Optimal Placement and Power Allocation for Jammers in Wireless Mesh Networks

S. Lall
Department of Electrical,
Electronic and Computer Engineering
University of Pretoria
Pretoria, South Africa

A. S. Alfa
Department of Electrical and
Computer Engineering
University of Manitoba
Winnipeg, Mb Canada
and
Department of Electical,
Electronic and Computer Engineering
University of Pretoria
Pretoria, South Africa

B. T. Maharaj
Department of Electrical,
Electronic and Computer Engineering
University of Pretoria
Pretoria, South Africa

***Abstract*—A novel physical-layer based security method that utilizes jammers to generate additional interference for devices that are eavesdropping on wireless network communication is proposed. The scheme involves the intelligent placement of continuous jammers in order to achieve maximum protection and data confidentiality for wireless mesh networks with multiple eavesdroppers, sources and destinations. Furthermore, the scheme is optimized in terms of the transmitting power associated with each jammer so that the energy expended by the jammers is kept at a minimum. The protection scheme precludes the use of any cryptographic techniques and is only physical-layer based. The security method is modeled as a minimization mixed integer non-linear problem and is approximated as the sequential solution of two linear optimization sub-problems relating to the placement and power allocation of the wireless jammers. The placement of the jammers takes the form of a multiple demand multidimensional knapsack problem with a minimization objective. The power allocation problem is modeled as a linear real-valued minimization optimization problem. The performance of the proposed security method is evaluated through appropriate simulations conducted on random network instances.**

***Index Terms*—Jammer Placement; Jammer Power Allocation; Optimization; Wireless Jammers; Wireless Mesh Networks; Wireless Network Security.**

I. Introduction

Wireless networks are gaining widespread use and popularity because of their progressive increase in affordability and convenience. Owing to the improved facilitation of communication and data transfer, wireless networks are being deployed in numerous modalities, ranging from wireless local area networks to mesh and sensor networks [1]. Wireless networks are often seen as a more attractive option to their wired network counterpart due to their increased mobility, expandability, cost efficiency and ease of integration. As a result of the need for mobility, data is broadcast using radio technology which implies that any unintended receiver in range will be able to listen in on the transmission and compromise network confidentiality.

Wireless Mesh Networks (WMNs) have numerous applications in both civilian and military based environments. As a result of its low-cost set-up and scalability, they are ideal for the formation of communication networks in rural areas where there is a lack of infrastructure [2]. In the military domain, WMNs offer an efficient solution for the deployment of military tactical networks [3]. The networks need to be resilient and be able to withstand harsh propagation channels and interference, as well as constant changes in the network topology. The primary applications of WMNs is for sending out information related to troops positions and conditions which are termed as situational awareness communications. WMNs are rapidly gaining popularity in military functional areas including intelligence, war fighting and logistics to exchange vital information between separate small units and operation centers in a quick and optimal way [4].

The main disadvantage of WMNs is its susceptibility to interference and eavesdroppers that are able to intercept and listen in on the communication between the devices in the networks. Eavesdroppers can act as nonlethal weapons to combatants at war and can have dire consequences if vital information is obtained by the adversaries. Owing to the emerging and prevalent use of WMNs in military domains, protecting the information contained in the networks is of utmost importance in this information driven age. A physical-layer based protection mechanism is through the deployment of jammers which are used to ensure private communication within networks.

The security method proposed in this paper is used to maintain data confidentiality in WMNs through the use of protective jammers which generate interference for eavesdroppers, thereby preventing them from obtaining any meaningful information. The proposed scheme seeks to overcome the weaknesses evident in cryptographic based protection methods by strategically placing protective jammers in order to enhance the security of WMNs. The efficiency of the scheme is increased by minimising the number of jammers required to protect an area and reducing the power consumption levels of the jamming devices. The proposed security model is

978-1-4799-8091-8/15/$31.00 ©2015 IEEE

subject to constraints which ensure that sufficient interference is generated for malicious devices that seek to obtain confidential information, while legitimate communication within the network is not affected.

II. Prior Work

A. Wireless Network Protection

As a result of the open and shared broadcast medium, information theft is a rising concern in wireless networks. WMNs suffer from two main problems; one which relates to routing and multi-hop technology and the other which relates to the security of the networks. There is little attention being paid to securing WMNs and maintaining data confidentiality as opposed to the large amount of literature dedicated to providing solutions to the routing problems [5]. Confidentiality relates to preventing information leakage and securing messages that are exchanged between the nodes so as to prevent eavesdroppers from obtaining any critical information. Cryptographic techniques involving the application of traditional algorithms, such as Diffie-Hellman, RSA and elliptic curve cryptography, are largely used for securing networks and maintaining data confidentiality [6]. There are however several shortcomings related to utilizing cryptographic methods, such as increased complexity in protocol design, vulnerability to denial of service attacks as well as the lack of effective user identity protection mechanisms [7]. Although cryptography is able to provide authentication and confidentiality in wireless ad hoc networks, a prominent challenge in securing WMNs, as opposed to other ad hoc networks, is accounting for the numerous different technologies in the network nodes as well as dealing with the heterogeneous nature of the network. As it stands, these techniques have high memory and energy requirements and with the application to WMNs, there is added complexity and cost [6]. With the emergence of ad hoc and decentralized networks, providing security at the physical layer, in contrast to cryptographic techniques which are applied at the higher layers, has been of interest [8].

Physical layer security aims to maximize the rate of reliable information from the source to the destination while maintaining data confidentiality against eavesdroppers. The notion of exploiting the nature of the wireless medium to strengthen the security in wireless networks was first introduced by Wyner [9]. Wyner proposed that perfect secrecy can be achieved in wireless communication links without the use of any encryption methods. It was proven that when the eavesdroppers channel is a degraded version of the communication channel, which it wants to eavesdrop upon, the source and destination are able to ensure privacy of their messages. This is achieved through stochastic encoding of the additive noise that is used to impair the eavesdroppers channel. Through this method, there is an equivocation that is induced at the eavesdropper and by setting the equivocation rate to be arbitrarily close to the message rate, perfect secrecy can be achieved. The secrecy rate of a communication channel can be improved by increasing the signal to noise ratio (SNR) of the destination node or by decreasing the SNR of the eavesdropper. The SNR at the destination node can possibly be improved by shortening the distance between source and destination; however this is generally not feasible. Thus, in order to reduce the SNR at the eavesdropper, a suitable method would be the deployment of jamming devices which are capable of inducing controlled inference in the eavesdroppers channel [10].

B. Friendly Jammers and Power Allocation

Even though jamming is typically used for degrading the performance of networks, it has found application as a way of enhancing the security of a network by causing interference to the eavesdroppers so as to reduce its ability to decode the source's information [11]. In this case, the jamming is termed as being "friendly" or "protective". Friendly jammers are used as a way of providing physical layer security by protecting the wireless networks against information leakage.

A large portion of literature is dedicated to the use of intermediate relays to act as friendly jammers that are used to generate artificial noise or interference directed at eavesdroppers. Lai and El Gamal [12] made use of intermediate relay nodes for performing cooperative jamming by ensuring communication confidentiality from eavesdroppers. Similarly, cooperative jamming was studied in a multiple antenna scenario by Goel and Negi [13]. Al-nahari proposed and investigated a jamming scheme that creates interference at the eavesdropper during the decode-and-forward phase [14]. The interference can also be generated during the cooperative phase as suggested by Dong *et al.* [15]. It is assumed that the relays are trusted third parties unlike the work considered by Zhang *et al.* [16] in which external friendly jammers are used to protect the messages sent from the source to the destination against the relay which is used to forward the message. Traditional optimisation methods and the use of game theory are used to for determining the power values allocated to the friendly jammers given that there is a power constraint that the jammers have to adhere to [11], [17]-[19].

In the literature relating to the use of friendly jammers, it was assumed that the friendly jammers were placed far enough from the receivers or destination nodes to not have any detrimental effect on the communication channel in which the data that it wishes to protect resides. It is simply considered as a trade-off in the power allocation strategies of the friendly jammers [20]. However in practical scenarios, there is bound to be induced interference from the friendly jammer and it is not always possible to control it so that the SNR at the destination is maintained, especially in multiple source, eavesdropper and destination scenarios. Bayat *et al.* [20] considered a scenario with multiple source-destination pairs, with multiple jammers but a single eavesdropper. The authors propose an algorithm based on matching theory that matches every source and destination pair with a particular jammer. Although the authors propose a generalised scenario in comparison to the majority of literature which deals with single source-destination scenarios [11]-[19], the jammers are assumed to have no effect on the legitimate communication link and only a single eavesdropper is considered. A more

realistic scenario with multiple eavesdroppers and topologies in which source and destination nodes are not paired should be considered.

Shen *et al.* [21] proposed a technique called "Ally Friendly Jamming" in which connectivity between the source and destination is maintained even when the jamming signals affect the source and destination pair as well as the eavesdropper. This is achieved through the removal of the interference caused by the jammers to the legitimate receiver through signal processing techniques that utilise secret keys which is only known to the receiver and not the eavesdropper. The problem of the key possibly being leaked to the eavesdropper during the key exchange process is analogous to that experienced in networks utilising cryptographic methods for preserving data confidentiality. There is also added computation that needs to be performed at the receiver to remove the interference which increases the latency and is not preferable, especially in military and emergency scenarios where time is of utmost importance. It is therefore beneficial to consider the effect of jammer placement and power allocation in preventing eavesdroppers from intercepting network communication while not disrupting the legitimate communication taking place between the source and destination nodes.

III. Contributions

A novel method of utilizing jammers to protect WMNs against eavesdropper nodes in a multi-hop network with multiple sources, destinations and eavesdroppers is proposed. A mathematical model is developed for the joint optimal placement and power allocation of the wireless jammers. The model takes into account not only the effect that the jammers have on the malicious nodes, but also the impact it has on the communicating nodes. Measures are taken to prevent the jammers from having any ill-effect on the communication channels they are protecting. This is achieved through the careful placement of the jammers so that network continuity is maintained, while the principal purpose of degrading the eavesdroppers channel through controlled interference, is accomplished. The protection scheme precludes the use of any cryptographic techniques and is only physical-layer based. Focus has been placed on the ease of practical implementation of the proposed scheme as no additional computation or complexity is required from the legitimate communication nodes; only the intelligent placement of simple continuous jammers is needed to achieve maximum protection. The scheme is further optimized in terms of the transmitting power associated with the jammers so that the energy expended through use of the jammers is kept at a minimum. This work is largely targeted for protecting wireless networks in military domains which are very flexible and uncertain. To the best of our knowledge, there has not been any work jointly addressing protective jammer placement and power allocation which is used for the effective and efficient protection of multi-hop military-based networks with multiple sources, destinations and eavesdroppers.

IV. Method

A. Network Model

The environment used for simulating and testing the optimization problems is one which aims to closely represent the highly mobile, non-deterministic nature of WMNs in military battlefields where it would be difficult to physically prevent malicious nodes from entering the mesh network. The jammers are thus placed interspersed amongst the legitimate nodes and the malicious nodes in such a way so as to prevent the malicious nodes from gaining any information while not jeopardizing the communication between the legitimate nodes. The jamming devices are assumed to be fitted with omnidirectional antennas and generate random noise. The legitimate communication nodes are also assumed to be fitted with omnidirectional nodes and function as both transmitters and receivers. Given a set of potential jamming locations, the goal of the scheme is to select the minimum number of jamming locations at which the jammers can be placed such that there is interference free reception by legitimate receivers and no malicious nodes are able to gain information as a result of a decrease in its SNR. A node is considered jammed if the combined jamming effectiveness of all jammers on that particular node is above some threshold value.

The jamming effectiveness is modeled by the variable q_k^j and depends on the power of its electromagnetic emission which is inversely proportional to the squared distance from the jamming device, j, to the node being jammed, k [22]. This is shown as:

$$q_k^j = \frac{\lambda_j}{(X_k - X_j)^2 + (Y_k - Y_j)^2} \tag{1}$$

Where $\lambda_j \in \Re$ is a constant that relates to the transmitting power of the jamming device, (X_k, X_j) and (Y_k, Y_j) are the coordinates of the jamming device and the node being jammed respectively.

B. Problem Formulation

The mixed integer non-linear problem regarding the optimal jammer placement and power allocation is given as:

$$Min.\ \ z = \sum_{k=1}^{N} (c_k + \rho\lambda_k) x_k \tag{2}$$

s.t.

$$\sum_{k=1}^{N} q_k^j x_k \leq \delta_L,\ \ j = 1, 2, ..., m \tag{3}$$

$$\sum_{k=1}^{N} q_k^j x_k \geq \delta_M,\ \ j = m+1, m+2, ..., m+w \tag{4}$$

$$\lambda_k x_k \leq \lambda_{max},\ \ \forall k \tag{5}$$

$$\lambda_k \geq 0,\ \ \forall k \tag{6}$$

$$x_k \in \{0, 1\},\ \ \forall k, \tag{7}$$

where

- c_k: The cost of installing a jamming device at location k. In a battlefield scenario, it may be risky to place a jammer very close to a malicious node, thus the associated installation cost will be higher.
- ρ: Factor that makes the cost of providing power be the same units as the cost of locating jammers.
- λ_k: The decision variable which is associated with the transmitting power of the jammers.
- x_k: The binary decision variable where 1 indicates that a jamming device is installed at location k and 0 indicates no jamming device at that location.
- N: The number of potential jamming locations.
- δ_L: Jamming threshold value for the legitimate nodes.
- δ_M: Jamming threshold value for the malicious eavesdropping nodes.
- λ_{max}: Maximum value for λ_k.
- m: The number of legitimate communication nodes.
- w: The number of eavesdropper nodes.
- q_k^j: The jamming effectiveness, as given in equation (1), experienced by node j from the jammer placed at location k. j is used to denote all the legitimate communication nodes and all the eavesdropper nodes in the wireless network. Nodes $j = 1$ to m denote the legitimate communication nodes, and nodes $j = m + 1$ to $m + w$ denote the eavesdropper nodes.

In addition, we define a vector $\mathbf{x} = \{x_1, x_2, ..., x_N\}$ which represents the solution to the problem.

In order to solve linear problems, the linear constraints are sketched and a feasible region is obtained, after which, an optimal solution is found at one of the corner or extreme points of the region. However, with regards to non-linear problems, it is significantly more difficult to solve the problem and is often reformulated as linear integer programming problems [23], [24]. The problem, as formulated, is computationally intensive and highly complex as a result of its non-linearity. Adding to the difficulty of solving the problem, is determining the factor ρ that is used to equate the units pertaining to the cost of placing the jammers to the cost of providing power. Therefore, an alternate approach is taken. The problem is decomposed into two sub-problems which serve as an approximation and the decision is then made sequentially. By this we mean that the number of jammers and their locations are first determined, and then the power allocation sub-problem associated with the selected jammers is solved. Essentially, an initial value, or a maximum transmitting power is set for all jammers; once the minimum number of jammers required to protect a certain network is established, the transmitting power is further decreased to an amount that satisfies all constraints thereby saving energy and increasing cost efficiency.

1) Jammer Placement Sub-problem: The jammer placement sub-problem is modeled as multiple demand multi-dimensional knapsack problem. Knapsack problems are known to be difficult to solve and are considered NP-hard [25]. This sub-problem aims to find the minimum number of jammers from N potential jamming locations such that the interference caused by the jammers do not affect the communication taking place between the legitimate nodes but reduces the SNR of the malicious eavesdropping nodes so that they are unable to obtain any information from the communicating nodes. The problem formulation is given as:

$$Min. \;\; z = \sum_{k=1}^{N} c_k x_k \tag{8}$$

s.t.

$$\sum_{k=1}^{N} q_k^j x_k \leq \delta_L, \;\; j = 1, 2, ..., m \tag{9}$$

$$\sum_{k=1}^{N} q_k^j x_k \geq \delta_M, \;\; j = m+1, m+2, ..., m+w \tag{10}$$

$$x_k \in \{0, 1\}, \;\; \forall k, \tag{11}$$

where the parameters are defined as for the main problem. The solution to this sub-problem will be a vector $\mathbf{x}^* = \{x_1^*, x_2^*, ..., x_N^*\} \in \{0, 1\}^N$. We also define L to represent the number of optimal jammer locations as $L = \sum_{k=1}^{N} x_k^*$. Further let $\mathcal{L} = \{i_1, i_2, ..., i_L\}$ where $x_{i_v}^* = 1$.

2) Power Allocation Sub-problem: The optimization sub-problem related to the power allocation of the jammers is given as:

$$Min. \;\; z = \sum_{k \in \mathcal{L}} \lambda_k \tag{12}$$

s.t.

$$\sum_{k \in \mathcal{L}} q_k^j \leq \delta_L, \;\; j = 1, 2, ..., m \tag{13}$$

$$\sum_{k \in \mathcal{L}} q_k^j \geq \delta_M, \;\; j = m+1, m+2, ..., m+w \tag{14}$$

$$\lambda_k \leq \lambda_{max}, \;\; \forall k \tag{15}$$

$$\lambda_k \geq 0, \;\; \forall k, \tag{16}$$

where the parameters are as previously defined. The solution to this sub-problem will be a vector $\boldsymbol{\lambda}^* = \{\lambda_1^*, \lambda_2^*, ..., \lambda_L^*\}$.

C. Approach

The optimization problems are solved using IBM ILOG CPLEX solver. The positions of the legitimate nodes and the malicious eavesdropping nodes are randomly generated. The parameters that are used for evaluating the protection scheme is given in table 1. The set of discrete points that constitute possible locations of where to place jammers was determined by superimposing a uniform grid, with a grid-space of 0.5, over the target area where the intersection points correspond to possible locations for placing a jammer. A visual depiction of the jammer placement of a random scenario is shown in fig. 1.

The branch-and-cut method and simplex method is used for solving the jammer placement and power allocation problems respectively. The simplex method is a simple way of obtaining the solution to a real-valued optimization problem. It basically moves along the edges of the polytope defined by the constraints, from vertex to vertex with successively

TABLE I
SIMULATION PARAMETERS

Parameter	Value
N	441
δ_L	1.15
δ_M	0.85
λ_j	1.0
Area	10x10
c_k for all jammers	1.0

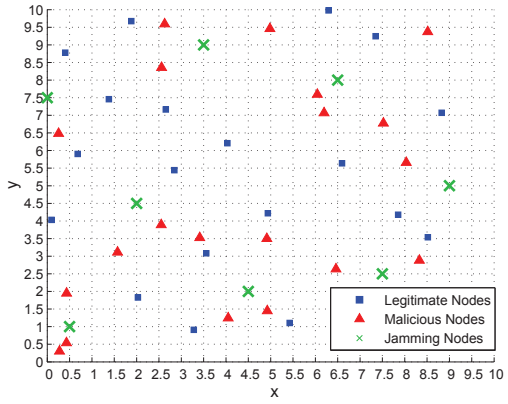

Fig. 1. Example of a random scenario showing the optimized number of jammers and their locations for protecting the network.

smaller values of the objective function, until the minimum is reached. The branch-and-cut method, on the other hand, is a more complicated method for solving mixed integer linear problems. In general, the branch-and-cut method solves a sequence of linear programming relaxations of the integer programming problem. The cutting plane method improves the relaxation of the problem to more closely approximate the integer programing problem, and the branch-and-bound algorithms use a sophisticated divide and conquer approach to solve the problem. The branch-and-cut algorithm used for solving the integer jammer placement problem is given as:

1) Initialization: denote the initial jammer placement integer problem as ILP^0 and set the active nodes to be $L = \{ILP^0\}$. Set the upper bound of the total number of jammers to be $\overline{z} = +\infty$. Select one problem $1 \in L$ and set its lower bound to be $\underline{z_1} = -\infty$.
2) Termination: If $L = \emptyset$, then the solution x^* which yielded the incumbent objective value z is optimal. If no such x^* exists $(z = +\infty)$ then the integer linear program is infeasible.
3) Problem selection: Select and delete a problem ILP^1 from L.
4) Relaxation: Solve the linear programming relaxation of ILP^1. If the relaxation is infeasible, set $\underline{z_1} = +\infty$ and go to step 6. If the relaxation is feasible, then let z_1 denote the optimal objective value of the relaxation if it is finite and let x^{1R} be an optimal solution; otherwise set $\underline{z_1} = -\infty$.
5) Add cutting planes: Search for cutting planes that are violated by x^{1R}; if any are found, add them to the relaxation and return to Step 4.
6) Fathoming and Pruning:If $\underline{z_1} \geq \overline{z}$ then go to Step 2. Otherwise if $\underline{z_1} < \overline{z}$ and x^{1R} is integral feasible, update $z = z_1$, delete from L all problems with $z_1 \geq z$, and go to Step 2.
7) Partitioning: Let S^{1j} be a partion of the constraint set S^1 of problem ILP^1. Add problems ILP^{1j} to L where ILP^{1j} is ILP^1 with feasible region restricted to S^{1j} and $\underline{z_{1j}}$ for $j = 1, 2, ..., k$ is set to the value of $\underline{z_1}$ for the parent problem 1. Go to step 2.

V. RESULTS

A. Jammer Placement

The effect of varying the number of malicious nodes on the average number of jammers required to protect a network with 20 randomly dispersed communicating nodes is shown in fig. 2. An average over a 100 simulation runs were obtained for the varying number of malicious nodes. As can be seen from fig. 2, there is an overall decrease in the rate at which the average number of jammers increase. This can be attributed to the fact that the area of the network remains the same as the number of malicious nodes increase thereby making the network more densely packed.

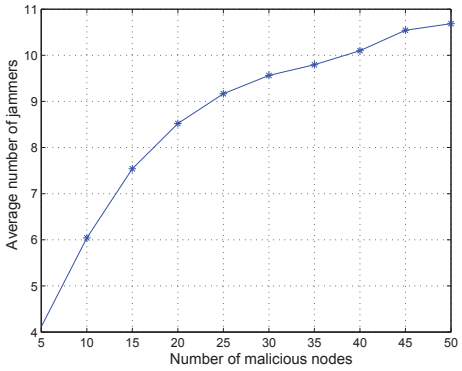

Fig. 2. The effect of the number of malicious eavesdropping nodes on the average number of jammers required to protect an area.

On the other hand, as seen in fig. 3, increasing the number of legitimate nodes while keeping the number of malicious nodes constant at 20, exhibits a fairly linear relationship with regards to the number of jammers needed to protect the network. This is a result of the added restrictions on the placement of the jammers due to the increase in the legitimate communication nodes; more jammers need to be placed closer to the malicious nodes thereby increasing the jammers to malicious nodes ratio.

B. Jammer Power Allocation

The transmitting power which is directly proportional to λ_j can be optimized for a particular scenario by minimizing λ_j associated with each jammer, while ensuring that it is still able to cause sufficient interference to the malicious nodes.

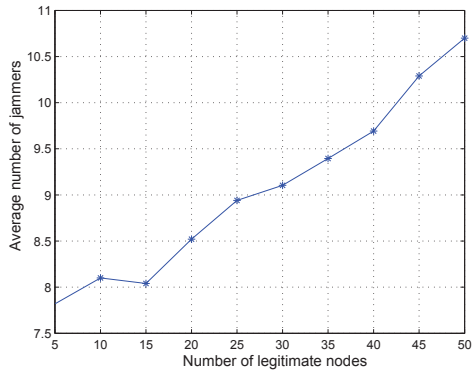

Fig. 3. The effect of the number of legitimate communication nodes on the average number of jammers required to protect an area.

For the initial jammer placement problem, λ_j is set to 1 for all the jammers and thus $\lambda_{max} = 1$ for the associated power allocation subproblem.

A plot of the total power reduction for 20 random scenarios over a 10x10 grid with 20 legitimate nodes and 20 malicious nodes is shown in fig. 4. It can be seen that the power reduction fluctuates for the varying network scenarios. The percentage reduction strongly depends on the topology, with as high as a 26% reduction and as low as 2% reduction being observed.

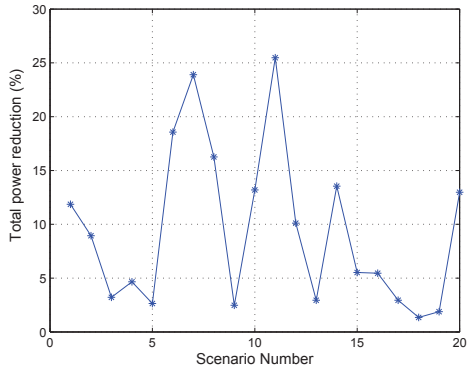

Fig. 4. Total jammer power reduction for 20 random scenarios.

VI. Conclusion

The need for protecting communication within networks is of utmost importance especially in environments where information is critical and loss thereof can result in disastrous consequences. The most popular method for ensuring data confidentiality is through the use of cryptographic techniques; however, as a result of the decentralised nature and power limited network nodes of WMNs, it is important to consider physical-layer based methods such as jamming. A protection scheme utilizing jammers to protect networks against randomly dispersed malicious eavesdropping devices is proposed. The efficiency of the scheme is increased by minimising the number of jammers required to protect an area and reducing the power consumption levels of the jamming devices. By carefully placing jammers to protect a particular WMN, the number of jammers can be significantly reduced while still providing high levels of security. The solution to the modelled nonlinear optimization problem was approximated as the sequential solution to two linear sub-problems. The branch-and-cut algorithm was used for solving the jammer placement subproblem and the simplex algorithm was employed for solving the power allocation sub-problem. The effect of varying the number of legitimate communication nodes and the number of malicious eavesdropping nodes were analysed. In worst case scenarios, approximately 11 jammers were required to protect a 50 node network against 20 eavesdropper nodes. After optimizing the transmitting power for the jammers, it was found that the total percentage power reduction was highly dependent on the topology and jammer placement. It thus highlights that the locations of the jammers are of paramount importance and emphasis is placed on the method of selecting these jammers. Future work involves the development of highly efficient algorithms for solving the multidimensional knapsack problem associated with the jammer placement.

References

[1] W. Xu, W. Trappe, W. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in *Proc. MobiHoc.*, 2005, pp. 46–57.

[2] S. Jayaprakasam, T. C. Chuah, and S. W. Tan, "Collaborative mesh networking for low cost wireless coverage in rural areas," in *Proc. IEEE Symp. Industrial Electronics Applications*, 2009, pp. 313–318.

[3] D. J. Shyy, "Military Usage Scenario and IEEE 802.11s Mesh Networking Standard," in *Proc. IEEE Military Communications Conf*, 2006, pp. 1–7.

[4] H. Hayes. (2012, Aug. 1) How mesh networks extend military comm. [Online]. Available: http://www.fedtechmagazine.com/article/2012/08/how-mesh-networks-extend-military-comm.

[5] R. DiPietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks - A survey," *Computer Communications*, vol. 51, no. 1, pp. 1–20, Sep. 2014.

[6] V. M. Rohokale, N. R. Prasad, and R. Prasad, "Reliable and secure cooperative communication for wireless sensor networks making use of cooperative jamming with physical layer security," *Wireless Personal Communications*, vol. 73, no. 3, pp. 595–610, May 2013.

[7] Z. Wang, Y. Xing, Q. Wang, and W. Liu, "A wireless mesh network secure access method based on identity-based signature," in *Proc. Wireless Communications Networking and Mobile Computing Conf.*, 2010, pp. 1–4.

[8] M. DiRenzo and M. Debbah, "Wireless physical-layer security: The challenges ahead," in *Proc. Int. Conf. Advance Technologies for Communications*, 2009, pp. 313–316.

[9] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[10] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[11] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: Interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 1–10, Jan. 2010.

[12] L. Lai and H. ElGamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[13] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[14] A. Y. Al-nahari, I. Krikidis, A. S. Ibrahim, M. I. Dessouky, and F. E. A. El-Samie, "Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers," *Trans. Emerging Tel. Tech*, vol. 25, no. 4, pp. 445–460, Apr. 2014.

[15] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Jun. 2009.
[16] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.
[17] J. Qu, Y. Cai, J. Lu, A. Wang, J. Zheng, W. Yang, and N. Weng, "Power allocation based on stackelberg game in a jammer-assisted secure networks," in *Proc. Int. Conf. Cyberspace Technology*, 2013, pp. 347–352.
[18] M. Ara, H. Reboredo, F. Renna, and M. R. D. Rodrigues, "Power allocation strategies for ofdm gaussian wiretap channels with a friendly jammer," in *Proc. Int. Conf. Communications*, 2013, pp. 3413–3417.
[19] J. Yang, I. Kim, and D. Kim, "Power-constrained optimal cooperative jamming for multiuser broadcast channel," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 411–414, May 2013.
[20] S. Bayat, R. H. Y. Louie, Z. Han, and Y. Li, "Physical-layer security in distributed wireless networks using matching theory," *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 5, pp. 717–732, May 2013.
[21] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in *Proc. IEEE Symp. Security and Privacy*, 2013, pp. 174–188.
[22] C. W. Commander, P. M. Pardalos, V. Ryabchenko, S. Uryasev, and G. Zrazhevsky, "The wireless network jamming problem," *Journal of Combinatorial Optimization*, vol. 14, no. 4, pp. 481–498, Mar. 2007.
[23] B. S. Awoyemi, B. T. Maharaj, and A. S. Alfa, "Resource allocation for heterogeneous cognitive radio networks," in *Proc. IEEE Wireless Communications and Networking Conf.*, 2015, pp. 1777–1781.
[24] S. D. Barnes, B. T. Maharaj, and A. S. Alfa, "Spectrum opportunity forecasting for energy efficient sensing in cognitive radio networks," in *Proc. IEEE International Symposium on Telecommunications Technologies*, 2014, pp. 128–132.
[25] H. Kellerer, U. Pferschy, and D. Pisinger, *Knapsack Problems*. Berlin, Germany: Springer, 2004.