University of Nevada, Reno

REAL-TIME INFERENCE OF TOPOLOGICAL STRUCTURE AND VULNERABILITIES FOR ADAPTIVE JAMMING AGAINST COVERT AD HOC NETWORKS

A Thesis Submitted in Partial Fulfillment
of the Requirements for the Degree of Master of Science in
Computer Science and Engineering

by

Vahid Behzadan

Dr. Shamik Sengupta / Thesis Advisor

May 2016

**UNIVERSITY
OF NEVADA
RENO**

THE GRADUATE SCHOOL

We recommend that the thesis prepared
under our supervision by

VAHID BEHZADAN

entitled

REAL-TIME INFERENCE OF TOPOLOGICAL STRUCTURE AND VULNERABILITIES FOR ADAPTIVE JAMMING AGAINST COVERT AD HOC NETWORKS

be accepted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE

Shamik Sengupta, Ph.D. – Advisor

Murat Yuksel, Ph.D. – Committee Member

Yantao Shen, Ph.D. – Graduate School Representative

David W. Zeh, Ph.D. – Dean, Graduate School

May 2016

ABSTRACT

With the emerging reliance of critical communications on ad hoc architectures, ensuring the security of such networks is paramount. Even though the independence of ad hoc networks from a single point of failure is seen as an advantage, the distributed nature of ad hoc communications introduces a variety of complex security problems. These problems are further intensified in mission critical networks deployed in hostile environments such as modern battlefields, where analysis and disruption of opponents' wireless communications is an essential component of combat. Therefore, resilience of network connectivity to disruption and concealment of communications is a priority in design of critical ad hoc networks. To this end, various techniques have been proposed for mitigation of disruptive attacks, the majority of which focus on routing and upper layers of the protocol stack, while very few consider implementing mitigation in the physical and link layers.

This thesis aims at demonstrating the vulnerability of covert ad hoc networks to adaptive jamming attacks that rely only on physical layer parameters. A novel transmission timing analysis technique is proposed to estimate the existence of hop-to-hop links based on the synchronicity of transmission timings in both time and frequency domains, complemented with a minimal thresholding method for classification of link estimations. Furthermore, this work proposes a computationally efficient method for identification of the most vulnerable region of the network via graph theoretical modeling. The computational cost of this method is further reduced by employment of a fast search space generation algorithm, as well as percolation modeling of the system. Both methods are shown to increase the efficiency of adaptive jamming when no a priori information about the topology or protocols of the network is available. Performance of the proposed methods is measured through graph theoretical and network simulations.

“The supreme art of war is to subdue the enemy without fighting.”

THE ART OF WAR - SUN TZU

ACKNOWLEDGEMENTS

I am forever grateful for the constant support, patience, and invaluable guidance of my advisor, Dr. Shamik Sengupta. His exceptional extent of knowledge and enthusiasm for research have been major sources of motivation for my work. I also thank my committee members, Prof. Murat Yuksel and Prof. Yantao Shen, for their valuable critiques and comments.

Graduate education and research is an inherently lonely path. I owe the survival of my social self to my colleagues in the Computer Networking Lab, whose liveliness, friendship and support have never failed to ease the ever-increasing pressure of work. Thank you guys.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

The emergence of ad hoc networks in mission critical applications is following a growing trend. Elimination of the need for a central communications infrastructure appeals to many scenarios as it allows seamless and quick deployment of networks, which is an essential requirement of many military communication networks. This advantage has given rise to a surge in development and deployment of critical civilian and tactical ad hoc networks: Wireless sensor networks operating in ad hoc mode are envisioned to be widely deployed in battlefields of the future [28], mobile communications are rapidly evolving towards technologies that no longer require a central relay and controller [9], and the emergence of swarms of UAVs for transportation, surveillance and combat applications cannot be imagined without mobile ad hoc networking to facilitate inter-UAV communications and formation control [3].

With this upcoming reliance of critical communications on ad hoc architectures, ensuring the security of such networks is paramount. Even though the independence of ad hoc networks from a single point of failure is seen as an advantage in the context of security, the distributed nature of ad hoc protocols introduces a variety of complex security problems specific to this type of networks [10]. The problem is further intensified in mission critical networks deployed in hostile environment such as modern battlefields, where analysis and disruption of opponents' wireless communications is an essential component of combat. Therefore, resilience of network connectivity to disruption and concealment of communications is a priority in design of critical ad hoc networks. To this end, various techniques have been proposed for mitigation of jamming in ad hoc networks, such as jamming-resistant routing [11] and deployment of decoy nodes [7]. While a great number of mitigation techniques focus on routing and upper layers of the network, very few consider implementing mitigation in the physical and link layers [6].

To demonstrate the necessity of physical and MAC layer defense techniques, this thesis presents a feasible adaptive attack framework for efficient jamming of multihop ad hoc networks operating. The proposed attack is aimed for covert networks whose communications are completely encrypted and therefore no information about their topology and protocols is available. To overcome this obstacle, a novel traffic analysis technique is proposed that estimates the existence of hop-to-hop links based on synchrony of transmission timings in time and frequency domains. Also, we present a study on the suitability of various adaptive thresholding techniques for labeling the estimated links, concluded with the proposal of an efficient and minimal metric. Equipped with this tool for estimation of ad hoc network topologies, an adaptive jammer can increase the impact of its attack by adjusting its transmission and targeting parameters according to the inferred topology. We then investigate further enhancement of such attacks by limiting the effective jamming area to a subset of the target network. To determine the criteria for feasibility of such attacks on critical networks with encrypted transmissions, we look into the problem of identifying the most vulnerable region of a multiphop communications network from its topological properties. Considering the energy and time limitations on practical implementations of this attack, we propose a computationally feasible method of estimating the maximally vulnerable point based on graph theoretical modeling and the continuum percolation theory. Our proposed framework is solely based on physical and lower MAC layer observations of ad hoc networks, thus illustrating the insufficiency of upper-layer countermeasures in mission-critical applications.

The remainder of this thesis is organized as follows: Chapter 2 presents the target and attacker models and formulates the problem. Chapter 3 describes the traffic analysis technique, followed in by the details of vulnerable region identification method in Chapter 4. Evaluation of the effectiveness and efficiency of the proposed framework is presented in Chapter 5, and Chapter 6 concludes the thesis with suggestions on future areas of work.

Chapter 2

Problem Statement

The aim of this work is to investigate the vulnerability of ad hoc networks to smart and adaptive jamming attacks that solely rely on physical layer activities of the target. In essence, a jamming attack is intentional disruption of communications by introduction of interference to the target's received signals. This is usually achieved by transmission of high powered signals on the same frequency channel as the receiver's. Transmission of jamming signal can be constant and continuous for the duration of the attack, which is costly in terms of energy consumption and can be easily detected and mitigated. Alternatively, the jammer may attack discontinuously by transmitting at random moments or selectively choosing the transmission times based on certain criteria, such as the state of the target. This state may be dynamic due to defensive mechanisms such as jamming recovery and self-healing techniques, therefore a sustained attack on this category of networks requires the attacker to be reactive towards changes in the target. Such attacks are known as Adaptive Jamming, defined as disruptive attacks whose parameters such as transmit power and transmission timings are adjusted according to the observable state of the target to maximize the impact of disruption.

Adaptive jamming may be continuous or discontinuous, and requires a mechanism for monitoring the target's condition. The flexibility of this attack and its adaptive nature forces the targets to employ more sophisticated detection and mitigation techniques, many of which are developed for upper layers of the network [24]. To demonstrate the inadequacy of such mitigation approaches, this work considers the case of a covert network targeted by an adaptive jammer, the descriptions and assumptions of which are detailed in this chapter.

2.1 Target Model

To analyze the most stringent conditions in ad hoc networks, the case of a typical covert network such as a tactical communications setup is considered. This network is consisted of N homogeneous nodes communicating in parallel over an ad hoc, multihop configuration. The nodes are assumed to be static relative to each other during each attack cycle, which can represent fixed position networks such as sensor nodes deployed for Intelligence, Surveillance and Reconnaissance (ISR) purposes, mobile meshes moving in formation such as Tactical Mobile and Flying Ad hoc Networks (MANETs and FANETs), and dynamic configurations with slow rates of change (e.g. Obstacle Avoidance). The independent and dynamic nature of such ad hoc networks in terms of topology and geometry, combined with the requirement of maintaining connectivity is shown to be suitably captured by the Poisson-Boolean model [34]. Accordingly, the distribution of target nodes in 2D space is considered to follow the Poisson Boolean model $G(\lambda, r)$, where λ is the density of nodes in the operation region of the network and r is the maximum range of communications for all nodes. In this model, the probability that there are k nodes in an area A is given by equation (2.1):

$$p(N_A = k) = e^{-\lambda A \frac{(\lambda A)^k}{k!}} \tag{2.1}$$

As is the case with the majority of current ad hoc technologies, the transmission mode of the network is considered to be omnidirectional. Due to the potential employment of privacy and security mechanisms by the network, length and duration of packets may change in the multihop forwarding process. It is also assumed that every layer of this network's transmissions are encrypted.

2.2 Attack Model

In line with the assumptions presented for the target, the jammer must be capable of targeting both static and mobile ad hoc networks. Radio jamming attacks are successful only when the target is in the effective range of jamming, therefore it is essential for the attack platform to be mobile so that it can track the target network while it is moving. Also, to capture performance of this attack in terms of practical feasibility, the attack model is limited to deployment of a single attacker. Consequently, the platform of this attack is considered to be a single aerial frame, capable of tracking mobile targets and controlling its altitude. The jamming interface is equipped with a beam-scanning antenna, allowing the jammer to adjust its point of attack and dynamically shift the jamming region over the target area. Figure 2.1 illustrates the attack scenario, in which the jammer is only targeting a sub-region of the network. As a practical perspective, it is assumed that the beam-width of the jamming antenna is fixed. The area of jamming region (depicted by the circle of diameter $2r_{jammer}$) may be varied by changing the attack altitude h, but due to propagation loss and operational limits of the airframe, the changes of altitude may be limited. In cases

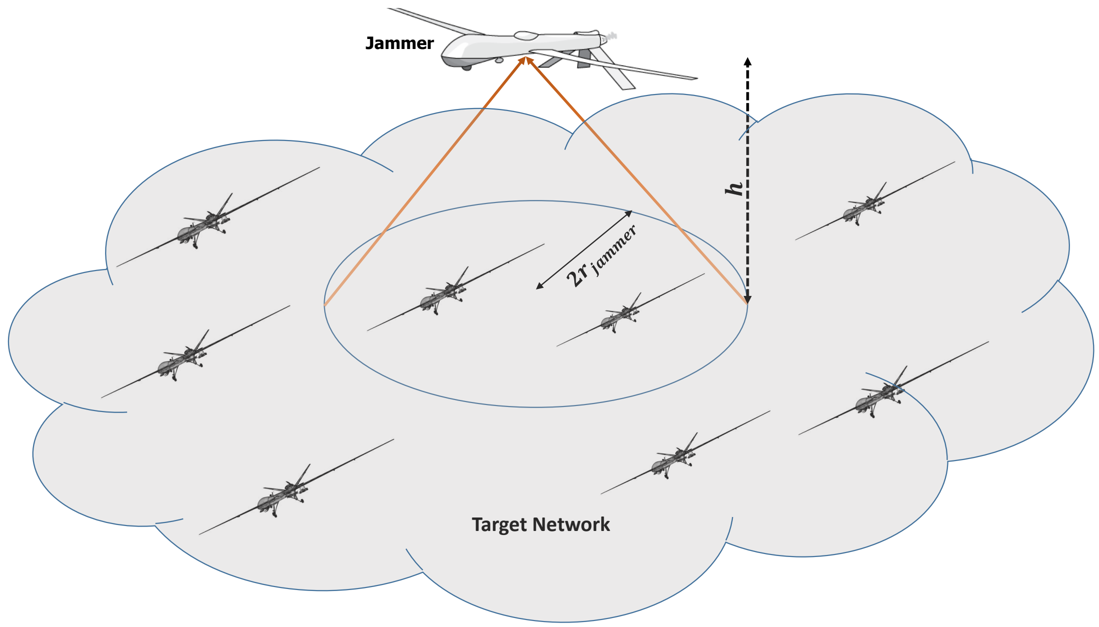


Figure 2.1: Attack Model

where the target is distributed over an area larger than the coverage bounds of the beam, the effect of jamming is limited to a subset of nodes.

The jammer is considered to have no a priori information about the target, meaning that it is not aware of its communication protocols, content of transmissions, physical layer links, flows and routes. The only features of target's communications that can be observed by the attacker are timing and location of individual transmissions, duration of each transmission and their frequency channels. It is also asumed that the jammer has real-time knowledge of the values of the observable parameters for the entire network. In practice, this may be achieved by addition of a sensing interface equipped with 2-D scanning antenna arrays and accurate Direction of Arrival (DoA) estimators such as MUSIC [29].

The attack problem hence becomes two-fold: First, the attacker must estimate the target's topology by inferring the existence of hop-to-hop (i.e. direct physical) links from the observed information. This type of passive inference is referred to as

Traffic Analysis. Then, as the jamming region is limited, it must identify the most vulnerable region of the target to attack. Vulnerability of a region depends on the type of disruption that the attacker desires to inflict on the target. Disruption can be incursion of maximum drop in the total connectivity of the target, or slowing the flows with larger data content (e.g. ISR information), or other case-specific definitions. It is also assumed that the attacker may have to perform its operation for a prolonged duration, therefore energy efficiency of the attack is one of the requirements. The following chapters provide details of our proposed solutions to both problems.

Chapter 3

Traffic Analysis

3.1 Formulation

Multihop ad hoc networks are based on the concept of peer transmission, in which one or more neighbors of a source node relay the original transmission to their neighbors until it reaches the intended destination. In such cases, it can be hypothesized that if a node A repeatedly transmits a short time after the transmission of a close-by node B, it is likely that A is relaying the transmission of B and hence a link exists between the two. This hypothesis initially proposes that the future state of the network does not follow a memoryless process such as stationary Markov process, in the sense that it may be dependent of the previous states, meaning that if $S_t = \{s_{1,t}, s_{2,t}, \ldots, s_{N,t}\}$ denotes the transmission state of the network at time t, where $s_{(}i, t) \in \{0, 1\}$ indicates whether node i is transmitting or not, then $S_t + 1 = f(S_t, S_{t-1)}, \ldots, S_0)$. This corollary conforms with the definition of multihop communications, which states that a signal transmission by a source node causes retransmissions by relays until the signal reaches its destination. Furthermore, the hypothesis claims that there is a correlation between the time when a source transmits a signal, and the transmission time of the corresponding relay node. The strength of such correlations in multihop networks have been extensively studied in the context of investigating queuing delays [35] [8], providing both analytical and experimental models for different MAC schemes (i.e. CSMA/CS, TDMA, ALOHA), topologies, and traffic conditions. The results emerging from such studies demonstrate the existence of correlations between the source transmission/arrival time of a signal to a relay node and the departure time from that node, with MAC and other studied parameters only affecting the degree of correlation.

Several aspects of this hypothesis need further emphasis: Firstly, the transmissions of A is not necessarily always relays of B; node A may also transmit its own data, or relay some other node's transmission. Hence, the word "repeatedly" is used as opposed to "consistently". Second, this hypothesis does not define a hard limit for the time delay between two transmissions to estimate the likelihood of a source-relay relationship. This parameter is not only dependent on the network, but may be time-variant, meaning that the relay transmissions do not necessarily occur at fixed times $t_0 + \Delta t$ as δt may vary for different observations. And lastly, the hypothesis only considers the timings of transmissions and not their length, duration or content. In cases such as networks that implement pairwise private key encryption, the length of a relay transmission may be different from the original transmission and hence cannot be a reliable measure of similarity between the two transmissions. Therefore, a link estimation technique developed upon this hypothesis must satisfy its assumptions and consequences by considering the following specifications:

i) The estimation must only consider the timing of transmissions and not their content-related parameters such as length, duration, modulation and bit sequence.

ii) The likelihood of a relay relationship between a pair of nodes (i, j) must be a decaying function of $r_{ij} = distance(i, j)$, i.e. the farther the two nodes are, the likelihood of them being in a source-relay relationship is lessened. This is consistent with the multihop model, in which the propagation loss forces a node to utilize a nearby node as intermediary to reach its distant destination.

iii) The estimator must be inversely related to Δt_{ij}, the time difference between transmissions of i and j. In other words, if the delay between two transmissions is longer, it should be less likely that the two form a source-relay pair.

iv) If during the observation period of duration T_{obs}, transmissions of node i repeatedly follows the transmissions of node j, the likelihood of (i, j) being a source-relay relationship must increase.

3.2 Synchrony Score for Timing Analysis

This problem can be translated into measuring the synchrony between transmissions of two nodes i and j. A broad definition of synchrony is *the mutual entrainment of rhythms of oscillators by their weak interactions* [25]. Quantitatively, synchrony measures the degree of interaction between two or more agents, in terms of their influence on each other's actions and causality. In neuroscience and behavioral psychology, the similar definitions of synchrony are used as measures of the relationship between entities, such as determination of neural regions of the brain that are activated as a result of the same external stimulant [18], or estimation of the level of imitation that occurs between an adult performing a task and a child observing that task [12]. Various metrics of synchrony have been utilized in relevant literature of neuroscience and psychology, a thorough survey of each is presented in [17]. In the present work, we considered two of such metrics due to their relevance and applicability to the problem at hand. The chosen metrics are Pearson's product-moment correlati on coefficients, and cross-spectral coherence. Pearson's correlation coefficients, or simply correlation coefficients, defined by equation (3.1) measure the linear correlation between two dataset, resulting in a value in the range [1,-1], where 1 denotes total positive correlation, 0 is no correlation and -1 is total negative correlation. In the case of samples taken over time, correlation coefficients are considered a time-domain metric of correlation between two samples.

$$\begin{aligned} R_{xy} &= \frac{cov(x,y)}{\sigma_x \sigma_y} \qquad (3.1) \\ cov(x,y) &: \text{Covariance of x and y} \\ \sigma_x &: \text{Standard deviation of } x \end{aligned}$$

Coherence (3.2), on the other hand, is a spectral metric of relationship between two signals. This metric not only characterizes the relationship of two signals, but under certain conditions can estimate the causality between them as well. The conditions for this estimation to be accurate are two-fold: the measured signals must be ergodic, and the system function must be linear. Previous work on traffic analysis of wireless networks by Partridge et al. [23] have shown the validity of these conditions for multihop wireless transmissions for approximate results. One may pose the idea that since correlation coefficients and coherence both provide a measure of similarity, while coherence is additionally capable of estimating causality, then coherence alone could be chosen as the more applicable metric. But a study on accuracy of correlation and coherence on sampled timing signals [15] shows that the accuracy of these two metrics varies differently under different noise conditions, differences in amplitude, time difference and changes in phase. Hence, in this work, we consider both coherence and correlation with the aim of reducing the estimation error of one metric via the better accuracy of the other.

$$\begin{aligned} C_{xy}(f) &= \frac{\mid G_{xy}(f) \mid^2}{G_{xx}(f)G_{yy}(f)} \qquad (3.2) \\ G_{xy}(f) &: \text{Cross spectral density of } x \text{ and } y \\ G_{xx}(f) &: \text{Autospectral density of } x \end{aligned}$$

As noted in Chapter 2, only the timing of individual transmissions are to be considered, since duration, power and other parameters are not consistent measures of synchrony. Therefore, at any given time, a node is considered to be either transmitting or idle, i.e. transmission states can be represented as a boolean value of 1 or 0. Consequently, the observed transmission timings of each node can be represented with a binary sequence $\{b_1, b_2, \ldots, b_i\}$ where $b_n \in \{0, 1\}$ is the state of the node in the nth observation. This representation requires encoding of the observed data in the following fashion: Let $D = \{D_1, D_2, \ldots, D_N\}$ be the set of observation datasets, where $D_i = \{d_i(t), d_i(\delta t), \ldots, d_i((n-1)\delta t)\}$ is the observed dataset of node i. $d_i((n-1)\delta t)$ is the observed transmission information of node i which has been uniformly sampled at intervals of δ seconds. The encoded dataset of D_i is ãĂŰ$D'_i = \{d'_i(t), d'_i(\delta t), \ldots, d'_i((k-1)\delta t)\}$ where $d'_i((n-1)\delta t) \in \{0, 1\}$ is the transmission state of node i, with 1 denoting transmission and 0 is idle. Accordingly, we propose the following Synchrony Score metric as a measure of the synchrony between two nodes i and j $(i \neq j)$. The synchrony score is an undirected metric (i.e. $S_{ij} = S_{ji}$) and is defined as:

$$S_{ij} = \frac{\frac{C_{ij} + |R_{ij}|}{2}}{r_{ij}^2} \qquad (3.3)$$

Where C_{ij} is the coherence function and $\mid R_{ij} \mid$ is applied in the form magnitude of correlation coefficient to remove the directionality. As is the case in wireless propagation loss, S_{ij} is also inversely proportional to the square of the distance between the two nodes r_{ij}^2 to take into account the fact that far away nodes are less likely to be directly connected to each other. The output of this process is a conversation matrix S, whose entries are S_{ij} for every $i \neq j$, and 0 otherwise.

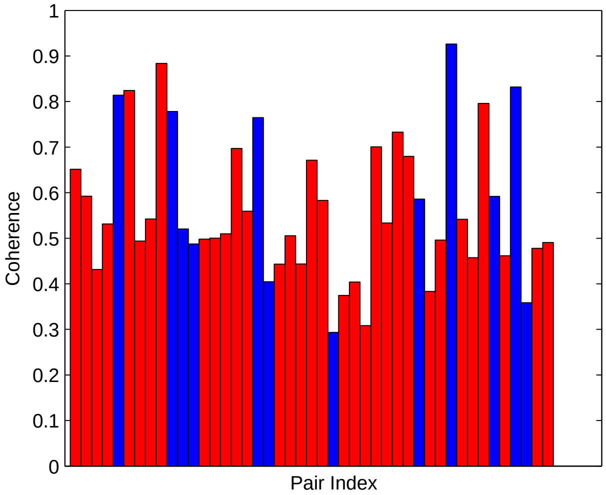


Figure 3.1: Coherence between each pair of nodes

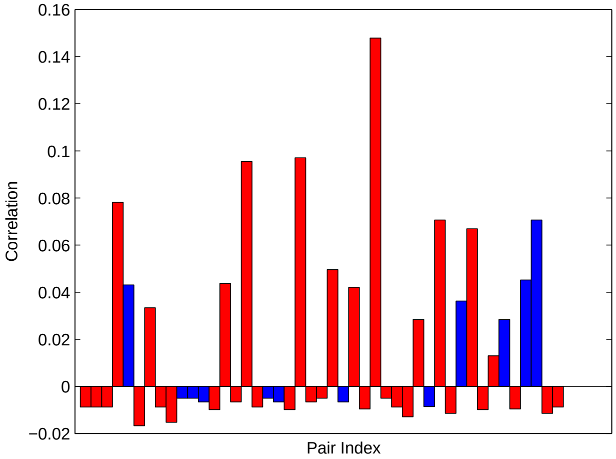


Figure 3.2: Correlation Coefficient of each pair of nodes

To demonstrate the accuracy of the proposed synchrony score, results of a test case is selected from the simulation analysis of this method presented in Chapter 5. Figures(3.1 - 3.4) compare the performance of the considered metrics (coherence, correlation, average of these two and the proposed synchrony score) for arbitrarily

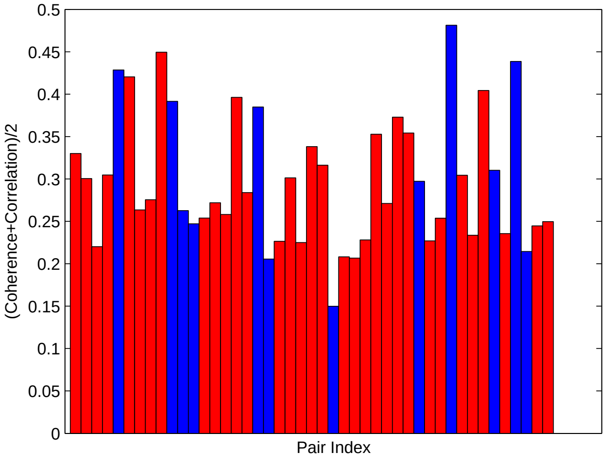


Figure 3.3: Average of Coherence and Correlation values

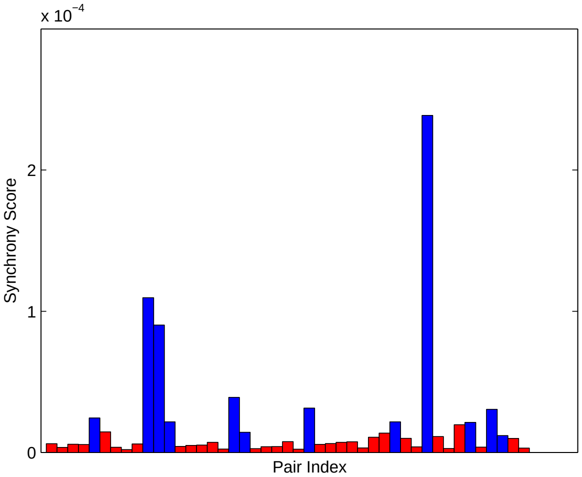


Figure 3.4: Synchrony score

indexed pairs of nodes in a test case of 10 ad hoc nodes geometrically distributed according to the Poisson-Boolean model (equation (1)), where blue bars represent linked pairs and red bars are disconnected pairs. Observing the performance of coherence in Figure 3.1, it can be seen that the difference between values of unlinked and linked pairs of this test case is not distinctly distinguishable, and hence the estimation of linked pairs from coherence may not follow a straight-forward and general approach. In Figure 3.2, the value of correlation for most disconnected pairs is higher than that of the linked ones, and the values of both are not widely spread, therefore in this case also the metric fails to provide a quick and simple measure for estimation of linked pairs. The effect of expected mutual error cancellation of coherence and correlation when averaged is depicted in Figure 3.3, where although the variation of values for both groups seems to be less than the preceding case, the difference between categories is not yet sufficiently distinct for a fast classification of the pairs. Figure 3.4 on the other hand, demonstrates a distinguishable difference between the synchrony scores of linked and unlinked pairs when the inversed euclidean distance of nodes is factored in the statistical properties of observations.

3.3 Thresholding

Another noteworthy observation in Figure 3.4 is that the majority of the linked pairs have distinctly higher synchrony score values compared to the disconnected pairs, hinting at the possibility that a simple and computationally efficient statistical metric may be applied as a threshold for accurate classification of the scored pairs. In the context of this investigation, threshold is generically defined as:

$$T(G\{V,E\})\ s.t. \begin{cases} S_{ij} \geq T(G\{V,E\})\ if\ P(x) \geq P_0 \\ S_{ij} < T(G\{V,E\})\ if\ P(x) < P_0 \end{cases} \tag{3.4}$$

Where the threshold $T(G\{V,E\})$ is a function of the network topology $G\{V,E\}$ such that the probability of an event x is more than a set value p if the synchrony score S_{ij} of the pair is greater than the threshold. A relevant example of the event x is $x = \{i,j\} \in E$, i.e. the pair of nodes i and j being linked. Selection of the value p is dependant on the application of the threshold. For a general investigation into statistical properties of synchrony score, we let $p = 0.5$ to measure how the chosen thresholds distinguish our proposed method from classification by pure chance. Aiming for a computationally fast method for determining the threshold, we investigated the Mean, Standard Deviation and Median of the synchrony scores as potential candidates for a global threshold. Also, the applicability of a local adaptive thresholding technique similar to Niblack's image intensitiny thresholding method [21] is studied. In this technique, the *local threshold* value $T(x, y)$ of each synchrony score S_{ij} is determined according to:

$$T(i, j) = m_{w \times w}(i, j) \tag{3.5}$$

Where $m_{w \times w}(i, j)$ is the local mean of all synchrony scores in a window of size $w \times w$ scores centered on $S_{i,j}$. The performance of each metric is compared and presented in Chapter 5.

Chapter 4

Identification of Most Vulnerable Point (MVP)

With an estimation of target's topology at hand, the jammer may increase the impact of its attack by identifying the Most Vulnerable Point (MVP) of the network to jamming. The vulnerability of this region is determined by the level of impact that its disruption will incur on the network as a whole. The problem of MVP identification has analogs in fields such as neuroscience, criminology and epidemiology, where measuring the vulnerability of individual nodes in a network has been studied through graph theoretical modeling. Neuroscientific studies focus on finding the effect of diseases disrupting certain regions of the brain on the overall functionality of the nervous system [27], while network-based studies in epidemiology consider the problem of identifying nodes whose removal from the network (i.e. population) would maximally slow the propagation of epidemics [13]. In the context of criminology, modeling a group of criminals as a network allows law enforcement entities to identify those nodes whose arrest would cause maximum disruption to the criminal activities of the group [22]. Resemblance of such problems to the one presented in this chapter motivates the adoption of a similar approach for MVP identification.

This chapter studies the problem of topological vulnerabilities and proposes a computationally fast method of identifying the Most Vulnerable Point (MVP) to jamming attacks through graph theoretical modeling and analysis of target networks.

4.1 Formulation

The problem of identifying the set of nodes in a multihop network whose removal leads to maximum disruption is analogous to the graph theoretical Critical Node Problem (CNP). Let $G = (V, E)$ be an undirected and unweighted graph consisted of the set of vertices V and set of edges E. Nodes $i, j \in V$ are pairwise connected if there exists a path between i and j. The Critical Node Problem aims to select a subset $Q \subseteq V, \|Q| \leq k$ to be removed in order to minimize connectivity in the residual subgraph $G(V \setminus Q)$. Vertices of Q are hence known as *critical nodes.* The formal definition of CNP is given by:

Definition 4.1.1. Critical Node Problem (CNP):
INPUT: Undirected graph $G = (V, E)$, int k
OUTPUT: $A = argmin \sum_{i,j \in (V \setminus Q)} u_{ij}(G(V \setminus Q)) : |Q| \leq k$
Where:

$$u_{ij} = \begin{cases} 1, & \text{if } ij \in edgeset \text{ of } G(V \setminus Q) \\ 0, & \text{otherwise} \end{cases}$$

It is well-known that the decision problem for existence of such a set of size k is

NP-complete [1]. Also, [2] provides the following proof for NP-hardness of CNP:

Theorem 1. Finding the set of nodes of maximum size k whose removal minimizes pairwise connectivity in graph $G(V, E)$ is NP-hard.

Proof. By removing each set of k vertices from G, the number of connected pairs can be calculated using DFS or BFS in polynomial time, therefore the problem is in NP. NP-hardness of CNP can by reduction from the Vertex Cover problem: Given a graph $G = (V, E)$ where $|V| = n$, is there a vertex cover of size at most k? Through forward reasoning, it emerges that if there is a vertex cover of size k, then the deletion of those k nodes leads to total disconnection of the network. Vice versa, if the removal of k nodes disconnects all pairwise connections, then there is no edges left, and thus there exists a vertex cover of size k.

□

The MVP problem investigated in this chapter is in essence the same as CNP, with an extra constraint. As depicted in Figure 2.1, the effective impact area of the jammer is limited to a circular region A_{jam} of radius r_{jam}, which is the base of a cone whose lateral height h is the relative altitude of the attacker with respect to the target. The maximum value of h is bounded by practical conditions, one of which is the maximum operational altitude of the jamming platform, beyond which it cannot fly. Also, the further the attacker is from the target network, the more power it must transmit to affect the target, which is not desirable in terms of energy efficiency.

Therefore, depending on the spatial distribution of target nodes, the attacker may only be capable of jamming a limited group of nodes that fall within the jamming region A. Considering this constraint, the attacker must be equipped with a fast mechanism to identify the group of nodes that are within a bounded area of size

A whose jamming causes maximum disruption in the entire network. Definition of disruption in this context is dependent on the aim of the mission and a real-time cost-benefit analysis. Ideally, the objective of the attack is to cause maximum connectivity drop in the network so that none of or fewer nodes can communicate with each other. But if this cannot be feasibly achieved (e.g. when attacking none of the jamming regions in the network can inflict sufficient drop in connectivity), the aim of attack can be changed to minimizing the throughput of flows in the network by maximizing congestion. Hence, the mechanism responsible for identifying the point of attack shall take all of these definitions into account.

The conversation matrix S calculated in the traffic analysis phase is an estimate of the target network's topology. This topology can be mapped to a weighted, undirected and connected graph $G := (V, E)$, where V is the set of vertices representing N nodes and E is the set of edges corresponding to links in the network. Weight of each edge is the same as its corresponding link's conversation likelihood value. Therefore, the adjacency matrix of G is the same as the conversation matrix S. Alternatively, it can be mapped to a graph $G_{thresh} : (V, E)$, where G_{thresh} is an unweighted undirectional graph generated by an adjacency matrix obtained by thresholding the conversation matrix.

Based on this mapping, identification of MVP can be translated into the graph theoretical problem of determining the most vulnerable region in the graph G. Equation (4.1) represents this problem as an optimization problem.

$$\max(f(L)), L \subset V, A(L) = 1 \tag{4.1}$$

Where L is a subset of vertices V, and $A(L)$, defined by equation 4.2 is a function that determines whether all of the members of L can fit in a circle of radius r_{jam}.

$$A(L) = \begin{cases} 1, & \forall i, j \in L : \text{distance}(i, j) < 2 \times r \\ 0, & \text{otherwise} \end{cases} \tag{4.2}$$

The function $f(L)$ is the measure of disruption inflicted on the graph $G(V, E)$ by removing L from G. Depending on the aim of attack and definition of disruption, $f(L)$ can take various definitions, including the following:

i) Connectivity Drop: In this work, connectivity of a graph is defined as the total number of pairs of vertices in that graph which can reach each other through a path consisting of edges in the graph. In a completely connected undirected graph of N vertices, the connectivity is $N*(N-1)/2$. Consequently, Connectivity Drop $f_{conn}(L)$ is defined as the difference of connectivity values between the original graph and the graph whose subset L of nodes is removed. A more computationally expensive Note that this definition is different from the formal graph connectivity, defined as the size of a minimal vertex or edge cut.

ii) Global Efficiency: The efficiency of a network is a measure of how efficiently it exchanges information. Equations (4.3) and (4.4) define global efficiency as the average efficiency $E(G)$ normalized by the efficiency of the ideal graph (a completely connected graph with the same number of nodes). It is proposed by Latora and Marchiori [19] as a method of quantifying small world behavior [26] in networks, but can also be used as a replacement for Average Path Length, defined as the average of lengths of all shortest paths in the network, which itself is a measure of efficiency in information exchange. Both of these metrics are measures of path lengths in networks, but average path length measures the efficiency in a network which has only one packet flowing at any given time, while

Algorithm 1: Generation of Search Space

```
input : Set of nodes and their positions $N$, minimum number of nodes obtained
        from percolation threshold $Nmin$
output: $SearchSpace$
$SearchSpace = \{\}$
for $n \in N$ do
    $C \leftarrow \{n\}$
    $S \leftarrow$ list of all nodes whose distance to n is less than $2 \times r_{jam}$
    for $i \in S$ do
        if $distance\ of\ i\ and\ every\ element\ in\ C <= 2 \times r_{jam}$ then add $i$ to $C$;
    end
    if $size(C) >= Nmin\ and\ C \notin SearchSpace$ then add $C$ to $SearchSpace$;
end
```

Global Efficiency considers networks where all the nodes are exchanging packets in parallel. Therefore, the latter was chosen since it was more relevant to the problem.

$$E_{glob}(g) = \frac{E(G)}{E(G^{ideal})} \tag{4.3}$$

$$E(G) = \frac{2}{n(n-1)} \sum_{i<j \in G}^{n} \frac{1}{d(i,j)} \tag{4.4}$$

4.2 Efficient Generation of Search Space

With the optimization problem defined, the identification mechanism must then perform a fast search over the entire network to identify all potential targets in the network and compare the effects of their disruption. As time and cost efficiency are of priority in this attack framework, generation of all such sets must be performed in a fast, yet computationally tolerable manner. One possible approach is the brute-force approach of Algorithm 1. The basis of this algorithm is visiting every node and calculating its distance with every other node, and is solved in $O(n^2)$ time. An alternative is to model this problem as a fixed-radius near neighbors set problem in

2D space [4]: Given a set of points P on a plane and a fixed distance $r > 0$, find all pairs of points $p, q \in P$ such that the distance between them is less than or equal to r. The problem encompasses the requirement of our search algorithm for generating all clusters of nodes that fit inside the jamming area, and a grid-based solution to which is presented that runs in time $O(k) + n.T(n)$, where $T(n)$ is a grid search operation [4]. The algorithm finds all unique pairs of nodes which can be covered by a circle of radius r_jam, from which a minor linear search can be performed to generate unique clusters. With the enhancement provided by this algorithm, the performance of solving the optimization can be further improved via limiting the search space by considering certain criteria on clusters and nodes.

4.3 Reduction of Search Space by Percolation Modeling

The size of search space can be reduced if the attacker is able to determine the minimum number of nodes that it must attack to maximize the total disruption. This can be achieved by applying the Continuum Percolation theory [14], which states that if the node density of a network, denoted by λ, is larger than a critical density λ^*, the network has a high probability of being completely connected. On the other hand, if $\lambda < \lambda^*$, the network has a higher probability of being disconnected. To find a lower bound on the number of nodes that must be jammed, the attacker can determine the value of λ^* for the target network. Although there is yet no analytical method of calculating λ^*, numerical approximations have been proposed for special cases [20]. One such case is the Triangular Lattice [31], which can be used to model a 2D grid. The 2D topology of the target nodes can be converted to a triangular lattice of edge length $r/2$, where r is the communications range of each node [16]. Sites are then defined as the flowers centered at a vertex of the lattice. Each flower

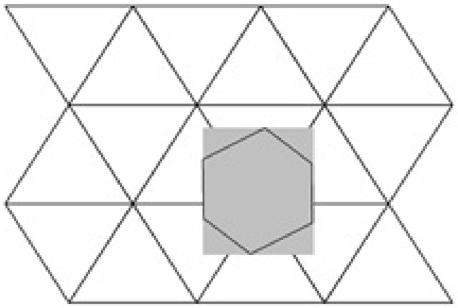


Figure 4.1: Mapping of a 2D grid to a triangular lattice

is bounded by six circular arcs, each of which is centered at a midpoint of one of the six edges adjacent to the vertex and have a radius of $r/2$. A site is occupied if there exists a node from the target network $G(\lambda, r)$ in the associated flower. If two adjacent flowers are occupied, then the distance between the two is no more than r. Figure 4.1 illustrates a triangular lattice with the flower denoted by the shaded area. Percolation in triangular lattices occurs when site occupancy probability is not less than a critical value p_c, which for the case of 2D lattices is equal to 0.5 [31]. The flower occupancy probability is calculated as:

$$p_f = 1 - e^{-\lambda A_f} \tag{4.5}$$

Where A_f is the area of the flower and is approximately $0.206r$. Therefore, λ^* can be calculated from:

$$0.5 = 1 - e^{-\lambda \times 0.206r} \tag{4.6}$$

Thus, the minimum number of nodes in MVP cluster is determined by:

$$N_{min} = (\lambda - \lambda^*) \times 0.206r \tag{4.7}$$

4.4 Fast Metrics of Disruption

The final stage of identification is to compare the effect of disrupting each cluster and determine the one which leads to maximum disruption. One approach to this problem is to calculate the disruption metric (such as connectivity drop) for every cluster by removing its nodes and associated links from the adjacency matrix. But this process is computationally slow and is not suitable for a real-time attack. Therefore other metrics must be sought which can act as measures of vulnerability of a cluster while lowering the computation time. Graph theory provides a class of metrics that measure the "importance" of nodes in a graph, namely the centrality metrics. If the attacker considers each cluster as a single node in the graph, such metrics can be applied to measure the influence of the cluster on the network. The definitions of centrality metrics considered in this work are given in the following.

i) *Modified Eigenvector Centrality*: This metric measures the influence of a node in the network. It assigns a relative score to the node based on the concept that connections to high-scoring nodes contribute more to the score of the node compared to connections to low-scoring nodes. The scoring scheme is described by $x_v = \frac{1}{\lambda} \sum_{t \in M(v)} x_t$, where x_v is the score and $M(v)$ is the set of all neighbors of v. First, eigenvalues and eigenvectors of the adjacency matrix are calculated. Then, one of the eigenvalues is selected based on the condition that its associated eigenvector is comprised of positive values only. If the conditions for Perron-Frobenius theorem [33] are satisfied, it can be shown that the chosen eigenvalue is the largest eigenvalue of the adjacency matrix. The score is finally calculated as the sum of corresponding values in the eigenvector for all neighbors of the node. The score can be normalized by dividing this value over the first eigenvalue.

This metric is especially popular in search engines and have been widely used for similar applications [30]. But applying it to our problem gives rise to a number of issues. Firstly, the validity of Perron's theorem is only held for matrices that are composed of all positive values. Since the adjacency matrix includes zeros as entries, this condition does not hold. Furthermore, the generalization of Perron's for non-negative matrices by Frobenius is only valid for a irreducible matrices [5], whereas, to the extent of our knowledge it has not been proven that adjacency matrices of connected Poisson-Boolean graphs necessarily comply with this condition. Therefore it is possible that an eigenvector of all positive values does not exist for an adjacency matrix. However, in all of our simulations it was observed that the largest eigenvalue corresponds to either a vector with all positive values or one with all negative values. Further simulations confirmed the hypothesis that in case of vectors with all negative values, their absolute values act effectively as well as those with all positive values. Thus, in calculations of eigenvector centrality we consider the largest eigenvalue associated with either a vector of all positive or all negative values as the basis of the scoring mechanism. A similar approached is analytically developed and presented in [32].

ii) *Betweenness Centrality*: This metric is the number of shortest paths in the network that pass through a node.

iii) *Degree Centrality*: This metric corresponds to the number of links (edges) incident on a node.

iv) *Number of nodes in the cluster*: This metric is the fastest one in our selection, with the assumption that attacking the cluster with the largest number of nodes results in highest level of disruption. This assumption is further inspected in Chapter 5. The issue with this metric is that it is not necessarily unique, as more than one cluster may have the same number of nodes. Therefore, this computationally inexpensive metric can be used to further reduce the search space for more time consuming metrics.

v) *Clustering Coefficient*: Local clustering coefficient of a node quantifies how close its neighbors are to being a clique (complete graph) [14]. Clustering coefficient is defined as the ratio of links between the vertices within its neighborhood over the maximum number of links that could possibly exist between them. Neighborhood is the set of all nodes that are directly connected to the node in question. In the context of the MVP problem, higher values of clustering coefficient for clusters indicate that their disruption is less effective on the entire network, as their highly connected neighbors are capable of replacing the disconnected nodes.

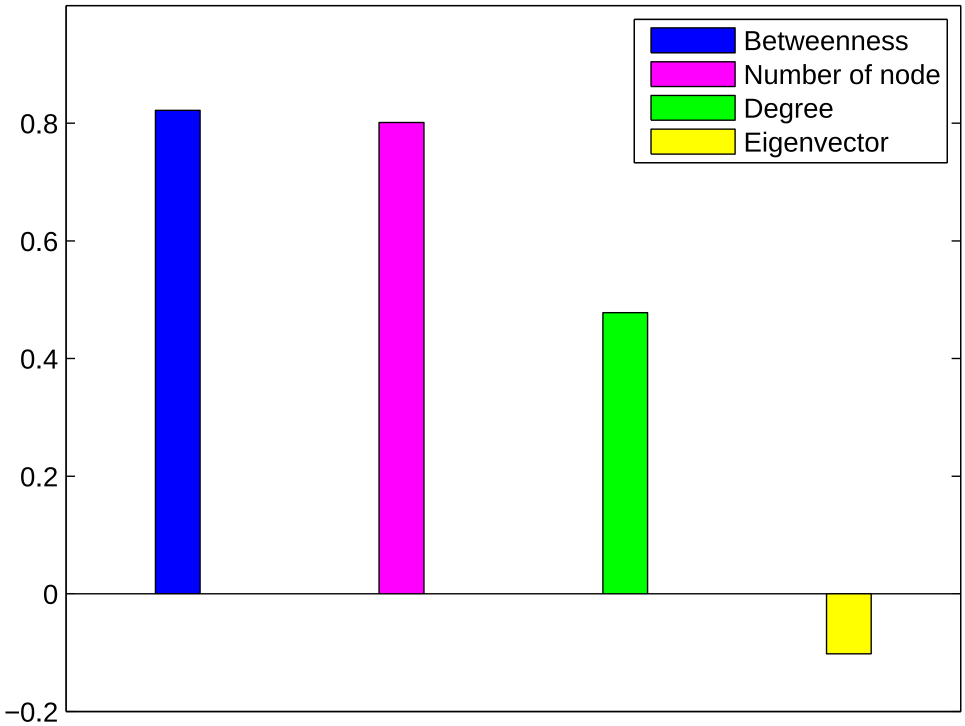


Figure 4.2: Spearson Correlation of metrics and Connectivity Drop

To investigate the relationship between these metrics and the optimization metrics (i.e. Connectivity Drop and Global Efficiency), a jamming attack was simulated. In every iteration of the simulated attack, unique clusters of nodes coverable by the fixed circular area of jamming were selected by turn, and their edges were disconnected from the rest of network to observe the impact of their removal on the connectivity and global efficiency of the network. Fast metrics of disruption such as betweenness centrality were then recorded alongside the values of the optimization metrics.

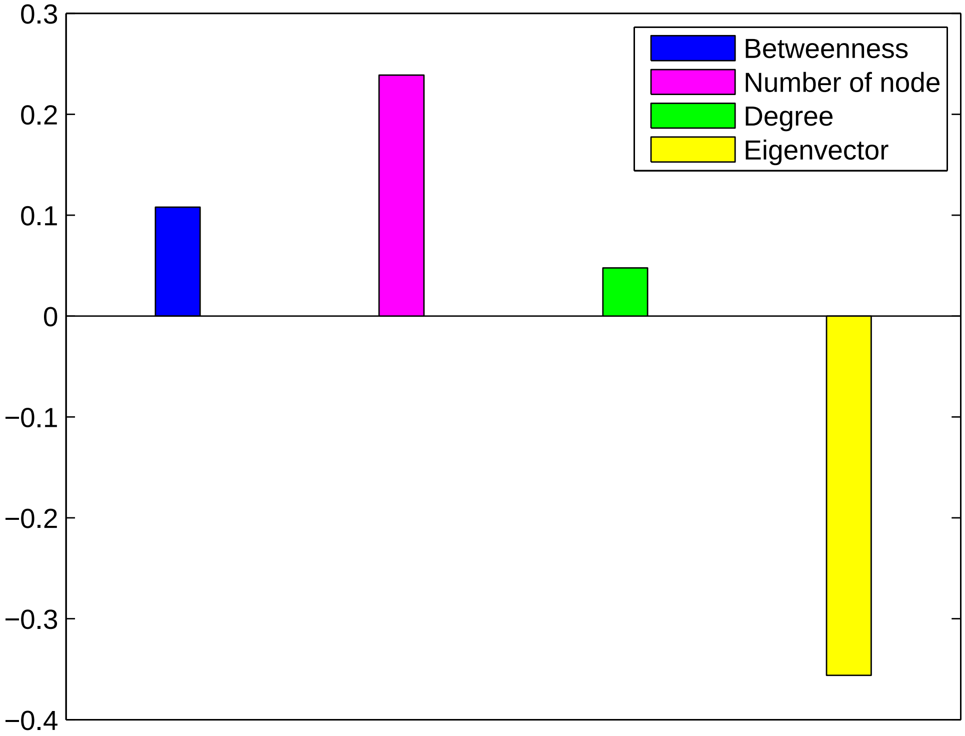


Figure 4.3: Spearson Correlation of metrics and Global Efficiency

In the first step of analysis, the Spearman correlation coefficients between connectivity drop and each pair of the fast metrics and the optimization measures were calculated, the results of which are presented in Figure 4.2. It is evident that the correlation coefficients of the attacked clusters' betweenness centrality and their number of nodes have a relatively strong correlation with connectivity drop. While all of the fast metrics fail to show a strong relationship with global efficiency. Figure 4.3 illustrates the corresponding Spearman correlation values for global efficiency, which do not represent a strong correlation between the fast and optimization parameters.

Further simulations were performed on Poisson-Boolean connected graphs, leading to the observation that the number of nodes in the targeted cluster has a seemingly direct and strong relationship with drop in connectivity. As it is demonstrated in Chapter 5, maximum number of nodes in a cluster has almost always occurred in the cluster whose removal leads to maximum drop in connectivity of the graph. This is in accord with the intuition that disconnecting more number of nodes results in higher disruption in the remaining network. But as the jamming area is fixed, the maximum number of nodes that can be covered by the jammer tends to saturate after a threshold, which builds the possibility that multiple clusters may have the same maximum number of nodes. Hence, this metric cannot be used as a sole identifier of the most vulnerable cluster. The observed statistics of correlations and co-occurrences of maximal values suggests the adoption of an alternative approach to fast selection of MVP, which is to first reduce the size of search space by selecting the clusters with largest number of nodes, and then measure their betweenness centrality as the second most related fast parameter. Thus, this proposal relieves the cost of optimization by providing a relatively cheap metric for selection of the most vulnerable region, and twice reducing the size of search space. The efficiency and performance of this approach is further confirmed by simulation results presented in the next chapter.

Chapter 5

Simulation And Results

For evaluation of the proposed framework, graph theoretical and network simulations were performed to measure the validity and accuracy of the developed methods. Simulation of graph properties were based on modified Random Geometric graphs to model Poisson-Boolean distribution and density. In this approach, the uniform allocation of positions by the Random Geometric graph generators was adjusted in compliance with a Poisson point process. The establishment of links between nodes followed a deterministic function of euclidean distance for an accurate representation of ad hoc wireless networks. To ensure the connectedness of the generated graphs, percolation threshold of a triangular lattice over the simulation grid was given as a parameter to the graph generator. The essential aim of graph theoretical simulations were to investigate the effect of intentional removal of nodes on the structure and features of the abstract graph model.

For more realistic measurements, network simulations were implemented in NS-3. For every simulation, wireless ad hoc networks were setup by configuring fixed

Table 5.1: Simulation Parameters

Parameter	Value
Number of Node	25
MAC Protocol	802.11b
Routing Protocol	OLSR
Tx Power	16.0206 dBm
Rx Threshold	−96.0 dBm
Propagation Loss Model	Free Space (Friis)
Communications Range	1403.346 m
Run Time	450 s

nodes as 802.11b radios operating in ad hoc mode. Also, to enhance the accuracy of measurement, allocation of positions to nodes were based on scaled coordinates of Poisson-Boolean connected graphs generated in the graph simulator. The propagation loss model considered in these simulations was the Friis free space model, and the remaining of the protocol stack parameters were kept to their default values. Table 5.1 presents a list of such relevant parameters.

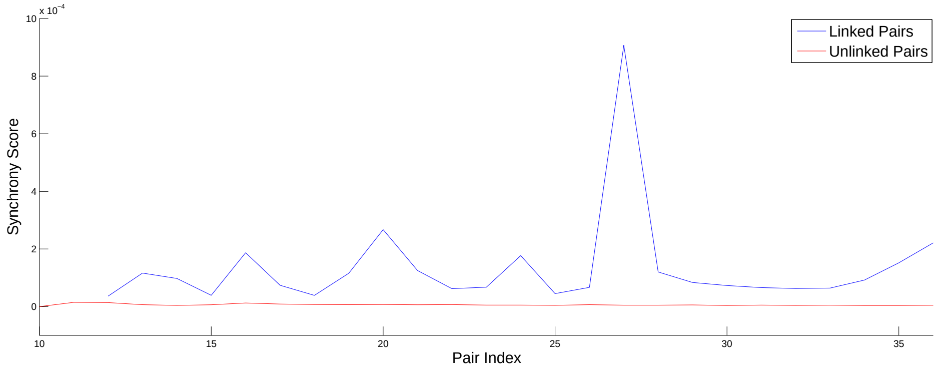


Figure 5.1: Average of Synchrony Score for different number of nodes with 2 parallel flows

5.1 Performance of Synchrony Score

The initial aim of network simulations were to generate and capture near-realistic data as the input of the traffic analysis technique. The collection of data was perfomed by a passive sniffer, capable of receiving transmissions of every node in the network. The captured data were transmission trigger times and the originating node, and no network or other physical layer parameter was recorded. The traffic analysis system was then tasked with preprocessing the data by sorting the transmission traces of each node, and removing multiple instances of a broadcast transmission occurring at the same instant. This phenomenon is an internal configuration of NS-3, therefore trimming such events does not affect the quality of data in the context of our experiments. Once preprocessed, a 20-second block of the sample is passed to the Synchrony module, which in turn generates the corresponding conversation matrix per steps detailed in Chapter 3. Validity of the generated pairwise estimations was inspected by comparison with the original adjacency matrix and routing table of the target network for different parameters.

Figure 5.1 illustrates the difference between averages of synchrony scores of linked and unlinked pairs for different number of nodes. It is evident that regardless of number of nodes, linked pairs have a distinguishably higher average of synchrony score than that of the unlinked pairs. Also, the variation of average for unlinked pairs is distinctively less in comparison with linked pairs. This feature can be exploited for efficient and accurate classification of linked and unlinked pairs based on the link estimation values. It is noteworthy that the number of flows in this simulation is fixed and equal to 2 simultaneous multi-hop flows of different sizes.

The distinction of synchrony score for different number of flows is depicted in

Figure 5.2. The results indicate that increasing the number of simultaneous flows does not significantly affect the differentiation of linked and unlinked pairs, thus the proposed method can be used for accurate classification of pairs.

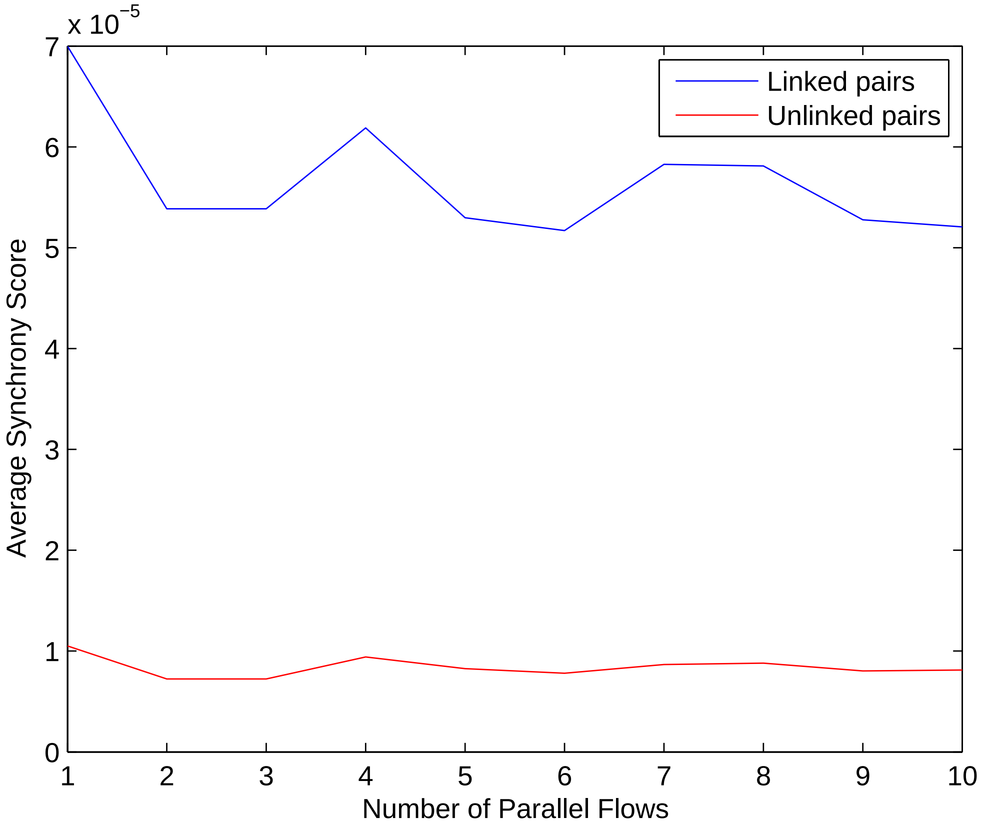


Figure 5.2: Average of Synchrony Score for different number of flows in 25 nodes

As this attack is designed for real-time applications, the limits on duration of observation required for accurate estimation need to be established. Figure 5.3 demonstrates the effect of sampling duration on the average of synchrony scores for a network of 10 nodes. The plot shows a gradual decline in the score of linked pairs, which can be explained by the fact that in prolonged observations, false correlations might be made between events occurring at distant points of time. It is also observed that when the timescale of observation is in seconds, this gradual decline does not significantly

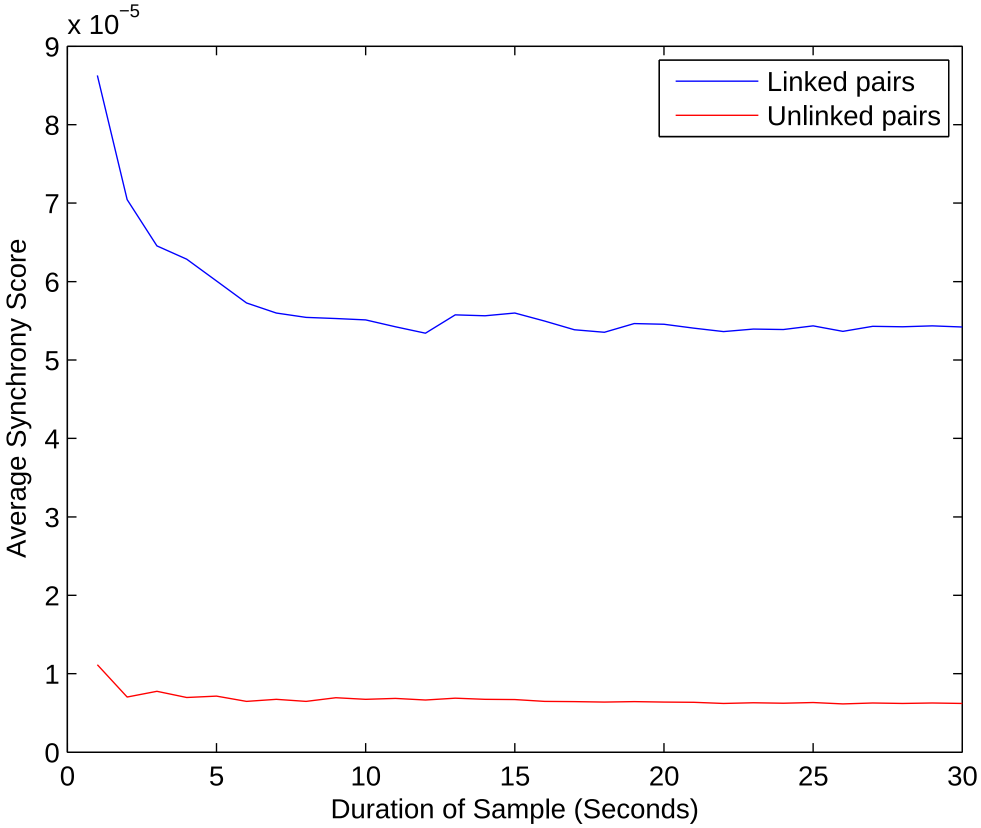
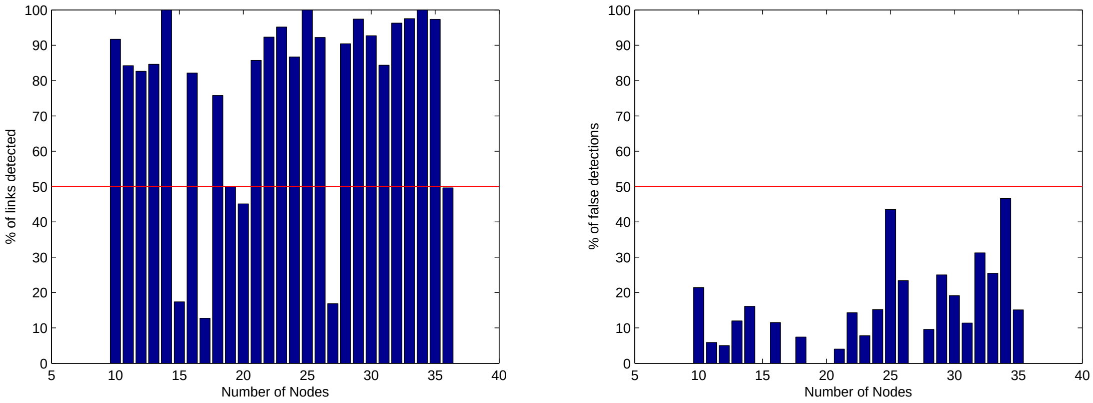


Figure 5.3: Average of Synchrony Score for different sampling durations on 10 nodes and 2 flows

affect the performance of our proposed method, as the difference between the average of linked and unlinked pairs remains distinctly large. Therefore, the proposed method can produce accurate estimations with observation periods as short as 1 second.

5.2 Thresholding Metrics

As discussed in Chapter 3, a set of global metrics, namely mean, standard deviation and median were selected as potential global thresholds for link estimation based on synchrony score. The performance of each metric is studied on the simulated set of networks described in the previous chapter according to two metrics, Correct



(a) Percentage of links correctly detected

(b) Percentage of links falsely detected

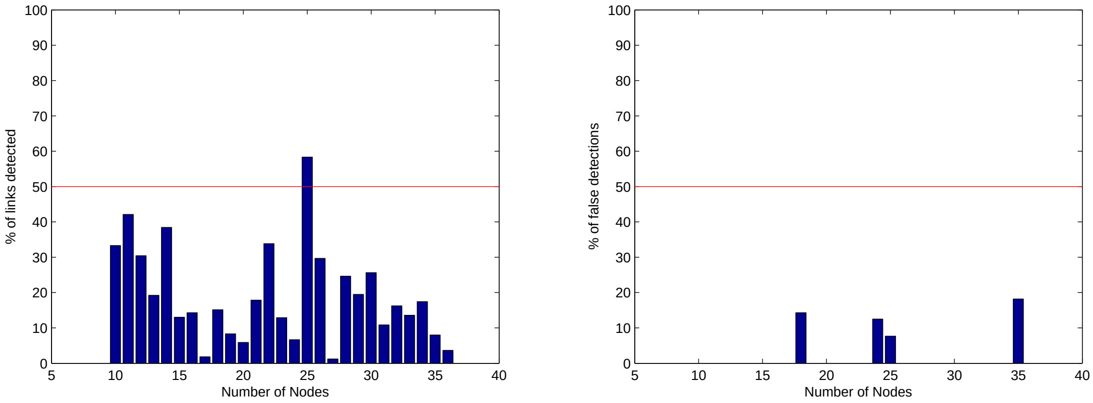
Figure 5.4: Performance of Mean as Threshold

Detection Rate (CDR) and False Detection Rate (FDR). CDR is defined as the ratio of number of links correctly detected to the total number of links, while FDR is the number of falsely detected links over total number of detected links. Following the criteria determined in Chapter 5, an example of a threshold is one that has more than 50% CDR and less than 50% FDR. Based on the results of multiple test cases, it was observed that the value of synchrony score for linked pairs never falls below half of the global mean. Therefore an extra thresholding condition is applied to all test cases to account for this observation.

Figure 5.4 illustrates the results of using the mean of all synchrony scores as threshold. It can be seen that this threshold succeeds in surpassing the requirement of 50% CDR for the majority of the tested networks. It also satisfies the FDR criteria for all tested network.

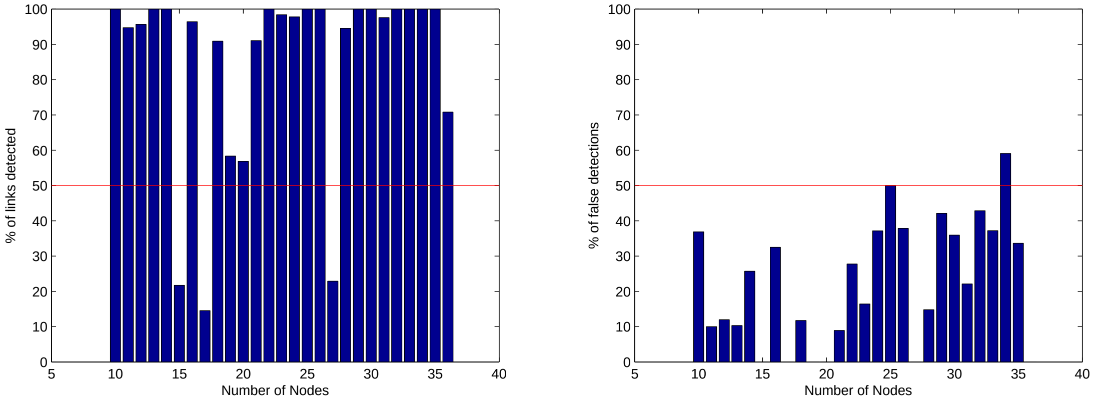
On the contrary, Figure 5.5 shows that standard deviation of synchrony scores almost never satisfies the CDR criteria, and therefore cannot be used as an accurate threshold.

In Figure 5.6, median is seen to be an even more suitable choice of threshold than



(a) Percentage of links correctly detected (b) Percentage of links falsely detected

Figure 5.5: Performance of Standard Deviation as Threshold

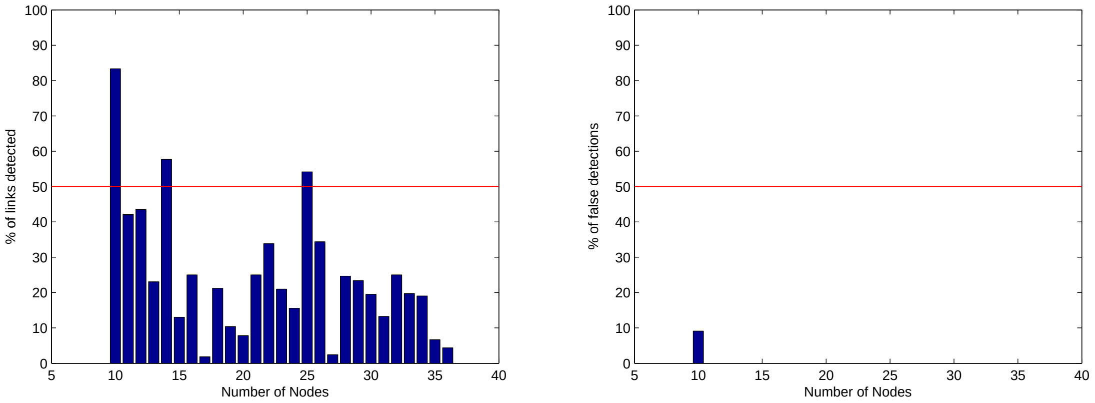


(a) Percentage of links correctly detected (b) Percentage of links falsely detected

Figure 5.6: Performance of Median as Threshold

mean, as it demonstrates a much higher CDR and a similar FDR in comparison with those resulted from using mean as threshold. And lastly, Figure 5.7 shows the results for the local thresholding technique based on a window size of 5 × 5. Even though the FDR performance of this technique is significantly better than all other thresholds, the low values of CDR necessitates its eliminations from the list of candidates.

Following the comparison of the presented results, Median is seen to provide the best performance as a threshold and therefore is used in generating adjacency matrices from the estimated Conversation matrix for simulations on MVP selection, described



(a) Percentage of links correctly detected (b) Percentage of links falsely detected

Figure 5.7: Performance of Local Adaptive Thresholds

in the following chapter.

5.3 Performance of MVP Method

The MVP identification method was used for target selection in the graph simulator to measure the resulting drop in connectivity. Points of comparison were also generated by simulating attacks on all other possible clusters, and the maximum connectivity drop achievable by attacking any of the clusters was compared with that of the MVP-selected cluster. The results, presented in Figure 5.8 indicate that clusters selected based on the MVP criteria lead to maximum connectivity drop for any number of nodes, thereby confirming the accuracy of the proposed MVP selection method.

This method was then applied on the topology estimations based on synchrony score, and the incurred connectivity drops were compared with the results of previous simulations. Value of r_{jammer} was set to 0.6th of the network's communications range and the attack was simulated for different numbers of nodes, producing the results illustrated in Figure 5.9. Since betweenness centrality relies on the topology

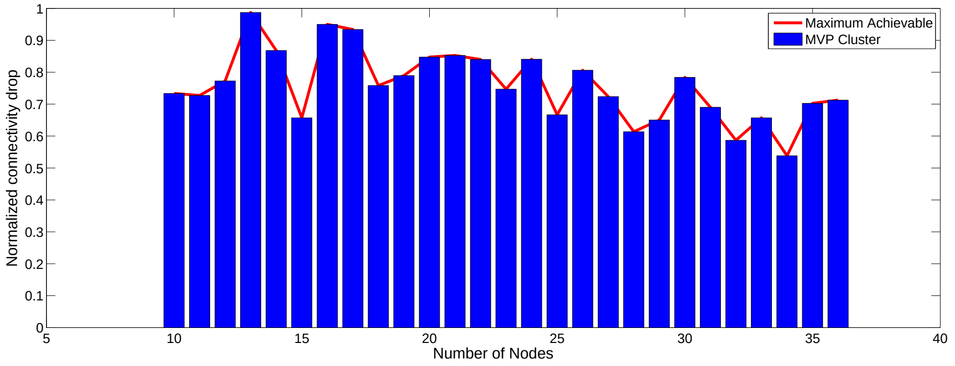


Figure 5.8: Disruption incurred by attacking the MVP-selected Cluster

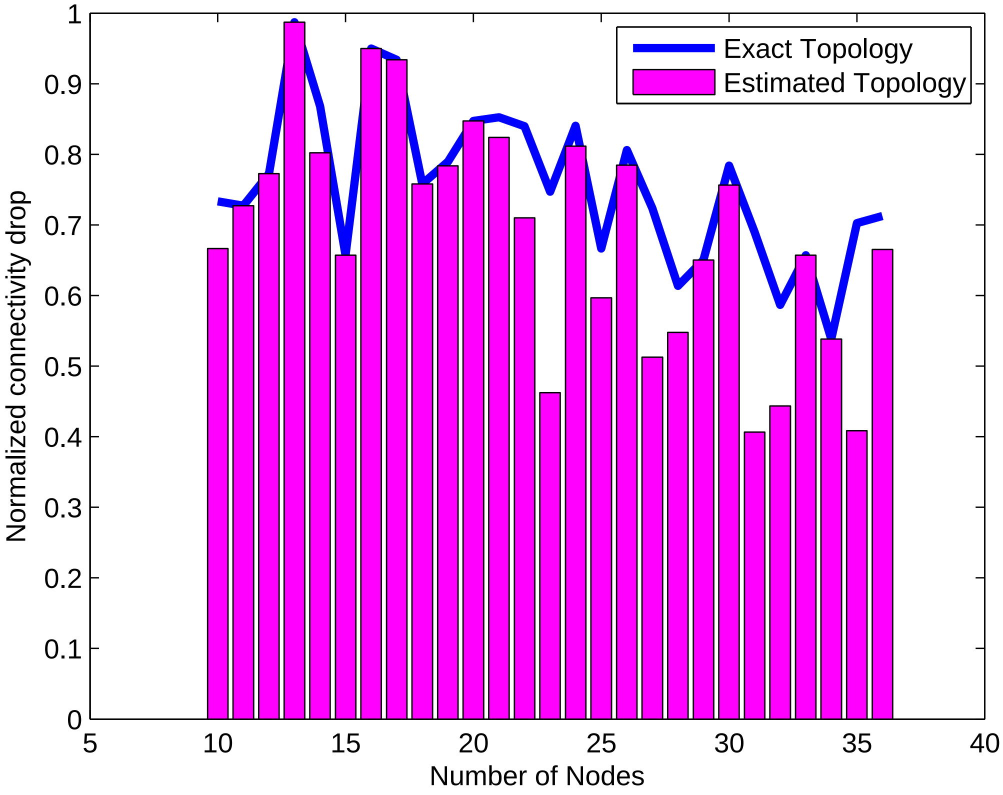


Figure 5.9: Performance of MVP in estimated topologies

of the network, inaccuracies in estimation of the topology results in errors in MVP. Therefore, with an increase in the elements of the topology, a larger error is expected. Also, since the jamming radius is fixed, by increasing the number of nodes the jammer covers a smaller area of the network. Thus, it is expected that the impact of jamming decreases with an increase in the size of the network. This phenomenon is evident in Figure 5.9, where the normalized connectivity drop follows a declining trend with an increase in the number of nodes. But to the extents of these inherent limits, the proposed MVP selection method is shown to result in large -and in most test cases, maximal values of disruption.

Chapter 6

Conclusion

This thesis demonstrates the vulnerability of covert ad hoc networks to jamming attack adaptive to physical layer parameters. For this purposes, a novel traffic analysis technique is proposed, which is capable of accurately estimating the topology of a target network in real-time. Also, a vulnerability analysis technique is proposed for detection of the most vulnerable point of attack when the jamming region of attacker is smaller than the area of the target network. Both methods were evaluated by simulations, which indicate the high accuracy of the traffic analysis technique, as well as the optimality of the proposed vulnerability analysis method.

Several future work items are inline. Firstly, this framework is yet to be experimentally validated. Validation of a temporal correlation between transmission onsets of connected hops may provide grounds for further developments in the privacy and covertness aspects of ad hoc networks. Also, measuring the temporal granularity of this attack for various MAC schemes may lead to design guidelines for covert networks and protocols. Lastly, The proposed framework is aimed at static or quasi-static targets. For a more realistic and accurate result, it may prove useful to include the dynamics of the target network in the model, and apply methods of optimal control theory to the inference and attack stages. The resulting model may form the foundations of a novel approach to investigation of cascade failures in multihop networks.

Bibliography

[1] Bernardetta Addis, Marco Di Summa, and Andrea Grosso. Removing critical nodes from a graph: complexity results and polynomial algorithms for the case of bounded treewidth. *Optimization online (www. optmization-online. org)*, 2011.

[2] ASHWIN Arulselvan, Clayton W Commander, Panos M Pardalos, and OLEG Shylo. Managing network risk via critical node identification. *Risk management in telecommunication networks, Springer*, 2007.

[3] Ilker Bekmezci, Ozgur Koray Sahingoz, and ŞAmil Temel. Flying ad-hoc networks (fanets): A survey. *Ad Hoc Networks*, 11(3):1254–1270, 2013.

[4] Jon L Bentley, Donald F Stanat, and E Hollins Williams. The complexity of finding fixed-radius near neighbors. *Information processing letters*, 6(6):209–212, 1977.

[5] Abraham Berman and Robert J Plemmons. Nonnegative matrices. *The Mathematical Sciences, Classics in Applied Mathematics*, 9, 1979.

[6] Suman Bhunia, Vahid Behzadan, P R Regis, and Shamik Sengupta. Performance of adaptive beam nulling in multihop ad-hoc networks under jamming. In *IEEE International Symposium on Cyberspace Safety and Security (CSS 2015)*, 2015.

[7] Suman Bhunia, Shamik Sengupta, and Felisa Vázquez-Abad. Performance analysis of cr-honeynet to prevent jamming attack through stochastic modeling. *Pervasive and Mobile Computing*, 2015.

[8] Herwig Bruneel and Byung G Kim. *Discrete-time models for communication systems including ATM*, volume 205. Springer Science & Business Media, 2012.

[9] Raffaele Bruno, Marco Conti, and Enrico Gregori. Mesh networks: commodity multihop ad hoc networks. *Communications Magazine, IEEE*, 43(3):123–131, 2005.

[10] Marco Conti and Stefano Giordano. Mobile ad hoc networking: milestones, challenges, and new research directions. *Communications Magazine, IEEE*, 52(1):85–96, 2014.

[11] Carolina Del-Valle-Soto, Carlos Mex-Perera, Raul Monroy, and Juan Arturo Nolazco-Flores. On the routing protocol influence on the resilience of wireless sensor networks to jamming attacks. *Sensors*, 15(4):7619–7649, 2015.

[12] Emilie Delaherche and Mohamed Chetouani. Multimodal coordination: exploring relevant features and measures. In *Proceedings of the 2nd international workshop on Social signal processing*, pages 47–52. ACM, 2010.

[13] Ayalvadi Ganesh, Laurent Massoulié, and Don Towsley. The effect of network topology on the spread of epidemics. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 2, pages 1455–1466. IEEE, 2005.

[14] Ingmar Glauche, Wolfram Krause, Rudolf Sollacher, and Martin Greiner. Continuum percolation of wireless ad hoc communication networks. *Physica A: Statistical Mechanics and its Applications*, 325(3):577–600, 2003.

[15] Miguel Angel Guevara and María Corsi-Cabrera. Eeg coherence or eeg correlation? *International Journal of Psychophysiology*, 23(3):145–153, 1996.

[16] Hong Huang, Nihal Ahmed, and Santhosh Pullurul. Jamming dust: A low-power distributed jammer network. Technical report, DTIC Document, 2010.

[17] Thomas Kreuz. Measures of neuronal signal synchrony. *Scholarpedia*, 6(12):11922, 2011.

[18] Thomas Kreuz, Daniel Chicharro, Conor Houghton, Ralph G Andrzejak, and Florian Mormann. Monitoring spike train synchrony. *Journal of neurophysiology*, 109(5):1457–1472, 2013.

[19] Vito Latora and Massimo Marchiori. Efficient behavior of small-world networks. *Physical review letters*, 87(19):198701, 2001.

[20] Ronald Meester and Rahul Roy. *Continuum percolation*. Number 119. Cambridge University Press, 1996.

[21] Wayne Niblack. *An introduction to digital image processing*. Strandberg Publishing Company, 1985.

[22] Giles Oatley, KEN McGARRY, and Brian Ewart. Prioritizing of offenders in networks. In *6th WSEAS International Conference on Simulation, Modelling and Optimization*, pages 22–24, 2006.

[23] Craig Partridge, David Cousins, Alden W Jackson, Rajesh Krishnan, Tushar Saxena, and W Timothy Strayer. Using signal processing to analyze wireless data traffic. In *Proceedings of the 1st ACM workshop on Wireless security*, pages 67–76. ACM, 2002.

[24] Konstantinos Pelechrinis, Marios Iliofotou, and Srikanth V Krishnamurthy. Denial of service attacks in wireless networks: The case of jammers. *Communications Surveys & Tutorials, IEEE*, 13(2):245–257, 2011.

[25] Arkady Pikovsky, Michael Rosenblum, and Jurgen Kurths. *Synchronization: a universal concept in nonlinear sciences*, volume 12. Cambridge university press.

[26] S Unnikrishna Pillai, Torsten Suel, and Seunghun Cha. The perron-frobenius theorem: some of its applications. *Signal Processing Magazine, IEEE*, 22(2):62–75, 2005.

[27] Mikail Rubinov and Olaf Sporns. Complex network measures of brain connectivity: uses and interpretations. *Neuroimage*, 52(3):1059–1069, 2010.

[28] Bart Scheers. Introduction of dynamic spectrum access technology in nato europe tactical communications. In *Military Communications Conference, MILCOM 2013-2013 IEEE*, pages 737–742. IEEE, 2013.

[29] Ralph O Schmidt. Multiple emitter location and signal parameter estimation. *Antennas and Propagation, IEEE Transactions on*, 34(3):276–280, 1986.

[30] Leo Spizzirri. Justification and application of eigenvector centrality. *Algebra in Geography: Eigenvectors of Network*, 2011.

[31] MF Sykes and JW Essam. Some exact critical percolation probabilities for bond and site problems in two dimensions. *Physical Review Letters*, 10(1):3, 1963.

[32] Stanley Wasserman, Katherine Faust, and Joseph Galaskiewicz. Correspondence and canonical analysis of relational data. *Journal of Mathematical Sociology*, 15(1):11–64, 1990.

[33] Duncan J Watts and Steven H Strogatz. Collective dynamics of âĂŸsmall-worldâĂŹnetworks. *nature*, 393(6684):440–442, 1998.

[34] Cedric Westphal. On maximizing the lifetime of distributed information in ad-hoc networks with individual constraints. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 26–33. ACM, 2005.

[35] Min Xie and Martin Haenggi. Towards an end-to-end delay analysis of wireless multihop networks. *Ad Hoc Networks*, 7(5):849–861, 2009.