi-hop networks with eavesdroppers for two cases: when eavesdropper locations and channel gains are known and when their positions are unknown. We propose a two-phase solution which consists of finding activation sets and then obtaining transmit powers subject to SINR constraints for the case when eavesdropper locations are known. We introduce methods to find activation sets and compare their performance. Necessary but reasonable approximations are made in power minimization formulations for tractability reasons. For scenarios with no eavesdropper location information, we suggest *vulnerability region* (the area having zero secrecy rate) minimization over the network. Our results show that in the absence of location information average number of eavesdroppers who have access to data is reduced.**

I. Introduction

Eavesdropping on the information in transit poses a threat to data secrecy of wireless sensor networks and therefore concerns the research community gravely [1]. In these kind of attacks, an adversary can introduce new receivers or modify existing nodes in the network to passively eavesdrop on information transmission [2]. The attacker model can vary from an isolated eavesdropper to an organized group of eavesdroppers. Existing countermeasures for those attacks are from the cryptographic perspective, where, by using secret keys, sensor nodes ensure information secrecy from malicious users.

But cryptographic measures become ineffective if the adversary has superior computational capability [3], [4] or is able to retrieve the secret keys. Changing keys at intervals can be a possible solution, but its implementation becomes cumbersome. This is where *Information Theoretic Secrecy* model appears promising: it guarantees equivocation of the eavesdropper regarding the message, irrespective of its computational capability.

The *physical layer security* approach under the information theoretic secrecy model achieves a non-zero secrecy rate *only* when the eavesdropper channel is degraded with respect to the legitimate receiver's channel [5], [6], [7]. In general, however, eavesdropper channels can have relatively higher gains. In such cases, a feasible solution is to deploy jammers in the network to interfere with eavesdroppers' reception while retaining adequate SINR at legitimate receivers.

We consider a single source, single destination multi-hop network; paths stretch from source to destination via trusted relay nodes. We initially assume that eavesdropper location information is available, which is a strong assumption. Nevertheless, we assume this because we are interested in understanding whether, even with this convenient assumption, it is possible to operate the system such that it satisfies the twin goals of conveying bits at adequate quality to legitimate receivers while defeating passive adversaries.

In some application scenarios, the characteristics of the physical terrain may restrict adversary locations severely. For example, if there is a large water body in the terrain, then it is reasonable to assume that no adversary can be located in that area. In this way, possible eavesdropper locations can get narrowed down sufficiently: eavesdroppers can be located only at certain spots, and our approximation becomes more and more reasonable.

Another example is when trusted relay nodes that were initially part of the network become eavesdroppers as they exhibit malicious behavior with time (as a consequence of planned or accidental damage). In this case, in fact eavesdropper locations are known.

We further assume that channel gains are known, and address power allocation (PA) for a contention-based wireless scenario where a transmission is successful if the SINR at receiver nodes is maintained above a certain threshold. To accomplish this: (1) we propose methods to identify link activation sets (AS) and schedule links to reduce interference at legitimate receivers and to increase interference at eavesdroppers, (2) we formulate an optimization problem to allocate power for activation sets satisfying SINR constraints. The formulation results in a non-convex objective function with non-linear constraints, owing to which we propose an approximate linear optimization formulation.

Even with eavesdropper locations known, we are talking of coordinated transmissions from several transmitters, so that legitimate receivers get the data but eavesdroppers see unacceptable interference. This means centrally coordinated, tightly synchronized operation, which is not practically feasible (as it may involve too much overhead). However, since this is a "first-cut" study about whether the proposed idea is workable at all, we assume centralized operation.

Keeping the centralized mode of operation intact, we later relax the assumption about eavesdroppers' location information. We modify our activation sets for this case and formulate an optimization problem to minimize the vulnerability region, *i.e.*, zero-secrecy rate region, in the network.

The main contributions of this paper are:

- We discuss methods to find *activation sets* such that *every* eavesdropper corresponding to those sets is jammed.
- We formulate an optimization problem to calculate activation fractions for activation sets and optimal transmit powers for nodes in the network.
- We compare the methods for choosing activation sets for a given gain matrix G using the optimization problem solution.
- We formulate an optimization problem for the scenario when nodes are not aware of eavesdroppers' locations and minimize the *vulnerability region*.
- We analyze our results from *information theoretic secrecy* perspective and show that non-zero secrecy rate is achieved for example networks.

Our paper is organized as follows: In Section II, we survey the related work. The model, assumptions and notations used throughout this paper are introduced in Section III. In Section IV, we propose different methods to schedule and provide illustrative examples for each. The optimization formulation for power allocation is discussed in detail in Section V. We discuss vulnerability region minimization in Section VI. In Section VII, we calculate *secrecy rate* using power values obtained from previous section. We conclude in Section VIII.

II. Related Work

Literature related to data security for sensor networks is well diversified. It ranges from application layer based implementations to physical layer based techniques. Link-layer based security protocol *TinySec* [2], public-key based *TinyPK* [8] use the cryptographic approach to address security issues in sensor networks. In physical layer based approach, the significance of jamming was introduced by Goel *et al.* [9]. Authors in [10], [11] discussed how cooperative jamming can improve wireless physical layer security. Achievable rate-equivocation region for relay-eavesdropper channel was evaluated by Lai *et al.* in [12]. Security improvement with the help of relays is captured by authors in [11], [13]. Using jammers to communicate securely via an untrusted relay node is presented in [14]. Cooperative jamming for the same is considered in [15]. *iJam* [16] presents implementation of jamming on an 802.11-like physical layer. Vasudevan *et al.* consider opportunistic relaying in a dynamic fading scenario for wireless networks [17]. Pinto *et al.* [18], [19] have considered *iS-graph* for wireless secrecy in large scale networks. Secret communication for large wireless networks in one and two dimension without any information on eavesdroppers' location is discussed in [20]; to improve secrecy, multiple message bits are sent to convey a single message, but this can waste precious wireless bandwidth. In [21], the authors discussed how eavesdroppers are confused by random link scheduling and hence are prevented from gaining any knowledge about transmission epochs. Authors in [22] discussed how to choose a relay and a jammer from a set of nodes to improve secrecy in transmission. Their work is extended in [23] to the case of a two-way network by performing joint relay and jammer selection. Power allocation for co-operative jamming using dirty paper coding is considered in [24]. [25] proposed an initial study on minimization of vulnerability region for a single relay network.

The models considered above mostly have one-hop transmission and a single eavesdropper. We consider multi-hop networks with multiple eavesdroppers, a scenario which is more practical.

Sensor nodes are always energy constrained. So, optimal power allocation for the network not only enhances lifetime but also improves aggregate data transmission. As a result, power allocation is studied extensively in the literature. Authors in [26] have considered joint scheduling and power allocation for *wireless ad-hoc networks*. Cruz *et al.* [27] took the duality approach to find the optimal policy for scheduling and power allocation. Unlike all previous approaches limited to link scheduling and power allocation only, we propose an optimization formulation with an additional aspect of jamming.

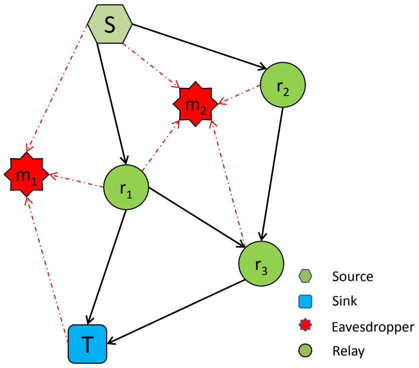

Fig. 1. Example network model with eavesdroppers. Links shown in solid black represent possible data routing paths. Eavesdropping links are depicted in dotted red. Interference due to node transmissions are not shown.

III. Network Model & Notation

We model the network by a directed graph, $\mathcal{G} = (\mathcal{V}, \mathcal{L})$, and assume the network to be static. We assume that a communication link from node i to j exists if node j is within the transmission range of node i. For a directed link $l := (i, j)$, let $s(l) = i$ denote the transmitting node, and $e(l) = j$ be the receiving node for that link. The node set in $\mathcal{G}$, *i.e.* $\mathcal{V}$, consists of source, destination, relay nodes and eavesdroppers. We denote $R = |\mathcal{R}|$ as the total number of nodes consisting of source, destination and relays, $E = |\mathcal{E}|$ as the number of eavesdroppers. Hence, $\mathcal{V} = (\mathcal{R} \cup \mathcal{E})$. The set of links in graph ($\mathcal{L}$) are of the following types: source to relay, relay to relay, relay to destination, source to eavesdropper, relay to eavesdropper and destination to eavesdropper. Information flow is directed from source node to the destination node via relays and both source node and relay nodes have always data to transmit.

We assume that a relay node in the graph follows the Decode and Forward (DF) strategy and at any instant, can either work as a transmitter or a jammer. We assume that the eavesdroppers are passive nodes: they can only receive signals but cannot transmit. The directed subgraph without eavesdroppers is denoted by $G_1 = (\mathcal{R}, \mathcal{L}_1)$ where $\mathcal{L}_1 := \{l \in \mathcal{L} : e(l) \in \mathcal{R} \setminus \{S\}\}$. For a set of links $\mathcal{L}'$, we denote the set of nodes attached to the links in that set as: $\mathcal{V}^{\mathcal{L}'} := \{v : v = s(l)$ or $v = e(l), l \in \mathcal{L}'\}$. In $\mathcal{V}^{\mathcal{L}'}$, the set of all transmitting nodes is denoted by $\widehat{T}_{\mathcal{V}^{\mathcal{L}'}} = \{v \in \mathcal{V}^{\mathcal{L}'} : v = s(l), l \in \mathcal{L}'\}$, whereas, the set of nodes that transmit to legitimate receivers is denoted by $T_{\mathcal{V}^{\mathcal{L}'}} = \{v \in \mathcal{V}^{\mathcal{L}'} : v = s(l), l \in \mathcal{L}_1\}$. Hence, nodes in the set $\widehat{T}_{\mathcal{V}^{\mathcal{L}'}} \setminus T_{\mathcal{V}^{\mathcal{L}'}}$ are jamming nodes for link set $\mathcal{L}'$. We define the *overheard set* for each eavesdropper m_i, where $i \in [1, 2, \ldots, E]$, as: $\Phi_{m_i} = \{v : v \in \mathcal{R}, s(l) = v \;\&\; e(l) = m_i$ where $l \in \mathcal{L}\}$. Similar notation is defined in terms of links: Ψ_{m_i}, a set of links such that any ongoing transmission on them is heard at eavesdropper m_i.

IV. Scheduling

In wireless networks, concurrent transmissions from nodes that are in radio range of one another result in interference. To ensure interference-free transmissions, we use the notion of a *Maximal Independent Set* (MIS) [28].

Maximal Independnet Set (MIS): A set of links which can be activated together without interfering each others transmission and no more links can be added to that set without violating this non-interfering property.

But in the presence of eavesdropper(s), whenever a message is transmitted from the source/relay node to another relay node/destination, eavesdroppers within range of the transmitter can intercept the message. This results in loss of data secrecy. To address this issue, our approach is as follows:
We schedule transmissions in such a way that eavesdropper(s) in the reception range of transmitters experience heavy interference due to other ongoing transmissions. At the same time, we want SINR at the legitimate receivers to be above a certain threshold for proper decoding of transmitted messages. In other words, from "Physical Layer Security" perspective, non-zero secrecy rate between transmitters and receivers is achieved by degrading the eavesdroppers' channel with respect to legitimate receivers.

With the motive mentioned above, we form *Activation Sets*, similar to the notion of Maximal Independent Sets (MIS).

Activation Set (AS): A set of links which contains non-interfering links for receiving nodes and interfering links for eavesdropping nodes.

Therefore, if we consider the restriction of activation sets to $\mathcal{G}_1$, then we get subsets of MISes. For clarity, we mention the fundamental criteria for forming activation sets.

- Nodes cannot receive and transmit simultaneously (primary interference constraint). Therefore, activation sets will contain links which have a certain node in transmitting end or receiving end, but not both.
- Nodes cannot decode concurrent transmissions from multiple transmitters, hence links ending at the same node can not be part of the same activation set.
- For a transmitter-receiver pair, if a receiver is in transmission range of a jammer, then we have to ensure that the SINR at that receiver is maintained above a certain threshold. (Section:V)
- For every eavesdropper corresponding to a transmitter-receiver pair in an activation set, the set should contain at least one more transmitter/jammer to interfere with that eavesdropper.

We propose three methods for finding activation sets. At first, we discuss *activation contention graph* method which provides us all possible activation sets for a network. But it is well known that finding all possible activation sets on an arbitrary graph has exponential complexity in number of links [29]. Hence, we provide two alternate and relatively less computationally expensive methods. Note that, as the activation sets depend on the eavesdroppers' location, it is possible that for some networks usefulness of activation sets cease to exist.

A. Activation contention graph method

Similar to the notion of *Link Contention Graph* [28], we introduce *Activation Contention Graph* to find activation sets. Since we have assumed the primary interference model, we follow a 1-hop adjacency constraint instead of the 2-hop adjacency constraint discussed in [28]. The rules for forming activation contention graph are as follows:

1) Adjacent links with one node from $\mathcal{R}$ in common in the original graph are connected nodes in the activation contention graph.
2) Non-adjacent links are not connected in the activation contention graph.

After forming the activation contention graph, we need to find activation sets following these conditions:

1) A set can contain only disconnected nodes of the graph.
2) In sets formed above, if a node belongs to a certain Ψ_{m_i}, then we ensure presence of at least one more node in that set which belongs to Ψ_{m_i}; else discard that node from that set.

Note that the nodes we are mentioning here are actually links in original graph $\mathcal{G}$. So the above two conditions ensure no or less interference at receivers and maximal interference at eavesdroppers.

B. Alternative methods:

1) MIS based: In this method we begin with an arbitrary MIS M_k for graph $\mathcal{G}_1$. We then proceed as follows to form an activation set.

1) We find the set of eavesdroppers for M_k.
2) We then consider an arbitrary eavesdropper m_i from that set.

3) In $\mathcal{V}^{M_k}$, *i.e.*, set of nodes which form the links of M_k, we search for nodes whose transmission can be eavesdropped by m_i.
   - If there are two or more such nodes in $\mathcal{V}^{M_k}$, then eavesdropper m_i's reception is hindered by simultaneous transmission from those nodes.
   - Else, if there is a single node, then either we have to add at least one more node from set $(\mathcal{R}\setminus\mathcal{V}^{M_k})\cap\Phi_{m_i}$ or if the this set is empty, then we remove that single node from $\mathcal{V}^{M_k}$ and remove the corresponding link from M_k.

4) We repeat the same procedure from step 2 until all the eavesdroppers are taken care of.

Finally, we obtain an activation set by adding or removing nodes from the initial MIS M_k.

2) Dominant Jammer method: We begin by finding a relay node whose transmission is received by most of the eavesdroppers. If we use this relay node as transmitter, we have to ensure that all the corresponding eavesdroppers are jammed. On the other hand, if this node acts as a jammer, it can jam many eavesdroppers simultaneously. This simple idea drives this method and hence the name. In fact, in case of dense networks, it is possible to find a set of relay nodes which can provide us optimal jamming solutions. The steps below describe the procedure to find the activation sets:

1) We denote the set of jammers by Θ, which is initially empty.
2) We pick an arbitrary relay node r from set $\mathcal{R}\setminus\{S,T\}$.
3) We then calculate I_r, which keeps track of the number of occurrences of node r in the set Φ_{m_i}, $\forall\ i$. I_r can be expressed as $I_r = \sum_{m_i\in\mathcal{E}} \mathbb{I}_{\{r\in\Phi_{m_i}\}}$
4) As the node with highest occurrence is of our interest, we find r_θ, where $r_\theta = \underset{r\in\mathcal{R}\setminus\{S,T\}}{\arg\max}\ I_r$. We add r_θ to the set Θ. In case of multiple such nodes, we choose the one which has smallest channel gains.
5) Deploying r_θ as jammer leaves us with a reduced set of eavesdroppers. We denote it as $\mathcal{E}_\theta$ which can be expressed as $\mathcal{E}_\theta = \mathcal{E}\setminus\{m\in\mathcal{E} : r_\theta\in\Phi_m\}$
6) We repeat the procedure from step 2 onwards with relay node set $\mathcal{R}\setminus\{S,T,r_\theta\}$ and eavesdropper set $\mathcal{E}\setminus\mathcal{E}_\theta$, till we are left with an empty set of eavesdroppers.
7) The set of relay nodes is now divided into two subsets Θ and $\mathcal{R}\setminus\{\{S,T\}\cup\Theta\}$. To form activation sets, we choose relay nodes from the latter set and corresponding jammers from the first set.
8) In case of $\mathcal{E}\setminus\mathcal{E}_\theta$ remains non-empty, we employ the source and destination node as jammer, if necessary.

C. Example

The scheduling methods introduced in section-IV are illustrated here for the example shown in Fig-1.

1) Activation Contention Graph based: Once the activation contention graph is drawn, it is easier to find out activation sets from that. Here is the activation contention graph for our example network.

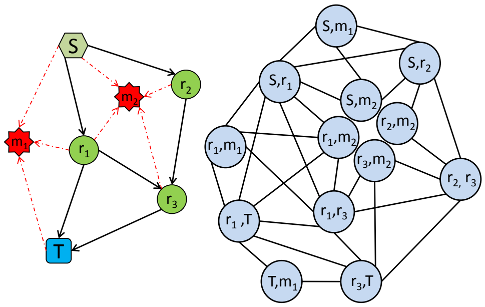

Fig. 2. Original graph and activation contention graph of example network.

We write down all the $\Psi_{(.)}$ as below
$\Psi_{m_1} = \{(S,r_1),(S,r_2),(S,m_1),(S,m_2),(r_1,T),(r_1,r_3),(r_1,m_1),(r_1,m_2),(T,m_1)\}$
$\Psi_{m_2} = \{(S,r_1),(S,r_2),(S,m_1),(S,m_2),(r_1,T),(r_1,r_3),(r_1,m_1),(r_1,m_2),(r_2,r_3),(r_2,m_2),(r_3,T),(r_3,m_2)\}$
It is easy to check from the original graph that $\{(S,r_2),(r_3,T),(r_1,m_1)\}$ is an activation set.

2) MIS based: We begin with an arbitrary MIS for graph $\mathcal{G}_1$, $M_k = \{(S,r_1),(r_2,r_3)\}$. The eavesdropper set for M_k is $\{m_1,m_2\}$. Eavesdropper m_2 is interfered with by transmitter set $\{S,r_2\}$. But m_1 is able to eavesdrop the transmission from S, so we deploy T as a jammer for m_1. As a result, the final activation set becomes $A = \{(S,r_1),(r_2,r_3),(T,m_1)\}$

3) Dominant Jammer based: I_r values for the relay nodes of the example graph turn out to be $I_{r_1} = 2$; $I_{r_2} = 1$; $I_{r_3} = 1$. Hence, node r_1 is capable of jamming all the eavesdroppers concurrently. Using the other two relay nodes, we form a path from source to destination: $S \rightarrow r_2 \rightarrow r_3 \rightarrow T$. Node r_1 works as a jammer whenever any link in this path is activated. As an example, activation set $A = \{(S,r_2),(r_3,T),(r_1,m_1),(r_1,m_2)\}$ can be easily derived from above mentioned procedure.

V. Power Allocation

In this section, we find the transmitter powers on links that are activated simultaneously in an activation set .

Sensor networks are energy constrained, so with an objective to minimize the effective power consumption, we formulate an optimization problem.

A. Optimization Problem Formulation:

P_i denotes the transmit power used by node i . The channel gain from the i^{th} to the j^{th} node is denoted as $G(i,j)$, which is assumed constant in our analysis. Hence, SINR at the j^{th} node is given by $SINR_{ij} = \frac{G(i,j)P_i}{\mu_j+\eta_j}$, where μ_j, η_j is the interference due to other transmitters, jammers and ambient noise at the receiver node j, respectively. We denote the set of interfering transmitters for receiver node j in activation set A_m as $\mathcal{S}_j^{A_m} := \{h\in\mathcal{V}^{A_m} : h = s(l),\ l\in A_m\ \&\ e(l)\neq j\}$. Hence, $\mu_j = \sum_{h\in\mathcal{S}_j^{A_m}} G(h,j)P_h$. Similarly, for an eavesdropper node, $SINR_{ik}$ can be expressed as $\frac{G(i,k)P_i}{\mu_k+\eta_k}$; μ_k, η_k represents the similar parameters as defined for node j. To keep the transmission decodable at the receiver, we want to ensure that the SINR should be at least above certain positive real threshold value β_1, whereas at an eavesdropper, it should be less than another positive real threshold value β_2 $(\leq \beta_1)$:

$$\begin{aligned} &SINR_{ij} \geq \beta_1, \quad \forall (i,j) \in \mathcal{L}_1 : i,j \in \mathcal{R} \\ &SINR_{ik} \leq \beta_2, \quad \forall (i,k) \in \mathcal{L} \setminus \mathcal{L}_1 : i \in \mathcal{R}, k \in \mathcal{E} \end{aligned}$$

For notational convenience, we combine both types of SINR constraints and represent it in matrix equation form. As an example, for activation set A_m with n transmitting nodes, if we denote the power vector of transmitter as $\mathbf{P}_{A_m} = [P_1 \ P_2 \ \ldots (-)P_n]'$, then the SINR constraints can be expressed as:

$$\mathbf{P}_{A_m} \geq \mathbf{F}_{A_m}\mathbf{P}_{A_m} + \eta_{A_m}$$

where $\mathbf{F}_{A_m}$ is a matrix with main diagonal elements being zero, and non-diagonal elements being functions of the gain matrix (G) and β values; η_{A_m} is a vector whose elements are functions of G, β and η values of receiver of set A_m.

Activation sets are activated in sequence, for times equal to activation fractions of the total duration. The effective power used by a node is the weighted (weights are activation fractions) average of the power used by that node for all activation sets in which it appears. Recall that the activation sets are $A_1, A_2, \ldots, A_M$, and the corresponding activation fractions for those sets are $a_1, a_2, \ldots, a_M$. Hence, if we denote the sum of the transmitter powers in activation set A_j by P_{A_j}, then the effective power can be expressed as $\overline{P} = \sum\limits_{j=1}^{M} a_j P_{A_j}$

The effective power minimization problem is formulated as shown below:

$$\begin{aligned} & \min \ \overline{P} && \text{(1a)} \\ \text{such that} \quad & \mathbf{Q}\mathbf{y} = \mathbf{x} && \text{(1b)} \\ & \mathbf{y} \leq \sum_j a_j \mathbf{C}_j(G, \mathbf{P}, \eta) && \text{(1c)} \\ & \mathbf{x} \geq \mathbf{t} && \text{(1d)} \\ & \mathbf{P}_{A_j} \geq \mathbf{F}_{A_j}\mathbf{P}_{A_j} + \eta_{A_j}, \quad \forall A_j && \text{(1e)} \\ & P_i \geq 0, \ \forall i && \text{(1f)} \\ & a_j \geq 0, \ \forall j \text{ and } \sum_j a_j \leq 1 && \text{(1g)} \end{aligned}$$

Equation (1b) represents the flow conservation constraints, where $\mathbf{Q}$ is the node-link incidence matrix; $\mathbf{y} = (y_l, l \in \mathcal{L}_1)$, is the flow vector for links; $\mathbf{x}$ is a vector with R elements, having value x & $-x$ corresponding to source (generator of flow) and destination (consumer of flow) and zero for others. Inequality (1c) is the capacity constraint which captures the maximum flow supported by a link. To retain clarity, we have shown in the expression that capacity of a wireless link is a function of channel gain, transmitter power, interference and noise power. The *wired equivalent link capacity* is the product of raw link capacity and sum of the activation fractions of sets for which the link was ON. For gain matrix G, we denote the capacity vector due to activation set A_j, as $\mathbf{C_j}$. This vector contains non-zero terms corresponding to the links in activation set A_j, which can be calculated from $\frac{1}{2}\log(1 + SINR_{(l)})$. (1d) tells that flow from the source should be more than some threshold $(\mathbf{t})$. (1e) is the compact SINR constraint. Non-negativity of power and activation fractions, upper bound on the summation of the latter is captured by last two constraints.

The objective function we have considered is non-linear and non-convex. Hence, for tractability, we approximate it by a linear objective function, *viz.*, simple average of the powers of activation sets. But unlike (1), this new objective function does not provide us activation fraction values. So we introduce throughput (x) in the objective function with appropriate scaling factor λ (≥ 0). Hence, the new objective is $f(\mathbf{P}, x) = \frac{1}{M}\sum\limits_{j=1}^{M} P_{A_j} - \lambda x$, which aims to minimize a linear combination of power and throughput.

Though we have removed the non-linearity from the objective function, owing to non-linear constraints, this optimization problem is still difficult to solve. So, we propose another approximation for tractability. Instead of considering capacity as a function of G and $\mathbf{P}$ and η, we assume it to be a constant; its value is determined by underlying physical layer technology. The assumption of treating capacity as a constant is fairly practical and can be validated for technologies like ZigBee [30], which provides constant data rate when the SINR value is above some threshold and transmit powers are at certain level, under fixed operational conditions (*e.g.*, frequency band, modulation technique etc.). Essentially, in an activation set A_j, transmit powers must be maintained such that, the SINR at a legitimate receiver node is adequate for capacity C_j. P_{th} is the smallest of such lower bounds. For other nodes (jammers), the lower bound of zero suffices. Hence, our new optimization problem becomes:

$$\begin{aligned} & \min f(\mathbf{P}, x) && \text{(2a)} \\ \text{such that} \quad & \mathbf{Q}\mathbf{y} = \mathbf{x} && \text{(2b)} \\ & \mathbf{y} \leq \sum_j a_j \mathbf{C}_j && \text{(2c)} \\ & \mathbf{x} \geq \mathbf{t} && \text{(2d)} \\ & \mathbf{P}_{A_j} \geq \mathbf{F}_{A_j}\mathbf{P}_{A_j} + \eta_{A_j}, \quad \forall A_j && \text{(2e)} \\ & P_i \geq P_{th}, \ \forall i \in T_{A_j}, \forall A_j && \text{(2f)} \\ & P_i \geq 0, \ \forall i \in \left(\widehat{T}_{A_j} \setminus T_{A_j}\right), \forall A_j && \text{(2g)} \\ & a_j \geq 0, \ \forall j \text{ and } \sum_j a_j \leq 1 && \text{(2h)} \end{aligned}$$

If feasible solution of this problem exists then it provides us with the optimal activation fractions and the power allocation vector.

Now, SINR at the receiver nodes of an activation set is solely due to transmitters of that set and independent of nodes from other activation sets. In addition to that, the simple average based objective function allows us to divide optimization problem (2) into smaller optimization problems for each of the activation sets, and these can be solved independently. Also, as we have removed the dependency of capacity on power, the throughput optimization problem can be formulated and solved independently of the power minimization problems.

B. *Activation set based power optimization*

We formulate an optimization problem to calculate optimal power values for every activation set.

$$\min \sum_{i=1}^{|A_m|} P_i \tag{3a}$$

$$\text{s.t.} \quad \mathbf{P}_{A_m} \geq \mathbf{F}_{A_m}\mathbf{P}_{A_m} + \eta_{A_m} \tag{3b}$$

$$P_i \geq P_{th}, \ \forall i \in T_{A_m} \tag{3c}$$

$$P_i \geq 0, \ \forall i \in \left(\widehat{T}_{A_m} \setminus T_{A_m}\right) \tag{3d}$$

C. *Throughput Optimization Problem*

The throughput optimization problem is mentioned below for the sake of completeness.

$$\max \ x \tag{4a}$$

$$\text{s.t.} \quad \mathbf{Q}\mathbf{y} = \mathbf{x} \tag{4b}$$

$$\mathbf{y} \leq \sum_j a_j \mathbf{C}_j \tag{4c}$$

$$\mathbf{x} \geq \mathbf{t} \tag{4d}$$

$$a_j \geq 0, \ \forall j \text{ and } \sum_j a_j \leq 1 \tag{4e}$$

D. *Comparison among the methods*

We solve the optimization problem (2) for alternate methods (MIS based and Dominant jammer method) also by choosing the activation sets according to the corresponding method. The value of the objective function corresponding to each method serves as a metric for comparison.

We also can compare the methods by calculating $\overline{P}$ for each method using the solution of optimization problem (2). For both the approaches, the lesser the value of the metric, better is the method for a given G.

Results

We demonstrate the dependency of objective function, effective power and throughput on $\frac{\beta_1}{\beta_2}$ by numerical calculations. Keeping $\beta_2 = 1$ (BER$\approx 10^{-4}$ for ZigBee networks [31]) we increase β_1. As $\frac{\beta_1}{\beta_2}$ increases, the SINR criterion for legitimate links relative to that of eavesdropper links gets more stringent. This results in infeasibility of power optimization for some of the activation sets. For higher $\frac{\beta_1}{\beta_2}$ values, we remove these infeasible activation sets and proceed with our optimization problem. Removal of activation sets leads to reduction in throughput. Figure 3 depicts these for several phases of optimization process. The impulses in the values of objective function show that certain activation set(s) have become infeasible and flows are routed through other activation sets which were inactive before.

Figure 4 depicts a comparison of objective function values for all three methods. Bar plots shows that *Activation Contention graph based* method has lowest objective function value and is superior to the other two. For all these results, we consider an example graph (Figure 1) of 5 nodes and 2 eavesdroppers with a gain matrix (G). We assume zero mean Gaussian noise with variance 0.0001.

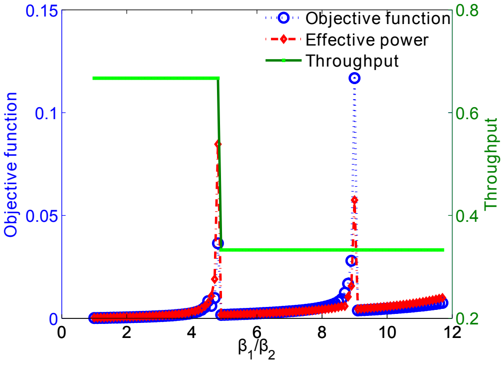

Fig. 3. Plot of throughput, objective function and effective power vs. $\frac{\beta_1}{\beta_2}$. η is assumed to be Gaussian with zero mean and variance = 10^{-4}

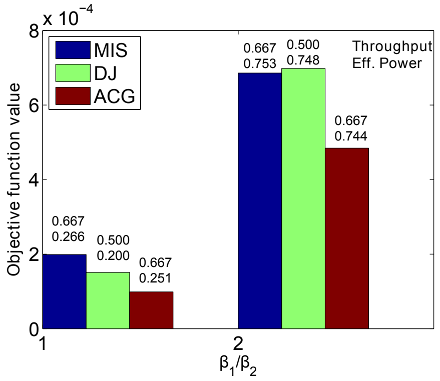

Fig. 4. Comparision of methods with respect to $\frac{\beta_1}{\beta_2}$ ($\lambda = 10^{-4}$, throughput is normalized and effective power is in mWatts).

VI. Without eavesdropper location information

Practical networks are vulnerable to attacks from eavesdroppers whose locations are *not* known a priori. In this section, we relax our assumption of known eavesdropper locations on which the previous analysis was based. We assume path loss based attenuation, with attenuation constant α, for all transmissions. Hence, the channel gain at node j due to transmitter node i becomes $G(i, j) = d_{i,j}^{-\alpha}$. For the rest of the analysis, a 2-D network is considered as shown in Figure 5; the distance between node i and node j is given by $d_{i,j} = ||\mathcal{C}(i) - \mathcal{C}(j)||$, where $\mathcal{C}(i)$ denotes the co-ordinates of node i and $d_{i,j}$ represents Euclidean distance between the position of these two nodes.

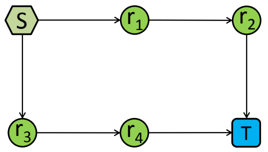

Fig. 5. Six node network for demonstration of jamming without eavesdroppers' location information.

For secure transmission to happen, it is important that no eavesdropper should lie in the transmitting range of a sole transmitter. Concurrent transmissions from other adjacent nodes reduce decodability of transmission even within the transmitting range. Refer to Figure 6 where transmissions corresponding to the activation set $(S \rightarrow r_3), (r_2 \rightarrow T)$ are shown. The area around nodes S and r_2 shown in red is susceptible to eavesdropping and hence it would be referred as *Vulnerability Region* [25], denoted as VR. VR for transmitter i is denoted as $\text{VR}_i = \{\mathcal{C}(j) : SINR_{ij} \geq \beta_1\}$.

Given a network, consisting of relay nodes, source and destinations, we form maximal independent sets (as discussed in Section IV for $\mathcal{G}_1$). For a certain MIS we allow all the nodes who are not in that MIS to act as jammers. So, for an MIS M_j we add the nodes from set $\mathcal{R} \setminus \mathcal{V}^{M_j}$ to M_j and call it an activation set, A'_j. Our objective is to minimize VR such that the SINRs at legitimate nodes are maintained above a threshold (β_1); throughput is above a certain threshold; total transmit power values for each of the activation set is non-negative and upper-bounded. The optimization formulation is as follows:

$$\min \sum_j \text{VR}_j \tag{5a}$$

$$\text{s.t.} \quad SINR_{ij} \geq \beta_1, \; \forall (i,j) \in \mathcal{L}_1 : i, j \in \mathcal{V}^{A'_j}, \forall A'_j \tag{5b}$$

$$\mathbf{x} \geq \mathbf{t} \tag{5c}$$

$$\mathbf{Q}\mathbf{y} = \mathbf{x} \tag{5d}$$

$$\mathbf{y} \leq \sum_j a_j \mathbf{C}_j \tag{5e}$$

$$\sum_{i=1}^{|\widehat{T}_{A'_j}|} P_i \leq P, \quad \forall A'_j \tag{5f}$$

$$P_i \geq P_{th}, \; \forall i \in T_{A'_j}, \forall A'_j \tag{5g}$$

$$P_i \geq 0, \quad \forall i \in \left(\widehat{T}_{A'_j} \setminus T_{A'_j}\right), \forall A'_j \tag{5h}$$

Results

Figure 5 shows a 6 node network where two eavesdroppers are distributed uniformly over the plane. In Figure 6, we plot the 2-D region to identify the *vulnerability region* for the network shown in Figure 5, corresponding to the activation set $\{(S \rightarrow r_3), (r_2 \rightarrow T)\}$. During the two ongoing transmissions, upper middle node (r_1) jams eavesdroppers in its vicinity (if any) and hence we get a distorted circle shaped *vulnerability region*. We further calculate the *expected number of eavesdroppers inside the vulnerability region for each activation set* which is given by, $\sum_{n=1}^{N} n * Pr(n$ eavesdroppers are in $VR)$. Then, we take the weighted average of these expectations, with weights being the activation fractions. For Figure 5 when N=2, the obtained value is **0.5065**, which was **0** when eavesdropper locations were known; this is the "cost" we pay for not knowing the eavesdropper location.

VII. Secrecy Rate

Till the last section, we pursued our aim of optimizing power with the constraint of jamming eavesdroppers. But we have neither introduced any performance metric nor evaluated our improvement in terms of data secrecy. *Secrecy Rate* is an appropriate metric in this aspect. It is defined as the rate at which reliable information is sent from the legitimate transmitter to the intended receiver in the presence of eavesdroppers [14], [18].

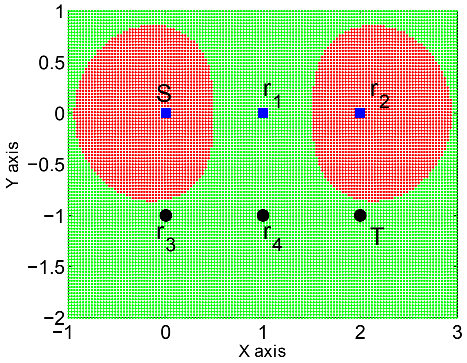

Fig. 6. Plot of vulnerable region (shown in red) for a 2-D network for $\beta_1 = 1$ and $\alpha = 2$.

For Gaussian channels, *Secrecy Capacity* (C_s) [7] is given by $C_s = [C_m - C_e]^+$, where C_m, C_e represent main channel and eavesdropper's channel capacity, respectively and $[x]^+$ is given by $\max(x, 0)$. We devise our schedules with an intention to cause interference to reception at eavesdroppers (by jammers or other ongoing transmission) so that C_e always remains less than C_m for every link and for every eavesdropper.

If the optimization problem introduced in the last section is solvable for certain G, then for that G we can calculate secrecy capacity of the links using the power vector and activation fractions obtained from the solution of that problem. Assuming that we have multiple independent eavesdroppers corresponding to a link between the legitimate transmitter-receiver pair, we express the secrecy capacity of that link (l) as $C_l^s = \min_e(C_l - C_e)$ where C_l is the information capacity of the link and C_e's are calculated for the set of eavesdroppers corresponding to link l. For the Decode and Forward (DF) relay channel, secrecy rate can be expressed as $R_{SD}^s = \min(C_{Sr}^s, C_{rD}^s)$ [12] for almost zero direct channel gain and independent observations by eavesdropper for source to relay and relay to destination transmission, where C_{ij}^s is secrecy capacity of link (i, j). To calculate *wired equivalent secrecy rate* of the network, we first replace the information capacity of every link by corresponding wired equivalent secrecy rate and then apply "max flow, min cut" theorem.

Results

Figure 7 shows that for a fixed set of activation sets, the *secrecy rate* of the network increases with increasing value of $\frac{\beta_1}{\beta_2}$. The sudden drop in secrecy rate is due to the infeasibility of some activation sets, which is already discussed for Figure 3.

VIII. Conclusion & Future Work

We describe a *physical layer security* approach to ensure data secrecy for a multi-hop wireless sensor network. We

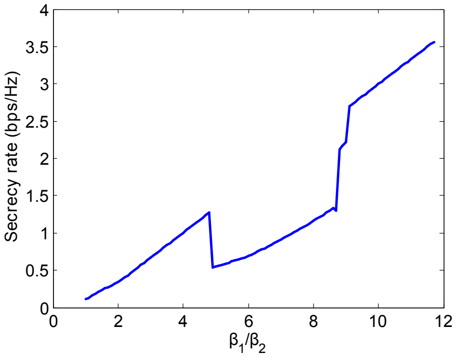

Fig. 7. Secrecy rate variation with respect to $\frac{\beta_1}{\beta_2}$ (the ratio of the target SINR value at legitimate receivers to that at eavesdroppers).

propose methods to find activation sets and optimization problems for power allocation for both the cases, namely with and without information about eavesdroppers' location.

Our analysis is based on single source, single destination multi-hop networks with fixed channel gain. In future, we would study scenarios that involve multiple sources and destinations with fading channels. Also for the low SINR regime we would like to investigate amplify and forward (AF) relaying. Another possible problem that we are yet to look at is the effect of network coding in guaranteeing data secrecy.

References

[1] A. Pathan, H.-W. Lee, and C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges," in *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, vol. 2, Feb 2006, pp. 6 pp.–1048.

[2] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a Link Layer Security Architecture for Wireless Sensor Networks," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, ser. SenSys '04. New York, NY, USA: ACM, 2004, pp. 162–175.

[3] P. Parada and R. Blahut, "Secrecy Capacity of SIMO and Slow Fading Channels," in *Proceedings of International Symposium on Information Theory (ISIT'05)*, Sept. 2005, pp. 2152 –2155.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *CoRR*, vol. abs/1011.3754, 2010.

[5] A. Wyner, "The Wire-tap Channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan 1975.

[6] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[7] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wire-tap Channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[8] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: Securing Sensor Networks with Public Key Technology," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, ser. SASN '04. New York, NY, USA: ACM, 2004, pp. 59–64.

[9] R. Negi and S. Goel, "Secret Communication using Artificial Noise," in *Proceeding IEEE 62nd Vehicular Technology Conference (VTC-2005-Fall)*, vol. 3, Sep 2005, pp. 1906–1910.

[10] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly Jamming for Wireless Secrecy," in *Proceeding IEEE International Conference on Communications (ICC'10)*, May 2010, pp. 1–6.

[11] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper," in *IEEE International Conference on Communications (ICC'11)*, Jun 2011, pp. 1 –5.

[12] L. Lai and H. El Gamal, "Cooperative Secrecy: The Relay-Eavesdropper Channel," in *IEEE International Symposium on Information Theory, 2007 (ISIT 2007)*, Jun 2007, pp. 931–935.

[13] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar 2010.

[14] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical Layer Security for Two Way Relay Communications with Friendly Jammers," in *IEEE Global Telecommunications Conference (GLOBECOM 2010)*, Dec 2010, pp. 1–6.

[15] X. He and A. Yener, "Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming," in *IEEE Global Telecommunications Conference (GLOBECOM 08)*, Dec 2008, pp. 1–5.

[16] S. Gollakota and D. Katabi, "Physical Layer Wireless Security made Fast and Channel Independent," in *Proceedings IEEE INFOCOM, 2011*, Apr 2011, pp. 1125–1133.

[17] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. Leung, "Multi-user Diversity for Secrecy in Wireless Networks," in *Information Theory and Applications Workshop (ITA-2010)*, Feb 2010, pp. 1–9.

[18] P. Pinto, J. Barros, and M. Win, "Techniques for Enhanced Physical-Layer Security," in *IEEE Global Telecommunications Conference 2010 (GLOBECOM 2010)*, Dec 2010, pp. 1 –5.

[19] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless Secrecy in Large-Scale Networks," *ArXiv e-prints*, Feb 2011.

[20] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret Communication in Large Wireless Networks Without Eavesdropper Location Information," in *Proceedings IEEE INFOCOM, 2012*, Mar 2012, pp. 1152–1160.

[21] P. Venkitasubramaniam, T. He, and L. Tong, "Relay Secrecy in Wireless Networks with Eavesdroppers," in *Proc. of Allerton Conference on Communication, Control and Computing*, 2006.

[22] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay Selection for Secure Cooperative Networks with Jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, Oct 2009.

[23] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint Relay and Jammer Selection for Secure Two-Way Relay Networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 310–320, Feb 2012.

[24] I. Krikidis, J. Thompson, P. Grant, and S. McLaughlin, "Power Allocation for Cooperative-based Jamming in Wireless Networks with Secrecy Constraints," in *IEEE GLOBECOM Workshops (GC Wkshps), 2010*, Dec 2010, pp. 1177–1181.

[25] N. Marina and A. Hjorungnes, "Characterization of the Secrecy Region of a Single Relay Cooperative System," in *IEEE Wireless Communications and Networking Conference (WCNC 2010)*, Apr 2010, pp. 1–6.

[26] T. ElBatt and A. Ephremides, "Joint Scheduling and Power Control for Wireless ad hoc Networks," *IEEE Transactions on Wireless communications*, vol. 3, no. 1, pp. 74–85, 2004.

[27] R. Cruz and A. Santhanam, "Optimal Routing, Link Scheduling and Power Control in Multihop Wireless Networks," in *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. INFOCOM 2003. IEEE Societies*, vol. 1, Mar 2003, pp. 702–711.

[28] F. Lo Presti, "Joint Congestion Control: Routing and Media Access Control Optimization via Dual Decomposition for Ad Hoc Wireless Networks," in *Proceedings of the 8th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, ser. MSWiM '05, 2005.

[29] E. Lawler, J. Lenstra, and A. Kan, "Generating all Maximal Independent Sets: NP-hardness and Polynomial-time Algorithms," *SIAM Journal on Computing*, vol. 9, no. 3, pp. 558–565, 1980.

[30] S. C. Ergen. (2004, Sep.) Zigbee/ieee 802.15.4 summary. [Online]. Available: http://people.ece.cornell.edu/land/courses/ece4760/FinalProjects/s2011/kjb79_ajm232/pmeter/ZigBee%20Specification.pdf

[31] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, "Performance Study of IEEE 802.15. 4 Using Measurements and Simulations," in *IEEE Wireless Communications and Networking Conference, 2006 (WCNC 2006)*, vol. 1. IEEE, 2006, pp. 487–492.