ASSESSING SECURITY RISK FOR WIRELESS SENSOR NETWORKS UNDER CYBER ATTACK

Brian Yarbrough

MIT Lincoln Laboratory
244 Sood Street, Lexington, MA, USA
brian.yarbrough@ll.mit.edu

Neal Wagner

MIT Lincoln Laboratory
244 Sood Street, Lexington, MA, USA
neal.wagner@ll.mit.edu

ABSTRACT

A common deployment strategy for wireless sensor networks is to position sensors according to a probabilistic distribution. Some sensor distributions offer advantages in redundancy, which helps ensure network survivability even with the loss of multiple sensor nodes to cyber attack. Properly selecting an initial sensor deployment distribution mitigates the threat of a denial of service (DoS) attack. While it is clear that some distributions are superior to others, it is not clear how to select the best sensor distribution as a defensive measure. Current strategies rely on mathematical analysis and are restricted to a subset of possible distributions. This paper examines the problem from an experimental perspective. We propose a novel method for evaluating how a given sensor deployment pattern may withstand a DoS attack based on agent-based simulation. We have implemented a first prototype of our model and illustrate its feasibility as part of a future decision support system.

Keywords: Wireless sensor networks, Cyber security, Agent-based modeling, Denial of Service cyber attack, Risk assessment

1 INTRODUCTION

In computer networks, devices are prone to being infected or compromised by malware that propagates from previously compromised neighbors. Devices that are more closely connected may be more at risk, yet "closeness" in a traditional network architecture is not typically due to physical proximity. In wireless networks, however, physical proximity plays a paramount role in determining the connectivity of two devices; a wireless node can directly communicate only with the subset of nodes that are within its radio range.

Separating wireless devices limits their ability to communicate, and thus limits the potential for malware to transfer between them. Just as with biological infections, separating the hosts can prevent spread. Network segmentation in software defined networks is a current application for this approach to network defense (Wagner, Şahin, Winterrose, Riordan, Pena, Hanson, and Streilein 2016). Segmenting a wireless ad hoc network into software defined clusters is common for performance improvements, but adding security to dynamic clusterhead protocols is challenging (Oliveira, Ferreira, Vilaça, Wong, Bern, Dahab, and Loureiro 2007). These segmentation and clustering approaches are focused on the proximity of devices as seen from the network routing layer of communication, and are described via software. We propose that the *deployment strategy*, the physical layout of wireless nodes in an ad hoc network, can impact how malware may propagate through a network. Furthermore, this behavior can be modeled and used to evaluate the

robustness of a particular layout to cyber attack. To demonstrate this, we use the example of a denial of service (DoS) attack on wireless sensor networks (WSN).

1.1 Wireless Sensor Networks

WSN are comprised of a large number of tiny, energy-constrained sensor nodes with weak processors and a small amount of memory. An individual sensor node is composed of sensor circuitry, a microcontroller, a wireless transceiver, and an energy supply (Islam, Shen, and Wang 2012). WSN of hundreds or thousands of sensors can be deployed on land, underwater, and underground, and have proven useful in military, industry, health, and environment applications (Nasir and Ku-Mahamud 2016) in which information is collected by sensor nodes and relayed by multi-hop routing to the sink, which acts as a base station. In practice WSN may cover several hundred square meters (Arora, Ramnath, Ertin, Sinha, Bapat, Naik, Kulathumani, Zhang, Cao, Sridharan, et al. 2005) and (Barrenetxea, Ingelrest, Schaefer, Vetterli, Couach, and Parlange 2008). The authors of (Taniguchi, Kitani, and Leibnitz 2011) and (Sharma, Patel, Bhaduria, and Prasad 2015) discuss methods for deploying wireless sensors over a large geographic area by means of controlled airdrop. While their efforts focus on achieving uniform deployment, similar techniques could be used to achieve an arbitrary distribution of sensors.

As with other ad hoc networks, WSN are very vulnerable to malicious cyber attack. An attacker's ability to wirelessly communicate with a node or to physically access an unmonitored node increases the attack surface. The decentralized decision making process relies on cooperation of multiple nodes; intrusion on a single node can paralyze a network or reroute information to the compromised node (Zhang and Lee 2000).

The spatial density of sensors within WSN is crucial. As sensors become more sparse in a given area, each hop must cover a greater distance. This effects power consumption, the number of hops required to reach the sink, and how messages might route through a network. For our purposes, this also changes how a DoS attack may degrade network operations.

1.2 Cyber Security Assessment

While there is a multitude of methods for evaluating WSN performance, none of these methods focus on optimizing a sensor deployment strategy to be more robust against cyber attack.

We propose a cyber security risk assessment tool that captures a WSN under DoS attack. The tool utilizes a modeling and simulation approach to assess the security posture of a given WSN and identify WSN deployment strategies that are less susceptible to a DoS attacks.

The rest of this paper is organized as follows: Section 2 discusses WSN and DoS attacks in detail, Section 3 describes our agent based modeling approach, Section 5 presents the experimentation and results, and Section 6 concludes.

2 WIRELESS SENSOR NETWORKS

2.1 Routing and Security

Numerous routing protocols exist for WSN and can be divided into *flat-based* routing, *hierarchical-based* routing, and *location-based* routing (Al-Karaki and Kamal 2004). In this study, we model location-based routing, which uses a sensor node's physical position in the network to determine routing. A subset of location-based routing is greedy packet forwarding, where traffic is always directed towards the sink. We

model *random nearer neighbor*, which allows the sender node to randomly select a node closer to the sink and forward the packet to that node. This strategy minimizes accuracy of information needed about neighbors, thereby reducing the number of operations required to send a packet (de Morais Cordeiro and Agrawal 2011).

The multi-hop nature of WSN and other ad hoc networks makes routing a primary concern, since every node is potentially responsible for receiving and forwarding traffic. As a consequence, numerous attacks focus on exploiting the network layer to deny service. Network layer WSN DoS attacks include modification of routing information, selective forwarding, sinkhole attacks, Sybil attacks, wormholes, HELLO flood attacks, and acknowledgment spoofing (Karlof and Wagner 2003). We focus on selective forwarding, in which a compromised node along the route refuses to forward certain messages; these messages are dropped from the network and never reach the sink. In the simplest case, a compromised node behaves like a black hole and refuses to forward any packets. This is known as a black hole attack.

In our model, a compromised sensor that becomes part of the black hole attack only has the opportunity to drop packets which would have been forwarded to it as part of the normal routing protocol. This is in contrast to a sinkhole attack, in which an attacker exploits the routing algorithm to direct a disproportionate amount of traffic to the compromised node and increase the impact of the attack. Our use of random nearer neighbor makes it difficult or impossible for an attacker to create a sinkhole (Sharma and Bahl 2017).

Defending against network layer DoS attacks is a challenging, ongoing area of research. There are several algorithms for detecting black holes and other intrusions in a network (Butun, Morgera, and Sankar 2014), but they all come with significant energy and complexity overhead. Additionally, many of these methods become less effective when multiple nodes in the network are compromised, or when a node uses intelligent selective forwarding. Redundant routing of messages across disjoint paths mitigates the risk of a node blocking messages to the sink, but is wasteful of power and bandwidth. Furthermore, it may be difficult or impossible to achieve redundancy in a sparse network (Raymond and Midkiff 2008).

An individual sensor node can be compromised through a variety of means, such as physical attacks and false node attacks (Padmavathi and Shanmugapriya 2009). These attacks can allow an attacker to set a foothold in the network. From this foothold, we assume that an adversary can spread an exploit from a compromised sensor node to a healthy one. In this way, the number of nodes acting as black holes increases and infection spreads towards the sink.

2.2 Coverage

One of the fundamental problems in WSN is the *coverage problem*, which reflects how well an area is monitored or tracked by sensors. Coverage focuses on how the network interacts with the terrain on which it is deployed. We are primarily concerned with the robustness of the network's ability to monitor an area during a DoS attack, so coverage is the natural performance metric for our purposes.

We use the definition from (Huang and Tseng 2005). Given a set of sensors, $S = s_1, s_2, ..., s_n$, in a two-dimensional area A, where each sensor s_i, $i = 1, ..., n$, is located at coordinate (x_i, y_i) inside A and has a sensing range of r_i, a location in A is said to be *covered* by s_i if it is within s_i's sensing range.

The authors of (Liu and Towsley 2004) demonstrate that for a 2D plane with a uniformly distributed WSN, the probability that a given point is covered by at least one sensor is governed by the sensing range of the sensors and the node density. This greatly simplifies the selection of a deployment strategy, as the network planner can simply deploy the appropriate node density to achieve the desired coverage probability. Unfortunately, uniform WSN deployments are unsatisfactory for many applications. The need to evenly distribute energy loading across a network, known as the energy hole problem, as well as the desire for

increased redundancy near the sink encourages deployment strategies that place sensors according to a Gaussian distribution with the sink at the center point.

Under a Gaussian distribution, the probability of a particular point being covered is governed by distance from the center point, Gaussian standard deviation, sensing range, and the total number of nodes (Wang, Xie, and Agrawal 2008). Multiple unknowns in the single equation increase the burden on the network planners. For example, if the network planners know the required area and minimum coverage probability, the equation can only provide either the number of nodes or the Gaussian standard deviation.

In cases where the deployment strategy does not follow a probability distribution, similar mathematical analysis is not tractable. To find the optimal network configuration a different approach is required. The approach which we propose to accomplish this is based on agent-based modeling.

3 MODELING SENSOR NETWORKS

3.1 Simulation Model

Agent-based (AB) modeling and simulation is a well-established scientific method for conducting complex system analysis. AB models are decentralized and define the behavior of many individual agents, where each agent follows its own behavioral rules. These agents operate and interact in the same environment, and these interactions reveal emergent systems dynamics (Borshchev and Filippov 2004).

The two types of agents in this model are wireless sensors, referred to as nodes, and sinks, which act as a base station. Each agent makes autonomous decisions according to a specified set of rules. This closely resembles how actual WSN function: algorithms are executed independently by nodes, without full network knowledge. In our model, a node agent can be either healthy or compromised. Healthy nodes attempt to generate, receive, and transmit messages. Compromised nodes attempt to compromise more nodes; they do not forward messages from healthy nodes to the sink. The sink agent receives messages from neighboring nodes and conglomerates results. Nodes and sink are deployed across an area. The size of this area is arbitrary and best defined as a relative size to the node radio range. This can be modified depending on the application being modeled.

Each node is connected to each of its neighboring nodes by a directed link. A node is a neighbor if it is within the specified radio range, and a link is formed from a node to any neighbors who are closer to the nearest sink along a straight line distance. The exception is if a node has the sink within its radio range, then it only forms a link to the sink. We deployed the sink in the center of the area, so the general form of each simulation was a distribution of nodes around the sink with links pointing to the center, as shown in Fig. 1.

Routing is performed by a series of autonomous decisions made by the concerned node at each hop of a route. We use a protocol that chooses one of k linked neighbors with probability $1/k$ and forwards the message to that node (Nelson and Kleinrock 1984); in the WSN world this is known as random nearer neighbor.

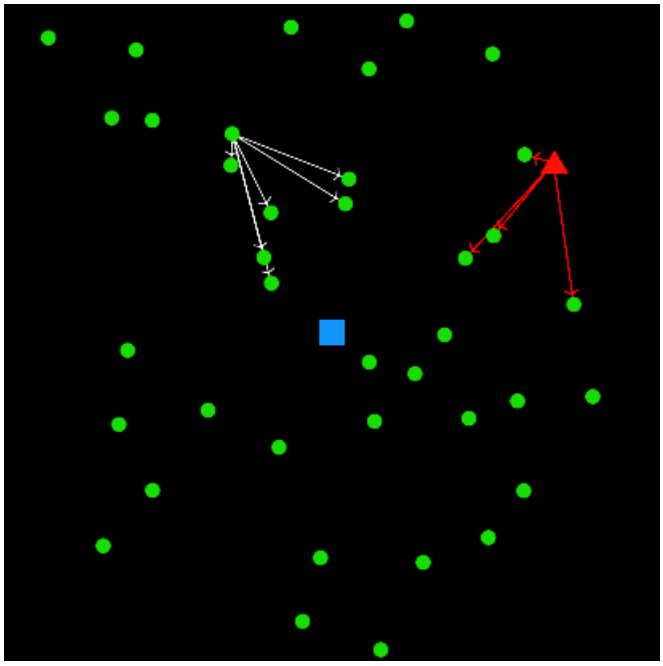


Figure 1: Example WSN model. Green circles are healthy nodes, the red triangle is a compromised node, the blue square is the sink. Directed links route traffic towards the sink or provide an avenue for compromise (most links are hidden for clarity).

Once a node agent becomes compromised, the rules that it uses to make decisions change. For example, compromised nodes take a much more aggressive stance and always transmit a message when given a chance within the routing protocols. By giving undue priority to its own messages, a compromised node is *greedy* and degrades legitimate traffic flow even if it is not directly intercepting messages (Wood and Stankovic 2002). A compromised node sends a message to a linked node, and with some probability compromises that node. This spread occurs along established communication channels, so tends to propagate towards the sink.

This AB model executes in time steps. We define a *step* as the opportunity for every node to send a message. Using steps in this manner allows us to study temporal dynamics: how the network changes over time. Some WSN applications may request reports from sensors several times a minute while others may only require information once a day; in each case, it is still a single simulation step. This increases the flexibility of this model.

While energy depletion is a primary concern for WSN, we assume that DoS attacks occur much more quickly than sensors deplete energy, so we leave the concept of dead agents to future work.

3.2 Performance Metrics

Adapting the definition of coverage presented in Section 2.2 to an agent based model yields the following: We are given a set of identical sensors, $S = s_1, s_2, ..., s_n$, in a two-dimensional area A, where each sensor s_i, $i = 1, ..., n$, is located at coordinate (x_i, y_i) inside A and has a sensing range of r_s. Let H be a subset of S where each sensor h_i is healthy and is connected to the sink via a route with only healthy nodes. The area A is divided into m squares, where each square p_j, $j = 1, ..., m$, is located at coordinate (x_j, y_j) inside A. A

square p_j is said to be *covered* if there exists at least k sensors in H where the distance between (x_i, y_i) and $(x_j, y_j) < r_s$.

Here, k is a natural number that specifies the minimum number of sensors which must cover a square. We use $k = 1$.

In other words, we define a square of area as covered if it is within the radio range of at least one healthy node and that node has at least one route of healthy nodes to the sink.

A given node will likely have multiple routes to the sink, so a square can be covered even if there is no guarantee that every single message from its covering node will reach the sink. Many WSN are intended to detect events, so it is not critical that every message makes it through to the sink; rather, there must be a certain level of confidence that at least enough messages will arrive (Krishnamachari, Estrin, and Wicker 2002).

In addition to measuring overall coverage, we measure coverage by Cartesian quadrants. The sink at the center of the area serves as the origin. This provides more insight as to how the DoS attack spreads through the network.

4 MODEL VERIFICATION

The purpose of this section is to present a verification of our proposed model. We accomplish this by comparing the initial state of our model to the analytical expectation for a WSN deployed according to a Gaussian deployment strategy. For the purpose of verification, sensor deployment has been bound to a circle of radius R, so as to coincide with the mathematical predictions. For the case study in Section 5, deployment occurs as a square to appropriately fill the area of concern.

In (Wang, Xie, and Agrawal 2008) Wang, et al. derive the coverage probability with respect to a 2D Gaussian distribution centered at a single sink and with the standard deviation independent and equal in the two dimensions x and y (i.e., $\sigma_x = \sigma_y = \sigma$). N represents the number of wireless sensor nodes, r_s is the sensing range of a single node, and R is the distance from the sink to the network boundary. The coverage probability f_d of a point p with a distance d, $r_s \leq d \leq R$, to the center point is given as

$$f_d(\sigma, d, r_s, N) = 1 - \left(1 - \int_{d-r_s}^{d+r_s} \frac{1}{2\pi\sigma^2} e^{\frac{-l^2}{2\sigma^2}} L\, dl\right)^N \tag{1}$$

where L is given as

$$L = 2l \cos^{-1}\left(\frac{l^2 + d^2 - r_s^2}{2ld}\right) \tag{2}$$

Together, equations 1 and 2 give the probability that a single point at distance d from the sink is covered. We desire to know the average probability that a point is covered for any d. Fixing σ, r_s, and N as constant yields the average coverage probability C.

$$C = \frac{1}{R - r_s} \int_{r_s}^{R} f_d(\sigma, d, r_s, N)\, dd \tag{3}$$

The value C provides an analytical estimate of what overall area coverage can be expected for a given sensor deployment strategy.

Comparing the average coverage probability to the overall coverage in the model allows for verification of the initial conditions of the model, before the start of the simulated DoS attack. Figure 2 shows the compiled results of 100 iterations for each deployment strategy when $r_s = 10$ and $R = 50$; the analytical predictions from equation 3 are superimposed as red X's.

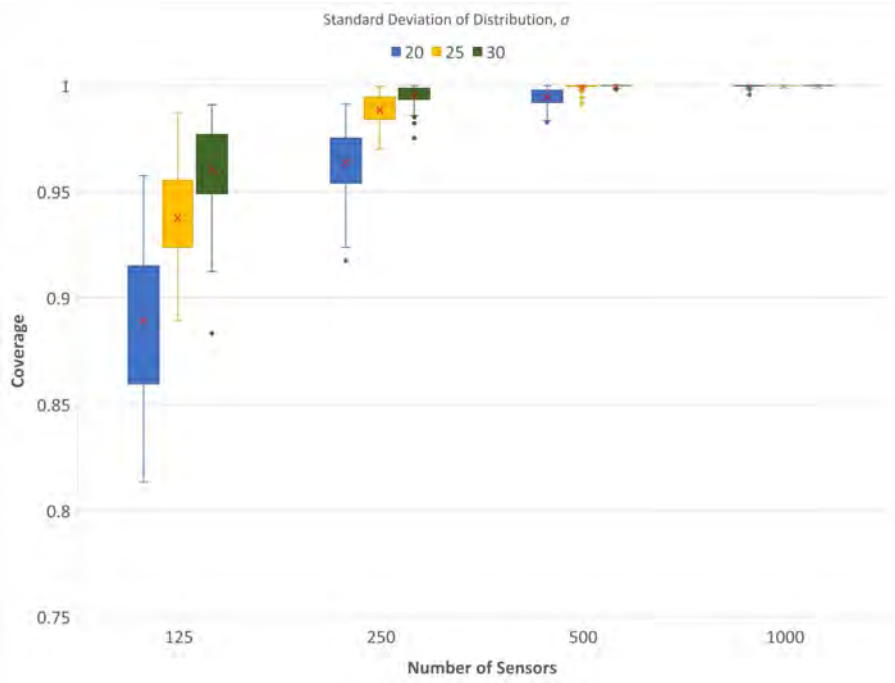


Figure 2: Verification of initial network conditions for various deployment strategies. Results from equation 3 are indicated by red X's.

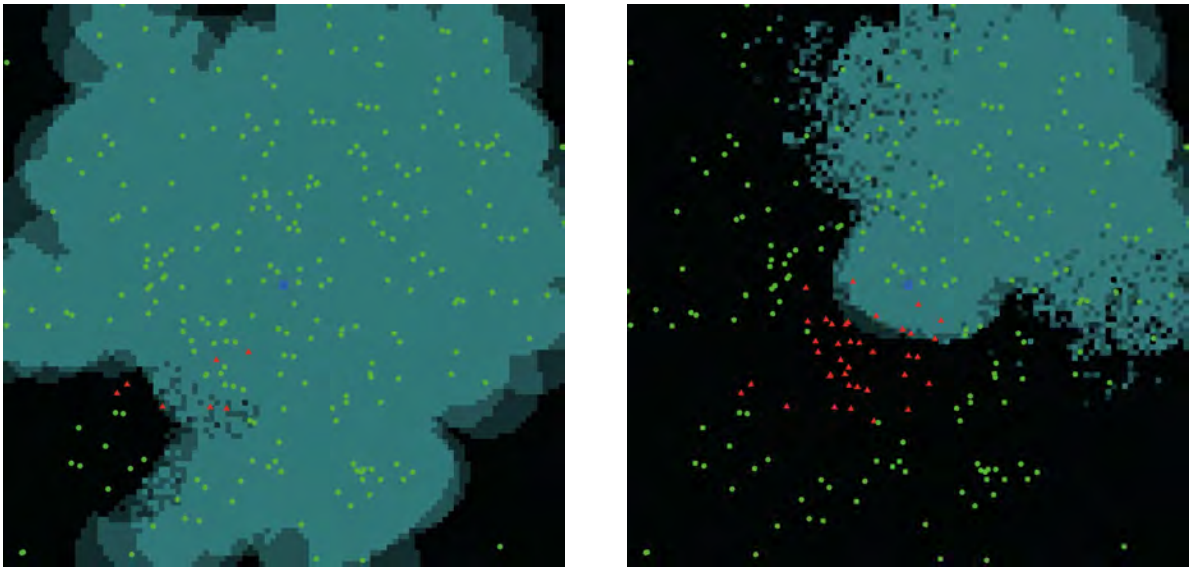
As is always the case, there is some variability between the theoretical predictions and the experimental results. Yet for these twelve deployment strategies, the mean squared error is only 8.30×10^{-5}. This extreme closeness in results verifies our model's initial predictions on coverage, and encourages confidence in the subsequent predictions, as the DoS attack occurs.

5 EXPERIMENTAL CASE STUDY

The proposed WSN simulation model is implemented in NetLogo (Wilensky 2017), a common software package for conducting AB experimentation. We illustrate the use of this model via a case study in which an adversary launches a DoS attack on the network, and we compare network performance based on deployment strategy.

5.1 Setup

To scale our environment, we base parameter ratios off of a common WSN mote, the TelosB (Memsic 2013). Our environment is an array of 10,201 squares arranged in a 101x101 grid. The radio and sensing range of each sensor is set to $r_s = 10$ squares. The real-world size of a square is arbitrary, but to be proportional to the wireless range of the TelosB, a single square represents anywhere from 2 to 10 meters. This places the maximum size of our environment at approximately one square kilometer. As discussed in Section



(a) Step 12; *coverage* = 84%

(b) Step 70; *coverage* = 38%

Figure 3: Screenshots of the simulation running. Covered squares are highlighted in cyan. The attack is moving in from the bottom left.

3, the length of time that each step represents is arbitrary, but the TelosB can be programmed to report measurements as frequently as every few seconds or as seldom as once every few days. For this study, we assume that a single time step is on the order of minutes.

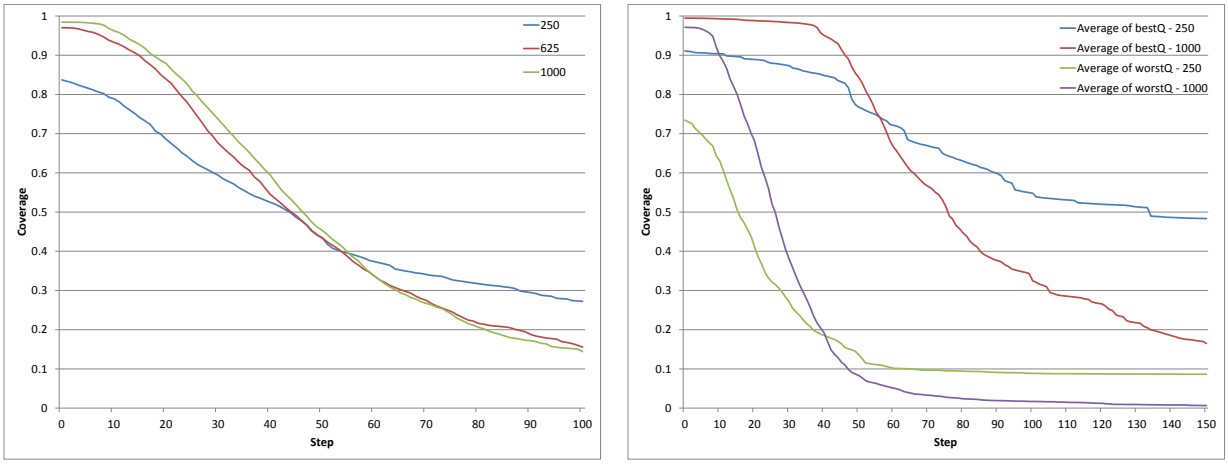
We consider only the case where a single sink is deployed at the exact center of the environment, and use a uniform distribution of sensors over the area as our baseline to compare against several Gaussian distributions. Having fixed the other parameters, the only two variables to consider in the model are N, the number of devices, and σ, the standard deviation of the Gaussian distribution.

It is the attacker, not the defender, who selects the starting point for the DoS attack. Although often the adversary may have an easier time compromising a device on the periphery of the network, this is not always the case. Because of this, we run an equal number of experiments with the initial compromise located at 30% and 85% of the distance between the sink and environment edge (approximately 15-squares and 43-squares from the sink, respectively).

The simulation is run with $N = 250$, 625, and 1000 while $\sigma = 20$, 25, and 30. These values were selected based on results of preliminary experimentation. Each of these combinations is run with five different random seed values, for a total of 120 runs, including the runs on the uniform distribution. These results are averaged to achieve a more complete picture of the behavior space. A screen-shot of the simulation running with $N = 250$ and $\sigma = 25$ is shown in Fig. 3.

5.2 Results

For this case study, we set the minimum acceptable area coverage at 70%. This is a much lower coverage than is acceptable for many applications, but may be sufficient for others. Fig. 4 shows the impact of deploying more sensor nodes.



(a) Average loss

(b) Best and worst quadrant loss

Figure 4: Coverage loss over time by number of sensor nodes, N.

We first consider average network coverage, Fig. 4a. Based purely on the objective of maintaining at least 70% coverage, more sensors are better because the results show longer network lifetime with more nodes. However, the additional 375 nodes from 250 to 625 nodes increases lifetime by 52%, while an additional 375 nodes from 625 to 1000 nodes yields only another 31% of network life. When these diminishing returns are coupled with a cost function, the extra nodes may not be worth the benefit they provide.

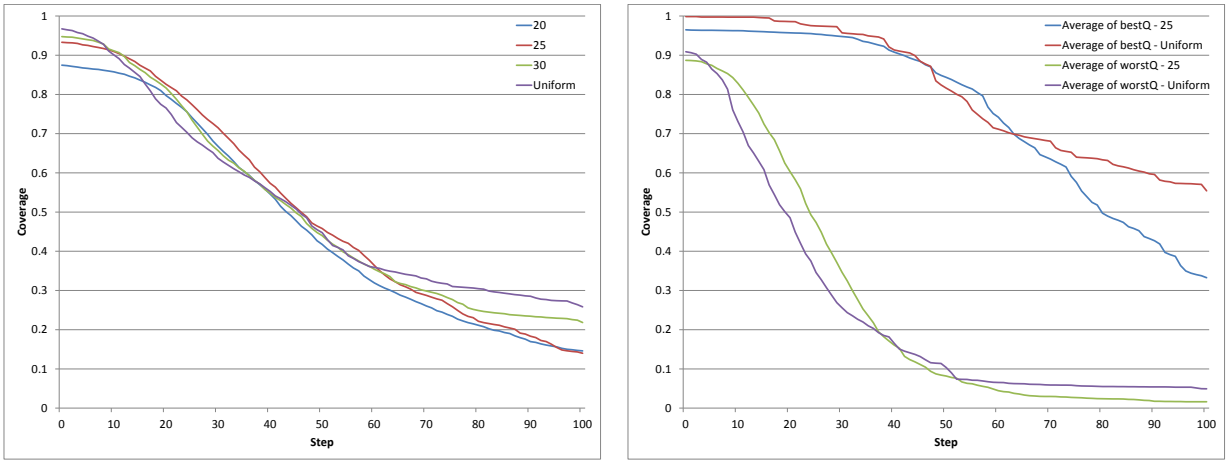
As the attack reaches the final stages, the sparsest network actually has the best coverage. The sparse network makes it more difficult for the attacker to spread compromise and, thus is more robust to attack than denser networks. Table 1 compares the percentage of the network that is compromised over time. The percentage of nodes throughout the network that are compromised is significantly greater in the denser networks. As a result, the impact on coverage is greater. Limiting the number of nodes in a network, for some WSN environments, places a ceiling on the damage that this type of DoS attack can achieve.

Step	$N = 250$	$N = 625$	$N = 1000$
30	8%	7%	7%
60	13%	16%	16%
90	15%	21%	22%

Table 1: Nodes compromised, by size of network.

Dissecting the coverage results into best and worst quadrants shows additional findings. In Fig. 4b we show the averages for the best and worst quadrants when $N = 250$ and $N = 1000$ (results for $N = 625$ are very close to $N = 1000$, and are omitted for clarity). The worst quadrant in the sparsely populated network, $N = 250$, barely has satisfactory performance at the start and quickly falls below the 70% threshold when the attack begins. The more redundant network, $N = 1000$, manages to last longer with its worst quadrant, but it still falls below the threshold long before the network as a whole does. Near total loss of an entire quadrant may be as unacceptable to a network defender as loss of the entire WSN. On the other hand, the performance of the best quadrant with $N = 250$ is actually better than $N = 1000$. Again, with how this attack spreads, the sparsity of nodes actually helps prevent the compromising of large percentages of the network.

These results show that merely adding additional nodes to WSN is not a good way of ensuring robustness; indeed, it may even hinder network performance during certain DoS attacks. It may be that two or more



(a) Average loss

(b) Best and worst quadrant loss

Figure 5: Coverage loss over time by distribution of sensor nodes, σ.

small, disjoint networks overlaid on the same environment may outperform a single large network. Not only could such an approach seek to increase the attack barrier for the adversary and mitigate a DoS attack, but using fewer total nodes might be cheaper for the network defender.

Next, we turn our attention to the distribution of the sensor nodes. The charts in Fig. 5 show our results for the different sensor distributions.

Unsurprisingly, the Gaussian distributions outperform a uniform distribution due to the extra redundancy in the key nodes surrounding the sink. As shown in Fig. 5a, $\sigma = 25$ has a 29% longer lifetime than does the uniform distribution. It also outperforms both the more dense and more uniform values of $\sigma = 20$ and $\sigma = 30$, respectively. This indicates that an optimal/near-optimal distribution lies somewhere within these bounds. Further simulations at finer granularity could more accurately determine this value.

Observing distribution by best and worst quadrant, Fig. 5b, also shows that the Gaussian distribution outperforms the uniform distribution. The advantage of the increased redundancy around the sink is clear when considering the best quadrant. The best quadrant shows longer lifetime and a less steep falloff than does the best quadrant for the uniform distribution. Looking at the worst quadrant shows approximately equivalent performance, with the the two distributions falling below the 70% threshold at step 63. In a similar manner to increasing the total number of nodes in the network, clustering them too tightly will allow this particular DoS attack to spread between more devices and cause greater damage.

By considering the results from our proposed model for this specific environment, we recommend a deployment strategy of $N = 1000$ and $\sigma = 25$. This combination provided the best performance according to our goal of maintaining overall network coverage of at least 70% as long as possible.

The results that we discuss in this case study very clearly indicate a non-trivial relationship between the number and distribution of devices to network performance during a DoS attack. The standard deviation of our results is relatively small, with a median of 12.3% of coverage, indicating that our results are statistically significant. Without some sort of analytic approach, a network defender risks incorrectly deploying WSN. Too few nodes or too dense of a distribution leaves large swaths of area uncovered from the beginning; too many sensors is expensive and can even be detrimental; too uniform of a distribution will lead to holes from attack or energy depletion surrounding the sink. Any of these mistakes lead to wasted resources and mission failure.

6 CONCLUSION

This paper examines the cyber decision problem of how to select an appropriate deployment strategy for a particular WSN with respect to robustness against DoS attacks. A novel agent-based model is built to analyze simulated network coverage during a DoS attack. The results from this model can be used to inform a deployment strategy: the number of sensor nodes and their distribution across the area of concern. A case study in performed using the model to demonstrate the viability of further developing this model into a full decision support system.

Future work is focused on developing a decision support system that is informed by the AB model. This system will seek to find the optimal/near-optimal deployment strategy for resisting DoS attacks. Additionally, we plan to analyze overlaying disjoint networks for greater robustness.

REFERENCES

Al-Karaki, J. N., and A. E. Kamal. 2004. "Routing techniques in wireless sensor networks: a survey". *IEEE Wireless Communications* vol. 11 (6), pp. 6–28.

Arora, A., R. Ramnath, E. Ertin, P. Sinha, S. Bapat, V. Naik, V. Kulathumani, H. Zhang, H. Cao, M. Sridharan et al. 2005. "Exscal: Elements of an extreme scale wireless sensor network". In *Embedded and Real-Time Computing Systems and Applications, 2005. Proceedings. 11th IEEE International Conference on*, pp. 102–108. IEEE.

Barrenetxea, G., F. Ingelrest, G. Schaefer, M. Vetterli, O. Couach, and M. Parlange. 2008. "Sensorscope: Out-of-the-box environmental monitoring". In *Information Processing in Sensor Networks, 2008. IPSN'08. International Conference on*, pp. 332–343. IEEE.

Borshchev, A., and A. Filippov. 2004. "From system dynamics and discrete event to practical agent based modeling: reasons, techniques, tools". In *Proceedings of the 22nd International Conference of the System Dynamics Society*, Volume 22. XJ Technologies.

Butun, I., S. D. Morgera, and R. Sankar. 2014. "A survey of intrusion detection systems in wireless sensor networks". *IEEE Communications Surveys & Tutorials* vol. 16 (1), pp. 266–282.

de Morais Cordeiro, C., and D. P. Agrawal. 2011. *Ad Hoc and Sensor Networks: Theory and Applications*. World Scientific.

Huang, C.-F., and Y.-C. Tseng. 2005. "The coverage problem in a wireless sensor network". *Mobile Networks and Applications* vol. 10 (4), pp. 519–528.

Islam, K., W. Shen, and X. Wang. 2012. "Wireless sensor network reliability and security in factory automation: A survey". *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* vol. 42 (6), pp. 1243–1256.

Karlof, C., and D. Wagner. 2003. "Secure routing in wireless sensor networks: Attacks and countermeasures". *Ad Hoc Networks* vol. 1 (2), pp. 293–315.

Krishnamachari, L., D. Estrin, and S. Wicker. 2002. "The impact of data aggregation in wireless sensor networks". In *Distributed Computing Systems Workshops, 2002. Proceedings. 22nd International Conference on*, pp. 575–578. IEEE.

Liu, B., and D. Towsley. 2004. "A study of the coverage of large-scale sensor networks". In *Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference on*, pp. 475–483. IEEE.

Memsic 2013. "TelosB Datasheet". Memsic.

Nasir, H. J. A., and K. R. Ku-Mahamud. 2016. "Wireless sensor network: A bibliographical survey". *Indian Journal of Science and Technology* vol. 9 (38).

Nelson, R., and L. Kleinrock. 1984. "The spatial capacity of a slotted ALOHA multihop packet radio network with capture". *IEEE Transactions on Communications* vol. 32 (6), pp. 684–694.

Oliveira, L. B., A. Ferreira, M. A. Vilaça, H. C. Wong, M. Bern, R. Dahab, and A. A. Loureiro. 2007. "SecLEACH—On the security of clustered sensor networks". *Signal Processing* vol. 87 (12), pp. 2882–2895.

Padmavathi, G., and D. Shanmugapriya. 2009. "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks". *CoRR* vol. abs/0909.0576.

Raymond, D. R., and S. F. Midkiff. 2008. "Denial-of-service in wireless sensor networks: Attacks and defenses". *IEEE Pervasive Computing* vol. 7 (1).

Sharma, U., and N. Bahl. 2017. "A Review on Security Issues and Attacks in Wireless Sensor Networks". *International Journal* vol. 8 (4).

Sharma, V., R. Patel, H. Bhaduria, and D. Prasad. 2015. "Policy for random aerial deployment in large scale wireless sensor networks". In *Computing, Communication & Automation (ICCCA), 2015 International Conference on*, pp. 367–373. IEEE.

Taniguchi, Y., T. Kitani, and K. Leibnitz. 2011. "A uniform airdrop deployment method for large-scale wireless sensor networks". *International Journal of Sensor Networks* vol. 9 (3-4), pp. 182–191.

Wagner, N., C. Ş. Şahin, M. Winterrose, J. Riordan, J. Pena, D. Hanson, and W. W. Streilein. 2016. "Towards automated cyber decision support: A case study on network segmentation for security". In *Computational Intelligence (SSCI), 2016 IEEE Symposium Series on*, pp. 1–10. IEEE.

Wang, D., B. Xie, and D. P. Agrawal. 2008. "Coverage and lifetime optimization of wireless sensor networks with gaussian distribution". *IEEE Transactions on Mobile Computing* vol. 7 (12), pp. 1444–1458.

Uri Wilensky 2017. "NetLogo". https://ccl.northwestern.edu/netlogo/. (Version 5.3.1).

Wood, A. D., and J. A. Stankovic. 2002, Oct. "Denial of service in sensor networks". *Computer* vol. 35 (10), pp. 54–62.

Zhang, Y., and W. Lee. 2000. "Intrusion Detection in Wireless Ad-hoc Networks". In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, MobiCom '00, pp. 275–283. New York, NY, USA, ACM.

AUTHOR BIOGRAPHIES

BRIAN C. YARBROUGH is a graduate student at Northeastern University and an Air Force Military Fellow at MIT Lincoln Laboratory. His research interests include cyber security and optimization. His email address is brian.c.yarbrough@gmail.com.

DR. NEAL WAGNER is a technical staff member in the Cyber Analytics and Decision Systems Group at MIT Lincoln Laboratory. His focus lies in developing problem-solving methods, tools, and techniques that combine artificial intelligence and modeling and simulation to create automated cyber decision-making systems. Prior to joining Lincoln Laboratory in 2013, he was at SolveIT Software, where he specialized in the commercialization of bio-inspired computing techniques for supply chain optimization of large organizations. His academic experience includes stints as a faculty member of the Computer Science and Information Systems Departments at Augusta University and Fayetteville State University. His email address is neal.wagner@ll.mit.edu.