An Analytical Black Hole Attack Model Using a Stochastic Topology Approximation Technique for Reactive Ad-Hoc Routing Protocols

Christopher W. Badenhop, Benjamin W. Ramsey, and Barry E. Mullins
(Corresponding author: Benjamin W. Ramsey)

Department of Electrical and Computer Engineering, Air Force Institute of Technology
2950 Hobson Way, Wright-Patterson AFB, OH 45433, USA
(Email: benjamin.ramsey@afit.edu)
(Received June 10, 2015; revised and accepted Sept. 6, 2015)

Abstract

This paper presents an analytical Black Hole attack model to predict the mean packet loss of ad-hoc networks using reactive routing protocols without apriori knowledge of the actual topology configuration. Topology information is summarized as a set of prototypical hop-distance profiles that describe likely hop distance perspectives within the topology and are generated using K-means clustering. Experiments are conducted to validate the theoretical attack condition, the hop-distance profiles, and prediction performance. Results show the model prediction falls within the 95% confidence intervals of packet loss through simulation of a variety of fixed and ad-hoc topologies.

Keywords: Ad-hoc networks, black hole attack, network availability modelling

1 Introduction

The computer network is a pervasive and critical asset in our society. It permits the sharing of distributed resources to achieve complex social, economic, and scientific objectives irrespective of locality. However, it is also a vulnerability to its hosts because any disruption, degradation, or denial of access to this network adversely affects the objectives of the distributed organization. Moreover, computer networks are subject to disruptive, degrading, and denial attacks at every layer of the network stack [2, 25, 38]. Ad-hoc networks are especially vulnerable to disruption because they rely on coordination *in-situ* rather than apportioning resources *apriori* as done in infrastructure-based networks. Ad-hoc networks provide data routing services to loosely coordinating groups or to address the need for multi-hop communication in environments without infrastructure. With respect to security analysis of systems, there has been significant research on the development of confidentiality and integrity analytical models. Classic models such as the Bell-LaPadula Confidentiality Model [7], Lipner's Integrity Model [24], and the Chinese Wall Model [10] have existed for decades. The body of this research has provided a foundational approach to proving security properties in systems under study.

Since networks provide a delivery service, the *availability* security property is of great importance to network designers. Unfortunately, the historical depth of research on analytical availability models is lagging behind that of *confidentiality* and *integrity* research. While there is some availability modeling research in [1, 14, 16, 23, 31, 39], the *de facto* approach to assessing the effects of availability attacks on networks is measured through simulation. Examples of this approach include work performed in [11, 19, 26, 32]. While the simulation approach has a clear utility, there are several drawbacks. First, the approach is exhaustive and scales poorly. High dimensional experiments may take orders of weeks or months to provide conclusions. Second, the simulation models require initial validation when used and revalidation upon any modification to the simulation model-base [4]. Third, complex interactions, such as causality, between simulation objects are abstracted and must be statistically estimated through repetition. Effective experiment design can certainly ascertain causality between simulated factors and response variables to generate regression models; however, their mathematical relationship remains hidden.

At the cost of fidelity, these challenges may be avoided by the use of analytical models for security analysis. The contribution of this research is the development of an analytical model for reactive ad-hoc protocols that measures availability degradation of networks subjected to Black Hole attacks. A Black Hole attack is a well-known denial of service attack for ad-hoc networks that deceptively attracts data to flow through nodes under control of an attacker. As packets arrive, they are silently dropped. Such a model can be used in conjunction with other availability models to influence design decisions of distributed system or ad-hoc network developers when limited imple-

mentation details exist. Moreover, the model explains the relationship between contributing factors for Black Hole attacks that are hidden when using simulated experimentation. While there has been extensive work in detecting, avoiding, and isolating Black Hole attacks, the relationship between the topology parameters and the attack effectiveness has not been extensively studied. Limited attack effectiveness has been measured using simulation in [17, 28, 34]; however, the scope of each study is limited to only a few topology types (e.g., protocol, number of Black Holes, number of nodes, and operating area). The results of these observational studies make it difficult to extrapolate performance for other types of ad-hoc topologies.

In [5], a theorem is developed for reactive ad-hoc routing protocols with hop-distance as a primary route metric selection criteria. During route discovery, if a Black Hole node is closer in hop distance than the destination to the source, then the Black Hole node may present a fake route to the downstream nodes with a metric that exceeds the metric of any legitimately proposed route. An analytical Black Hole attack model is developed that calculates the probability of this theorem being true for arbitrary source-destination pairs of a given ad-hoc network. Since the attack probability applies to any route in the network, it is a holistic measure of the susceptibility of a given network to Black Hole attack and may be useful for providing upper or lower bounds of network throughput degradation while under attack.

The analytical model in [5] is a function of the number of nodes in the network, the number of nodes conducting Black Hole attacks in the network, and the average node degree of the network. It assumes that the Black Hole nodes are uniform-randomly dispersed within the operating area of the ad-hoc network, and that all nodes within the network have equal probability of being a source or destination of new route. To avoid requiring absolute knowledge of the topology of the ad-hoc network under study, a topology approximation technique is used, seeded by one or more statistically estimated parameters of the topology under study. These parameters include the mean node degree of the network and the number of nodes. They are simpler to estimate prior to the instantiation of an ad-hoc topology than attempting to estimate the graph of the topology instance. The parameters are used to generate a n-ary 2-cube topology, which has average degree n and 2^n nodes [30]. The model uses this topology to calculate the probability of attack for all source and destination pairs of the ad-hoc network under study.

The motivation for the utilization of n-ary 2-cubes to approximate ad-hoc topologies is based on the intuition that high-dimensional topologies of an arbitrary orientation, when projected onto a 2-dimensional plane, *appear* as an ad-hoc topology. Moreover, the projection of a single n-ary 2-cube onto a plane may represent a set of flat topologies by rotating the n-ary 2-cube in the higher dimensional space. Unfortunately, the similarities are deceiving, and several issues make it challenging to use this as an approximation method. First, ad-hoc topologies have nodes with varying node degree, whereas the node degree for all nodes in a n-ary 2-cube have a constant degree. This means that as the variance of the node degree of an ad-hoc network increases, the approximation will not be able to represent portions of the network with extreme connectivity. Second, given an ad-hoc topology with a known node degree and number of nodes, it is likely that, due to the ridged definition of the n-ary 2-cube, a corresponding n-ary 2-cube approximation having the same values for both parameters does not exist. Any application using this approximation, including the Black Hole attack model, must perform a trade-off study to determine which n-ary 2-cube approximation minimizes calculation error, degrading the utility of the approximation. Third, ad-hoc topologies may become partitioned over their lifetime due to mobility or node failure. A n-ary 2-cube is unable to model network partitions because the node degree of the approximation is homogeneous within the topology. Fourth, two nodes may be within transmission distance within the projection of an arbitrarily rotated n-ary 2-cube onto a 2-dimensional plane; however, their Euclidean distance in the high dimensional space may beyond transmission range. This means that the projection will contain edges that do not exist in the n-ary 2-cube.

The work presented in this paper extends the work accomplished in [5] while addressing the disadvantages of using an n-ary 2-cube as an approximation technique. First, a simple simulated experiment is conducted to enhance the credibility of the theorems derived in [5]. Second, the Black Hole attack model is generalized for arbitrary network topologies. In this generalization, the topology state is known and a simulated experiment is conducted to show that the analytical model is able to predict the network level effects of Black Hole attack. Third, the generalized model is extended to incorporate unique aspects of ad-hoc networks; namely, that nodes may become partitioned and that the true topology state is difficult to realize prior to its instantiation. The n-ary 2-cube topology approximation is replaced by a set of prototype *neighborhoods*, derived statistically via k-means clustering. A third simulated experiment is conducted to validate the extended analytical Black Hole attack model. To illustrate the improvement of the analytical model derived in this work, it is compared with performance predictions using the original model defined in [5].

1.1 Ad-Hoc Network Routing Background

An ad-hoc routing service is comprised of four core components: 1) determining topology state, 2) calculating routes, 3) selecting a route, and 4) forwarding packets according to the selected route [35]. The predominant challenge for the routing service is to efficiently realize and maintain the state of network topology while contending

with confounding dynamics in the physical, RF, and logical domains. Examples of dynamic events include node power failures, RF interference, and topology discovery on initial deployment. Global awareness of these events is achieved through protocol coordination, through which participants discover and exchange local topology state information with peers to identify potential routes. The fittest route is selected from this state update per destination or as needed.

One major aspect of routing protocols is when routes are calculated. A *proactive* protocol will enforce a periodic synchronization between all nodes to achieve topology state coherency. A node with fresh topology information can immediately calculate the next hop in the forwarding path or, depending on the protocol, determine the complete route. To minimize coordination overhead, *reactive* routing protocols only coordinate when necessary. The trade-off between reactive and proactive strategies is route setup time and effective bandwidth. Proactive protocols have more deterministic route setup times at a cost of utilizing higher bandwidth [29]. Reactive protocols utilize less bandwidth for control packets, but have higher variance in the route setup period [22].

This research generally applies to reactive ad-hoc protocols; however, the specific work focuses exclusively on Ad-Hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing (DSR). Both of these have matured to be de facto reactive protocols and constitute a base design class from which other reactive protocols have been derived. In essence, to attempt a unified analysis, this work applies to the common aspects of all reactive protocols (i.e., the route discovery process) and, more specifically, to AODV and DSR.

1.2 Ad-Hoc On-demand Distance Vector Routing

AODV routing is a reactive routing, forward updating, hop-by-hop, flat, and single-path routing protocol [27]. The protocol is broken into three services: 1) Route Discovery, 2) Route Repair, and 3) Packet Forwarding. The Route Discovery process occurs when a source node desires to route to a destination. The source node sends a route request (RREQ) packet that is flooded throughout the network via broadcast. As the RREQ is propagating the network, intermediate nodes append their ID to the RREQ and store a forwarding rule towards the source in preparation of a reply message. When the destination (or an intermediate node that knows the forwarding path to the destination) receives a RREQ it responds with a route reply (RREP) message. The responding node places the path information collected during the RREQ into the RREP and sends it along the reverse path previously established during the RREQ flood to the source node. Each node that receives the RREP adds the forwarding rule to their route table and forwards the RREP toward the source. Because of the flooding nature of a RREQ, the destination generates a RREP for each discovered path.

Intermediate and source nodes, receiving a RREQ, RREP, or a route error (RERR) message, update their forwarding table if 1) the destination sequence number in the coordination message is higher than the one stored in their table, or 2) the destination sequence number is the same as the entry in its routing table, but the hop-count in the message is shorter. Coordination messages containing higher destination sequence numbers imply fresher routing information.

Packet forwarding is achieved via a distance vector table stored at each node in the network containing entries for each known destination. For each destination, the node stores the next hop, distance in hops to the destination, and the sequence number of the latest update to the route. When application packets arrive to be forwarded, the node examines the destination in the packet and determines the next hop using the appropriate entry in the routing table.

1.3 Dynamic Source Routing

DSR is a reactive, forward updating, source-based, and flat routing protocol [21]. Its route discovery and maintenance behavior is very similar to AODV; however, the major differences between the protocols are the manner of packet routing and how the routes are stored. Unlike AODV, the route is maintained completely by the source node in DSR. The source node is responsible for generating the route request and has complete freedom to select any route reply to use when routing packets. Instead of storing the route hop-by-hop, DSR uses source routing where the source node places complete routing information in each application packet. Each intermediate node along a route uses this information to determine the next hop. The intent of the designers is to follow the analog of the TCP/IP *fate sharing* [13] by placing the majority of the complexity burden at the end nodes.

The route selection method is not specified in [21], but rather, is left up to the implementation of the protocol. Many DSR implementations use hop count as the route selection metric, such as Network Simulator 2, PicoNet, and the Rice Monarch Project.

1.4 Related Work

A significant number of published research papers measure simulated Black Hole attacks on ad-hoc networks. Performance degradation from Black Hole attack is measured on AODV networks in [6, 11, 26, 28, 32]. For DSR, performance results can be found in [3, 9, 20, 33]. Performance measurements of Black Hole attacks in other networks types include [15, 17, 19]. Due to the large parameter space of ad-hoc networks, there is little overlap between each study; however, they all indicate that Black Hole attack decreases network throughput.

Several recent works develop analytical models to characterize the performance of Black Hole attacks. In [39],

a probabilistic model is developed to quantify the effects of a Black Hole attack in a smart grid network. In [12], an Adaptive Neural-Fuzzy Inference System (ANFIS) is created to detect Black Hole node behaviors. A Colored Petri-Net model is developed in [17]; however, the model must be simulated to derive results. The foundations of a formal Black Hole attack model for wireless sensor network routing protocols is proposed in [31].

In [1] an analytical model is presented to calculate network throughput under denial of service attacks; specifically, these attacks are Jellyfish and Black Hole. Their model estimates the availability of a network flow (i.e., a group of packets traversing a route) based the proportion of lifetime that a network flow incurs zero throughput. The expected time a route has zero throughput is calculated as the product of the probability that at least one malicious node is in an arbitrary route of a certain length and the expected correction time to expunge all malicious nodes from that route. The correction time is based on the number of attempts to detect the attack, rediscover an alternative route, and repair for each malicious node in the route. Given the expected interval of zero throughput, one can calculate availability as one minus the ratio of the time of zero throughput over the expected duration of the flow.

A completely different Black Hole model is proposed in [23] to model packet loss instead of throughput of an AODV Mobile Ad-hoc Network (MANET) during a Black Hole attack. Konig assumes uniform node density to simplify the topology so that the number of nodes included in a given topology search area may be determined. By letting the radius of this search area be a multiple of the transmission distance, one can geometrically determine the number of nodes reachable at each hop. The author of this method also makes an attempt to address the border effect errors with the uniform density assumption; however, the authors acknowledge that their method is imperfect. Given the set of nodes included in the i^{th} RREQ of the expanding ring search, Konig can find 1) the probability that at least one Black Hole is in the search area and 2) the probability that the destination is within the search area. By taking the product of these two probabilities for each phase of the ring search, the sum of products is the probability an arbitrary route in a network with a given network density is subject to Black Hole attack.

2 Revisiting the Hypercube Black Hole Attack Model

From [5], Black Hole node b in network topology G is able to provide a false route with a winning metric to drop application packets on a route from source node s to destination node d if:

$$\exists b \in B \quad s.t. \{h(s,d) > h(s,b)\}, \tag{1}$$

where $h(x,y)$ is the minimum hop distance between x and y in network topology G and B is the set of Black Hole nodes present in G. While a proof is provided in [5], the prior work did not provide experimental validation.

2.1 Validation of the Attack Condition

A series of simulated experiments are conducted to test the validity of Equation (1) by observing the effects of packet loss while varying the hop distances between the source, destination, and a Black Hole node over a linear topology. The use of a linear topology allows explicit control of the hop distances of each player in the experiment series. The linear topology consists of 21 nodes, where a single source node is placed in the center of the network and is flanked by 10 nodes on each side. For a given simulation experiment, the destination node is designated as one of the 10 nodes on the right of the source node and a Black Hole node is designated as one of the 10 nodes on the left. During the simulation, the source node attempts to establish a route to the destination. The Black Hole node participates during the route setup and attempts to move the route through itself. Once the route is selected, the source sends constant bit rate (CBR) traffic to the destination. If the Black Hole attack is successful, none of the packets reach the destination because they are being forwarded to the opposite side of the network to the Black Hole node, which drops all of them. Packet loss is recorded from 100 scenarios generated by testing all combinations of $h(s,b)$ and $h(s,d)$, where each hop distance takes on a value from 1 to 10. Each scenario is replicated 100 times to generate a mean normalized packet loss statistic, where normalized packet loss is the proportion of packets lost over the total number of sent packets. The entire sequence of experiments are conducted using both AODV and DSR protocols.

Each wireless ad-hoc node in the network is a simulation model, which is comprised of an antenna, radio, propagation model, and a protocol stack in Network Simulator 2.34 (ns-2.34). Specifically, the stack is comprised of an omni-directional antenna with unity gain, a 914MHz Lucent WaveLAN Direct Sequence Spread Spectrum (DSSS) radio, an implementation of IEEE 802.11 Medium Access Control (MAC) layer, and a reactive MANET routing protocol. The stack enables each node to provide packet routing for the wireless ad-hoc network. Besides basic routing services, some nodes are designated as application end-points, which send or receive CBR traffic. The linear topology is enforced by placing nodes in a line, where the transmission coverage area of each node contains a either two neighbors, or for the end nodes, a single neighbor. A Black Hole is a node with a modified MANET routing protocol designed to conduct Black Hole attacks and is identical to the simulation model used in [5]. The simulation transmission range of each radio is 250 meters.

The observed normalized packet loss for AODV and DSR as a function of destination and Black Hole hop distances are shown as a surface plot in Figure 1. A given point in the z axis is the normalized average packet loss observed when $h(s,b) = x$ and $h(s,d) = y$. The figure

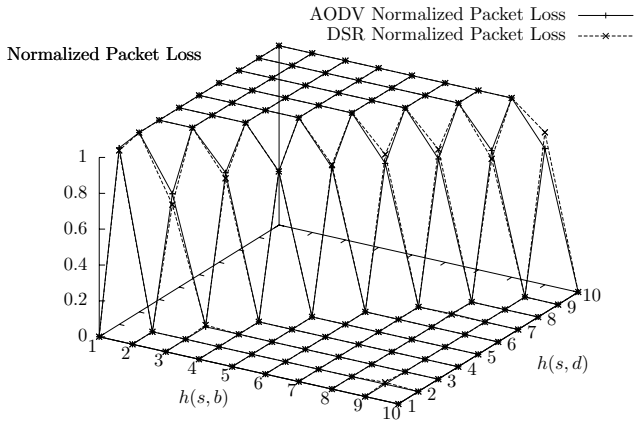


Figure 1: Normalized packet loss as a function of hop-distance

shows that in all cases where $h(s,b) \geq h(s,d)$, the packet loss is zero. Conversely, packet loss is incurred for each case where $h(s,b) < h(s,d)$. Packet loss is at 100% when $h(s,d) - h(s,b) > 1$. The reason that packet loss is only at 80% when $h(s,d) - h(s,b) = 1$ (i.e., the Black Hole node is one hop closer than the destination node to the source) is an artifact of the simulation models for AODV and DSR in ns-2.34. Recall that from [5], the shortest path a Black Hole can advertise to the source node without masquerading as the source has length $h(s,b)+1$. When $h(s,d) - h(s,b) = 1$ both the Black Hole and destination node will respond with routes having the same hop count metric. As a tiebreaker, the RREP arriving first is selected. Since $h(s,d) - h(s,b) = 1$, the RREP from the Black Hole node has fewer hops to traverse than the RREP created from the destination node. However, the simulation avoids RREQ broadcast collisions at each hop by waiting a uniformly random time period before rebroadcasting. When the destination and Black Hole hop distances to the source node are close, there are occurrences where the Black Hole node receives the RREQ at a later time than the destination because the predecessors of the Black Hole node encounter a larger cumulative random delay.

2.2 Decoupling the Hypercube Topology from the Model

The Analytical Black Hole model is the probability Equation (1) is true for all source destination pairs. This is calculated by considering all possible relative distances of $h(s,b)$ and $h(s,d)$ in a given network. From [5], the discrete probability of this event is

$$P(A) = \sum_{h=1}^{n} P(A|H=h)P(H=h), \tag{2}$$

where $P(A)$ is the probability of a Black Hole attack and $P(H)$ is the probability that $h(s,d) = h$. Given $h(s,d)$, the probability of a Black Hole attack is simply the probability that at least one of the B Black Hole nodes are closer than h hops to the source. This requires knowing the number of possible neighbors that are closer than h and finding the probability that at least one of the neighbors is a Black Hole node. The n-ary 2-cube topology is useful here because this quantity can be derived analytically given parameter n, which is the longest expected route length. Moreover, the symmetric properties of a n-ary 2-cube topology result in every node having the same quantity of unlabelled neighbors at each hop distance. This allows $P(A)$ to be calculated without considering the relative location of each source node within the topology. Let $q(x)$ be the quantity of neighbors including Black Hole nodes at hop distance x. The number of nodes that are closer than h hops is the sum of $q(x)$ for all $x = 1, 2, \ldots, h-1$. Given $q(x)$ is known for all values of x, N is the number of nodes in the topology, B is the number of Black Hole nodes in the network, then $P(A)$ is a hyper-geometric discrete random variable shown in Equation (3).

$$P(A) = \sum_{h=1}^{n} \left\{ \left(1 - \frac{\binom{(N-2)-\sum_{i=1}^{h-1} q(i)}{B}}{\binom{N-2}{B}} \right) \frac{q(h)}{N-1} \right\}. \tag{3}$$

Because this analytical model is derived for n-ary 2-cubes, the model assumes that all source nodes have the same $q(x)$ function. Decoupling the analytical model from the n-ary 2-cube topology requires that $q(x)$ is context dependent on the position of the source node within the network being analyzed. If the topology is known, then the number of $q(x)$ functions has an upper bound of N, implying that each node has a unique $q(x)$ function. Moreover, the conjecture is that the set of these $q(x)$ functions is sufficient to describe the network topology under study. If a topology exhibits symmetry, then there will consequently be duplicate $q(x)$ functions describing the network. Ignoring duplicate functions, fewer $q(x)$ functions are required to describe the symmetric topology. Let a *source node class* be a set of one or more nodes that share the same $q(x)$ function. More specifically, source node class C_k has $q_i(x) = q_j(x) \forall i, j \in C_k; x = 1, 2, \ldots, n$. When a route discovery is initiated, there is an associative probability that the source node originating the discovery belongs to a particular source node class. The source node class membership probability equation is simply the proportion of nodes in a class over the number of nodes in the network, where $|C_k|$ is the cardinality of class C_k. This is

$$P(s \in C_k) = \frac{|C_k|}{N} \forall C_k, k = 1, 2, \ldots, K. \tag{4}$$

Incorporating Equation (4) into the model results in

$$P(A) = \sum_{k=1}^{K} \sum_{h=1}^{n} P(A|H=h)P(H=h|s \in C_k)P(s \in C_k). \tag{5}$$

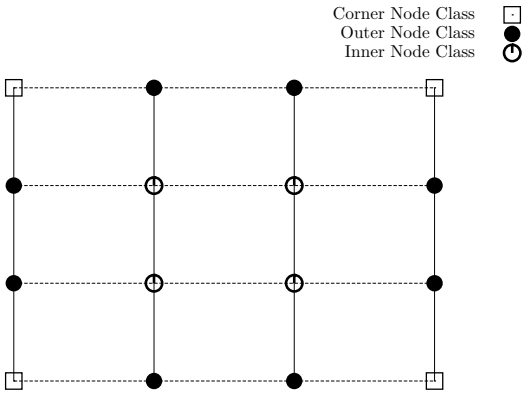


Figure 2: 4x4 Wireless grid topology with labeled source node classes

Note that K is the number of source node classes for the network and its value is a function of the topology under study. Expanding Equation (5) is

$$P(A) = \sum_{k=1}^{K} \sum_{h=1}^{n} \left\{ \left(1 - \frac{\binom{(N-2)-\sum_{i=1}^{h-1} q_k(i)}{B}}{\binom{N-2}{B}} \right) \frac{q_k(h)|C_k|}{N(N-1)} \right\}. \quad (6)$$

2.3 Validation of the Generalized Attack Model

Equation (6) is validated through a series of simulated experiments. To illustrate the concept of source node classes and $q(x)$ functions, these experiments use a simple fixed 4x4 grid network. To keep the topology fixed at 16 nodes and in a 4x4 grid structure, non-Black Hole nodes are removed from the network as Black Hole nodes are added. This keeps the number of source node classes and $q(x)$ functions constant. The distances between nodes force communication between only cardinally adjacent nodes in the grid. A 4x4 grid topology has three source node classes, labeled C_1: *Corner Nodes*, C_2: *Outer Edge Nodes*, and C_3: *Inner Nodes*. Figure 2 shows the topology with each node assigned to one of the three source node classes. From the figure there are four corner nodes in C_1, eight outer nodes in C_2, and four inner nodes in C_3 respectively. The $q_k(x)$ function (i.e., the quantity of neighbors x hops from a source node in class k) for each source node class is shown in Table 1.

Table 1: Values for $q_k(x)$ for each source node class in the 4x4 grid

Hop Distance	$x =$	1	2	3	4	5	6
Corner Nodes	$q_1(x) =$	2	3	4	3	2	1
Outer Edge Nodes	$q_2(x) =$	3	4	4	3	1	0
Inner Nodes	$q_3(x) =$	4	6	4	1	0	0

The normalized packet loss is observed as the number of Black Hole nodes are increased in the topology from one to eight. For each scenario, 50 4x4 grid topologies are generated. For each topology a subset of the 16 nodes are randomly designated as Black Hole nodes and 100 source-destination pairs are also randomly designated. Each connection pair is independently simulated, where the source attempts to establish a route with the destination in the presence of Black Hole nodes. Once the route exists, the source sends CBR traffic to the destination. Each simulation is repeated 10 times to account for the random packet delay incurred during the simulation and to avoid confounding effects of congestion and route caching, which are not currently accounted for in the analytical model. Statistics on the number of dropped, sent, and received packets are collected and used to estimate the mean normalized packet loss for each factor level combination.

The probability of attack is calculated using Equation (6) and is overlaid with the simulation results in Figure 3. Clearly the analytical model's predications are within the 95% confidence intervals (CIs) for all Black Hole levels for both protocols. The figure also shows that the attacker experiences diminishing returns as the number of Black Hole nodes grows, with an upper-bound at approximately 78% normalized packet loss. An attacker may use this curve to optimize cost of placement versus payoff. Using this network as a example, approximately three quarters of the maximum performance is achieved by deploying at least three Black Hole nodes. In terms of security defense analysis, the expected packet loss does not exceed 80%. System designers may use this upper-limit to implement distributed applications that tolerate operating conditions, such as through caching, redundancy, or multipath.

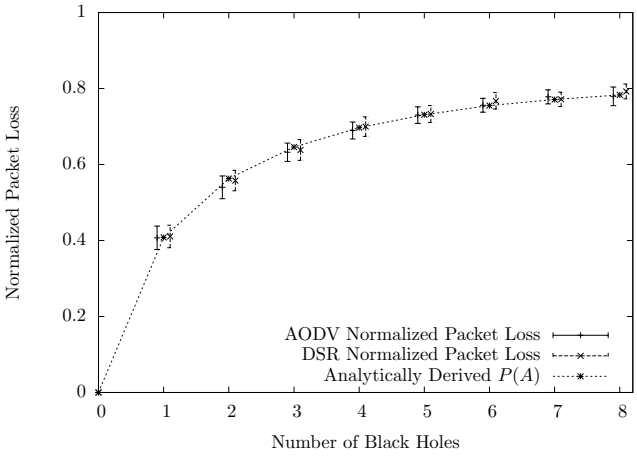


Figure 3: Normalized packet loss due to Black Hole attack for the 4x4 grid network

3 The Attack Model Adapted for Ad-hoc Networks

The analytical model presented in the previous section is generalized to account for any topology that may be described as a set of source node classes, each with a particular $q(x)$ function. However, there are several challenges to overcome so that this analytical model may be useful for ad-hoc networks while avoiding the n-ary 2-cube approximation technique. First, the topology is not known *apriori*, making it difficult to assess the susceptibility of a network is instantiated. Second, ad-hoc networks may be partitioned, which violates the assumptions of the original model. In this section, the analytical model is enhanced to address these two challenges.

3.1 Describing Ad-hoc Topologies Stochastically

In [8], the authors stochastically generate random topologies using a small set of parameters to empirically derive neighbor hop distance probability density functions for a variety of ad-hoc network types. This work expands on [8] by using K-means clustering on stochastically generated topologies to identify K distinct source node classes and the associative $q_k(x)$ functions (i.e., neighbor hop distance probability density functions) to represent an expected configuration of the ad-hoc network prior to its existence. Using this approach, only the deployment strategy, number of nodes, and operating area are required *apriori*. Unlike the case for known topologies, the number of classes is not bounded by the number of nodes N. Because the network may take on a variety of topology configurations, K may be orders of magnitude larger than N, which implies that a larger set of $q(x)$ functions are required to adequately describe an ad-hoc network than a particular topology instantiation such as the 4x4 grid topology, described in a previous section.

The strategy of this approach is to generate a set of source node classes that adequately describe the distribution of possible topology instantiations. This is accomplished stochastically by generating M random topology instances according to the expected number of nodes, area of deployment, and deployment strategy. For each of the M topology instances, the $q(x)$ function of every node is empirically derived, resulting in a collection of $M \times N$ distinct $q(x)$ samples. The $q(x)$ function samples are associated using K-means clustering [36]. This results in the identification of K source node classes, where the center of each class C_k is an n-dimensional vector of hop-distance quantities (i.e., $q_k(x)$). For stochastic topologies, the probability that source node s belongs to a particular source node class C_k is estimated as the proportion of the generated $q(x)$ samples in cluster k over the total number of generated $q(x)$ samples. The update to Equation (4) is shown in Equation (7).

$$P\left(s \in C_k\right) = \frac{|C_k|}{MN}, \tag{7}$$

where N is the number of nodes and M is the number of instantiated topologies.

3.2 Network Partitioning

Given the area, number of nodes, and deployment strategy, there is some probability that ρ nodes will be partitioned due to spatial separation. To account for partitioned nodes, let ρ_k be the average number of partitioned nodes for source node class C_k. This statistic can be derived using $q_k(x)$, where

$$\rho_k = N - \sum_{h=1}^{n} q_k(h).$$

When a destination node is partitioned from a source node, the existence of any Black Hole in the same network partition as the source node results in a Black Hole attack. Moreover, a route is established and additional network traffic is generated that would otherwise have not existed. The effect is that on a pair-wise comparison, partitioned networks with Black Hole nodes will not only have increased packet loss; they will also have an increase in the number of sent packets. Let ψ be a random event where the source attempts to connect with a destination that is one of the ρ nodes partitioned from the source node. With respect to a given source node class C_k, the probability a randomly selected destination is partitioned is

$$P\left(\psi_k\right) = \frac{\rho_k}{N-1}.$$

Given that the destination node is partitioned from the source node $s \in C_k$, the source node will only receive replies from Black Hole nodes during route discovery. Therefore, if there is at least one Black Hole node that is not partitioned from the source, then a Black Hole attack occurs. The equation for this is

$$P(A|\psi_k) = \begin{cases} B < \rho_k, & \left(1 - \frac{\binom{\rho_k - 1}{B}}{\binom{N-2}{B}}\right) \\ B \geq \rho_k, & 1 \end{cases} \tag{8}$$

Note that when there are greater or equal number of Black Holes nodes than the expected number of partition nodes, then at least one Black Hole node must exists in the same partition as the source node.

3.3 Stochastic Analytical Black Hole Attack Model for Ad-Hoc Networks

Considering the stochastic representation of the ad-hoc topology and accounting for partitioning, the revised form of the analytical model for Black Hole attack on ad-hoc networks is

$$P(A) = \sum_{k=1}^{K} \left\{ \left[P(A|\psi_k) P(\psi_k) + P(A|\psi_k^{'}) \left(1 - P(\psi_k)\right) \right] P(s \in C_k) \right\}. \tag{9}$$

Table 2: Four simulated ad-hoc network types under test

Type	Nodes	Area (m^2)	Density (m^{-2})
1	10	500	0.02
2	20	500	0.04
3	20	1000	0.02
4	40	1000	0.04

The probability of attack is the sum of the attack probabilities for all source node classes. For each class C_k, the attack probability accounts for events including partitioned destinations and non-partitions with probabilities $P(\psi_k)$ and $(1 - P(\psi_k))$ respectively. Since $P(A|\psi_k)$ is defined in Equation (8), this leaves $P(A|\psi_k^{'})$ to be defined, which is

$$\begin{aligned} P(A|\psi_k^{'}) &= \sum_{h=1}^{n} P(A|H)P(H=h) \\ &= \sum_{h=1}^{n} \left[\left(1 - \frac{\binom{N-2-\sum_{i=i}^{h-1} q_k(i)}{B}}{\binom{N-2}{B}} \right) \frac{q_k(h)}{N-\rho_k-1} \right]. \end{aligned} \quad (10)$$

Equation (10) is derived from Equation (3) and adjusted to account for partitioned nodes. With Equations (8), (10) and for completeness, the analytical model expression is expanded to

$$P(A) = \sum_{k=1}^{K} \left\{ \left[P(A|\psi_k) \frac{\rho_k}{N-1} + \left(1 - \frac{\rho_k}{N-1} \right) P(A|\psi_k^{'}) \right] \frac{|C_k|}{MN} \right\}. \quad (11)$$

3.4 Validation of Revised Model

An experiment is conducted via simulation to validate the revised analytical Black Hole attack model for ad-hoc networks. Four distinct topology types are chosen to represent a sample space of ad-hoc topologies that vary in operating area, number of nodes, and the resulting density. The properties of each topology type are described in Table 2.

Each topology type has its own set of source node classes, which are found using the population sampling and K-means clustering method described earlier in this paper. One thousand random topologies are generated to create large sample sizes for each topology type. K-means clustering is applied to each sample set, where $K = 200$ is found by analyzing the change in variance as K increases [37]. The experiment is a full factorial design with factors of topology type, number of Black Hole nodes (1 to 10), and ad-hoc network protocol (AODV and DSR), resulting in 80 distinct factor-level combinations. For each factor-level combination, 100 topology instances are generated and simulated independently. For each topology instance, 100 randomly selected source-destination pairs attempt to establish routes and transmit CBR traffic in the presence of Black Hole nodes. The quantity of replications is selected to minimize sampling bias in the results. The packet loss for each connection is recorded and used to derive an estimate of the expected packet loss for the factor-level combination. Because the analytical model does not account for congestion or mobility dynamics, they are not simulated in this experiment to avoid measuring confounding factors.

3.5 Results and Analysis

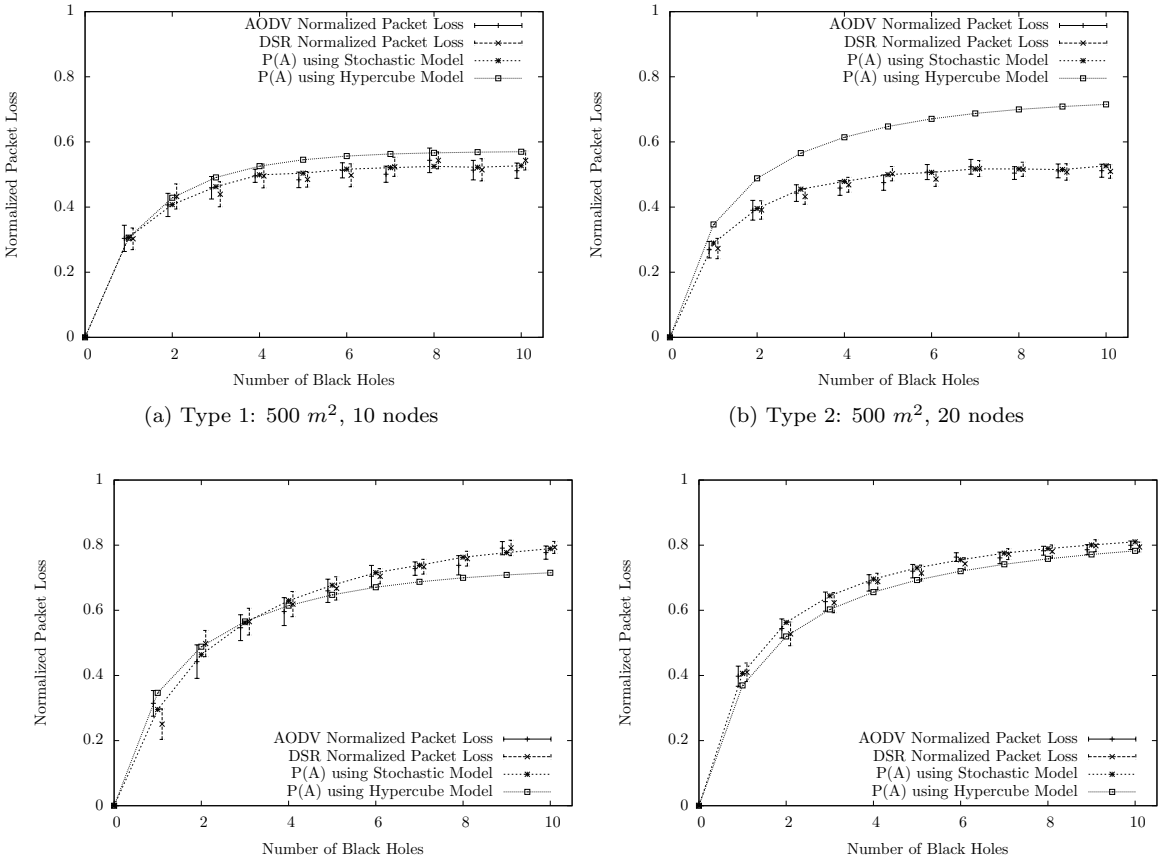
The results of the experiment are shown in Figure 4. For each topology type, the measured 95% CI of the normalized packet loss for AODV and DSR is plotted against analytical results calculated using Equation (11). The analytical model derived in [5] is also plotted to evaluate the benefits of the enhancements to this model. For this case, the hypercube with the closest number of neighbors is used as the topology approximation model. With respect to the figure, the x axis indicates the number of Black Hole nodes deployed into the network for a given normalized packet loss response.

The results show that the stochastic analytical model's prediction of packet loss falls within the 95% CI for all scenarios for each topology type. This is strong evidence in support of the claim that $P(A)$, as calculated by the revised analytical model, can be used to predict normalized packet loss of a network under Black Hole attack. Moreover, the original hypercube analytical model performs poorer than the stochastic model for the ad-hoc topology scenarios under study. In Figures 4a and 4d, the hypercube topology estimates are tolerable, but in several cases the analytically derived performance values are under or over estimating the simulation results. The hypercube topology approximation does not predict normalized packet loss for ad-hoc topology types 2 and 3. In Figure 4b the hypercube model significantly overestimates Black Hole attack. The hypercube performance curve in Figure 4c both under-estimates and over-estimates performance. Excluding the cases where there are zero Black Holes, the hypercube model prediction falls within the 95% CI packet loss in only nine of the 40 remaining data points presented in Figure 4.

Another noticeable difference between the performance predictions of the two models is that the stochastic curve has some slight variation between data-points while the hypercube performance curves do not. This is because the source node classes are derived statistically and consequently incur a degree of sample variation in the K class $q(x)$ functions. On the other hand, the hypercube analytical model uses the n-ary 2-cube topology, so it has no amount of variation in its single source node class $q(x)$ function.

4 Conclusion

This work provides a network availability model to be used to assess the impact of network disruption due to Black Hole attacks for insecure reactive ad-hoc protocols in ad-hoc topologies. Given the downsides to using a hypercube topology, the model is revised and a series of experiments are performed to validate these revisions.



(a) Type 1: 500 m^2, 10 nodes

(b) Type 2: 500 m^2, 20 nodes

(c) Type 3: 1000 m^2, 20 nodes

(d) Type 4: 1000 m^2, 40 nodes

Figure 4: Simulated packet loss of ad-hoc networks vs. hypercube and stochastic analytical model predictions

First, the attack condition is validated using an experiment where a linear topology is used to enforce a variety of hop distances between a source, destination, and Black Hole node. The results confirm the effectiveness of a Black Hole attack is based on the relative hop distances.

Second, rather than utilize the hypercube approximation technique, the analytical model is generalized to use arbitrary topologies for calculating the attack probability, where a topology is represented as a set of source node classes, each with a unique $q(x)$ function. A given $q(x)$ function represents an existential pattern within the topology that describes the number of neighbors at a given hop distance x. A second experiment is conducted using simulation for a grid network to validate the generalization of the analytical model. A 4x4 grid topology is used because the topology is deterministic and requires only three source node classes to represent the entire topology of 16 nodes. The experimental results show that the analytical model is able to utilize the $q(x)$ functions of the three source node classes to predict the mean normalized packet loss of the topology as a function of the number of Black Hole nodes in the topology.

Third, the analytical model is extended to account for specific aspects of ad-hoc topologies. Because the topology is not known until it is instantiated, the source node classes cannot be explicitly realized. Instead, they are statistically derived using K-means clustering on a large sample of instantiated topologies having the same number of nodes, operating area, and deployment strategy. The ad-hoc topology may contain zero or more network partitions. In this work, the model is extended to account for cases where the source node is partitioned from a destination node. A third experiment is conducted through simulation to validate the ad-hoc network adaptations to the model. Four different types of networks are studied by varying the number of nodes and operating area. The results show that the additions to the analytical model aid it in predicting the impact of Black Hole attacks on ad-hoc networks. Moreover, the experiment shows that the revised model provides better prediction of mean normalized packet loss than using the original hypercube model. For this experiment, the hypercube model correctly predicts 9 out of 40 scenarios, whereas the stochastic analytical model correctly predicts measured normalized packet loss for all 40 scenarios, suggesting a significant improvement in the model.

Given these accomplishments, there are several areas identified as future work. First, to minimize confounding effects and measure fundamental Black Hole attack response, the significant aspects of congestion and mobil-

ity have been avoided. With the foundational results of this research, future work should examine these aspects; the analytical work in [18] may provide a starting point. Second, there are several varieties of Black Hole attacks and many other types of network disruption attacks. The theory and model presented in this paper address a single type of Black Hole attack. This work can be readily extended to address other variants of the attack such as commandeering, masquerading, and wormholes.

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

References

[1] I. Aad, J.-P. Hubaux, and E. W. Knightly, "Impact of denial of service attacks on ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 16, no. 4, pp. 791–802, 2008.

[2] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile ad hoc networks," in *The 15th International Conference on Computer Modelling and Simulation (UKSim'13)*, pp. 693–698, 2013.

[3] A. S. Al Shahrani, "Rushing attack in mobile ad hoc networks," in *The Third International Conference on Intelligent Networking and Collaborative Systems (INCoS'11)*, pp. 752–758, 2011.

[4] T. R. Andel and A. Yasinsac, "On the credibility of manet simulations," *IEEE Computer*, vol. 39, no. 7, pp. 48–54, 2006.

[5] C. W. Badenhop and B. E. Mullins, "A black hole attack model using topology approximation for reactive ad-hoc routing protocols," *International Journal of Security and Networks*, vol. 9, no. 2, pp. 63–77, 2014.

[6] A. Bala, M. Bansal, and J. Singh, "Performance analysis of manet under blackhole attack," in *The First International Conference on Networks and Communications*, pp. 141–145, 2009.

[7] D. Bell and L. LaPadula, *Secure Computer Systems: Mathematical Foundations*, Technical Report MTR-2547, MITRE Corporation, 1973.

[8] C. Bettstetter and J. Eberspacher, "Hop distances in homogeneous ad hoc networks," in *The 57th IEEE Semiannual Vehicular Technology Conference*, vol. 4, pp. 2286–2290, 2003.

[9] N. Bhalaji and A. Shanmugam, "Association between nodes to combat blackhole attack in dsr based manet," in *The International Conference on Wireless and Optical Communications Networks*, pp. 1–5, 2009.

[10] D. F. C. Brewer and M. J. Nash, "The chinese wall security policy," in *IEEE Symposium on Security and Privacy*, pp. 206–214, 1989.

[11] K. Chadha and S. Jain, "Impact of black hole and gray hole attack in aodv protocol," in *Recent Advances and Innovations in Engineering (ICRAIE'14)*, pp. 1–7, 2014.

[12] A. Chaudhary, V. N. Tiwari, and A. Kumar, "A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in manets," *International Journal of Network Security*, vol. 18, no. 3, pp. 514–522, 2016.

[13] D. Clark, "The design philosophy of the darpa internet protocols," *ACM SIGCOMM*, vol. 18, no. 4, pp. 106–114, 1988.

[14] X. Fei and W. Wenye, "On the survivability of wireless ad hoc networks with node misbehaviors and failures," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 3, pp. 284–299, 2010.

[15] D. M. Gregg, W. J. Blackert, D. V. Heinbuch, and D. Furnanage, "Assessing and quantifying denial of service attacks," in *Military Communications Conference*, vol. 1, pp. 76–80, 2001.

[16] O.-E. Hedenstad, "Security model for resource availability - subject and object type enforcement," in *Military Communications Conference*, pp. 1–7, 2009.

[17] H. Hejiao and Z. Qiang, "Petri-net-based modeling and resolving of black hole attack in wmn," in *The 36th Annual Computer Software and Applications Conference Workshops (COMPSACW'12)*, pp. 409–414, 2012.

[18] X. Hui, W. Xianren, H. R. Sadjadpour, and J. J. Garcia-Luna-Aceves, "A unified analysis of routing protocols in manets," *IEEE Transactions on Communications*, vol. 58, no. 3, pp. 911–922, 2010.

[19] R. K. Jha, U. D. Dalal, and I. Z. Bholebawa, "Performance analysis of black hole attack on wimax-wlan interface network," in *The Third International Conference on Computer and Communication Technology (ICCCT'12)*, pp. 303–308, 2012.

[20] C. Jiwen, Y. Ping, T. Ye, Z. Yongkai, and L. Ning, "The simulation and comparison of routing attacks on dsr protocol," in *The 5th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–4, 2009.

[21] D. Johnson, Y. Hu, and D. Maltz, *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks*, Technical Report RFC-4728, IETF, 2007.

[22] D. Kiwior and L. Lam, "Routing protocol performance over intermittent links," in *Military Communications Conference*, pp. 1–8, 2007.

[23] A. Konig, D. Seither, R. Steinmetz, and M. Hollick, "An analytical model of routing, misbehavior, and countermeasures in mobile ad hoc networks," in *Global Telecommunications Conference*, pp. 1–6, 2009.

[24] S. Lipner, "Non-discretionary controls for commercial applications," in *Symposium on Privacy and Security*, pp. 2–10, 1982.

[25] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in rpl-based internet of things," *International Journal of Network Security*, vol. 18, no. 3, pp. 459–473, 2016.

[26] K. Pavani and D. Avula, "Performance evaluation of mobile adhoc network under black hole attack," in *The International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA'12)*, pp. 1–6, 2012.

[27] C. Perkins, E. Belding-Royer, and S. Das, *Ad Hoc on-demand Distance Vector (AODV) Routing*, Technical Report RFC-3561, IETF, 2003.

[28] N. Purohit, R. Sinha, and K. Maurya, "Simulation study of black hole and jellyfish attack on manet using ns3," in *The Nirma University International Conference on Engineering (NUiCONE'11)*, pp. 1–5, 2011.

[29] F. Qian, C. Zhongmin, Y. Jin, and H. Xunchao, "A performance comparison of the ad hoc network protocols," in *The Second International Workshop on Computer Science and Engineering*, vol. 2, pp. 293–297, 2009.

[30] Y. Saad and M. H. Schultz, "Topological properties of hypercubes," *IEEE Transactions on Computers*, pp. 867–872, 1988.

[31] K. Saghar, D. Kendall, and A. Bouridane, "Application of formal modeling to detect black hole attacks in wireless sensor network routing protocols," in *The 11th International Bhurban Conference on Applied Sciences and Technology (IBCAST'14)*, pp. 191–194, 2014.

[32] R. K. Sahu and N. S. Chaudhari, "Performance evaluation of ad hoc network under black hole attack," in *World Congress on Information and Communication Technologies (WICT'12)*, pp. 780–784, 2012.

[33] M. Salehi, H. Samavati, and M. Dehghan, "Evaluation of dsr protocol under a new black hole attack," in *The 20th Iranian Conference on Electrical Engineering (ICEE'12)*, pp. 640–644, 2012.

[34] K. J. Sarma, R. Sharma, and R. Das, "A survey of black hole attack detection in manet," in *The International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT'14)*, pp. 202–205, 2014.

[35] Z. Siyu, P. Yongxiang, Y. Yang, and L. Jianping, "An open architecture for the routing protocols design in ad hoc networks," in *The 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT'10)*, vol. 7, pp. 18–22, 2010.

[36] H. Suoto and S. B. Sen, "Cluster-based region formation for modeling manet," in *Military Communications Conference*, pp. 1–7, 2007.

[37] R. L. Thorndike, "Who belongs in the family?," *Psychometrika*, vol. 18, no. 4, pp. 267–276, 1953.

[38] P. Yau and C. Mitchell, "Security vulnerabilities in ad hoc networks," in *The 7th International Symposium on Communication Theory and Applications*, pp. 148–153, 2003.

[39] S. A. R. Zaidi and M. Ghogho, "Stochastic geometric analysis of black hole attack on smart grid communication networks," in *The Third International Conference on Smart Grid Communications (SmartGridComm'12)*, pp. 716–721, 2012.

Christopher Badenhop is a PhD student in the Department of Electrical and Computer Engineering, Air Force Institute of Technology. He received a Masters in Cyberspace Operations from Air Force Institute of Technology in 2012 and a Masters in Computer Engineering from Wright State University in 2006. His research interests include computer network security, embedded system security, and RF communications.

Benjamin Ramsey is an Assistant Professor of Computer Science at the Air Force Institute of Technology. He received the PhD degree in computer science from the Air Force Institute of Technology in 2014. His research interests include wireless network security and critical infrastructure protection.

Barry Mullins is a Professor of Computer Engineering at the Air Force Institute of Technology. He received the PhD degree in electrical engineering from Virginia Polytechnic Institute and State University in 1997. His research interests include cyber operations, software reverse engineering, computer and network security, critical infrastructure protection, and reconfigurable computing systems.