# Using SANs to Model the Effect of DDoS Attacks in Simple AMI Networks

Zach Yordy
Dept. of Electrical and Computer Engineering
University of Illinois, Champaign, IL 61820

## I. Introduction

The advanced metering infrastructure (AMI) uses smart metering devices to gather and disseminate energy usage information throughout a network. While many different network configurations exist, the United States has widely adopted a common standard for deployment. AMI is largely based on a Radio Frequency Mesh network architecture, wireless metering devices, and the ANSI C12.22 application-level protocol suite in this region. Since a wireless AMI network (as well as the specification of the C12.22 protocol) is easily accessible to the public, it becomes vulnerable to various types of cyber-attacks [1]. In this project, I model an exploit of a vulnerability in the C12.22 protocol that causes DDoS-like behavior in AMI networks. I use a stochastic activity network (SAN) to model the consequence of varying network parameters on the effectiveness of such an attack. Earlier studies [2, 3] have demonstrated in simulation that these types of attacks can be extremely effective, although this project helps gain insight about what sort of network configuration might best mitigate such an attack.

## II. Problem Description

In this project, I aim to model the effects on a DDoS attack that exploits a vulnerability in the *trace service* of the ANSI C12.22 protocol. Although many different services are specified in the definition of this protocol, the trace service is used to find out which route a C12.22 message uses in order to get between two points in the network. In particular, a *trace request* is made. The node that initiates the trace request specifies its own address as well as the destination node to which it wants to know the route. As the trace request is passed along the network, each node appends its own Node ID to the payload of the message. Once the message reaches the destination, the message is simply returned to the requestor who can parse the message and find out the route it traversed.

This service is easily exploited to produce DDoS-like behavior. If a malicious node spoofs a victim node's ID as the sender, all trace request messages are returned to the victim. Furthermore, the message grows as it traverses the network. The attacker can send out very small trace requests that all return large amounts of the data to the victim. If the attacker uses even a reasonable fraction of its bandwidth to send out trace requests, the victim's bandwidth can be almost completely overwhelmed. Since the victim is not able to respond to most legitimate requests, a successful DDoS attack is performed.

In an RF mesh network, quite a large area of the network can be overwhelmed by such an attack, especially if the attacker chooses an important victim network node like an egress node.

## III. Model Description

Simulation allows for a very detailed model about the effectiveness of this DDoS-like attack on a particular network, but because the topology of the network and assumptions about capacity or bandwidth are included in a simulation, the results might not be as widely applicable as one might like. A simple analytical model has the advantage of revealing the true nature about such an attack. By modeling the attack against different network configurations, we can determine which parameters best mitigate the effects of this attack.

I decided to look at the effect of three different parameters on the effectiveness of this DDoS attack: buffer size, network size, and background traffic. Although I was not able to model a network quite as realistically as I might have liked, I believe I pushed this modeling technique to its limits to give unique insight that will still be valuable.

The SAN model used assumes an average message size of about 100 bytes, and a bandwidth of 250 bps for each node. Although these numbers are somewhat arbitrary, they are good averages for a low-power AMI mesh network. Furthermore, all outgoing links within the network are assumed to have equal probability. All results were modeled over a 15-minute period.

Since I was varying both buffer size and network size, I had to be careful about the numbers I chose at the top end of the spectrum. Both buffer size and network size directly affect the size of the SAN model involved. Although a realistic buffer might be between 5 and 10 messages (500 bytes to 1 Kb), I chose to look at buffer sizes between 1 and 5 for reasons that will hopefully soon be clear. I also decided to look at networks between 5 and 8 nodes. Although this might not seem to be much variance at first, this change actually does make quite a big difference. Finally, I chose to look at background traffic values between 5 and 20% of the total bandwidth available. On a network of 5 nodes where each node can either have a message in its buffer or not (buffer size of 1), the SAN model outputs a very nominal 32 states. However, when these numbers are extrapolated to a network of 8 nodes and a buffer size of 5, the associated markov chain quickly grows to an unmanageable 1,679,616 states ($6^8$). A background traffic value of 20% results in 4 times the amount of events as 5% in simulation, so the longest simulation ran for quite a while (almost 7 hours!).

The 5- and 8-node topologies are shown below, in figures 1 and 2, respectively.

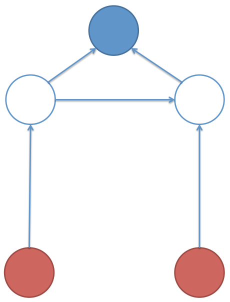


Fig. 1. 5-Node Topology

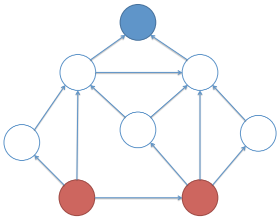


Fig. 2. 8-Node Toplogy

The transmission of each message was modeled by a Poisson process with rate 9,000 messages/hour, representing the available bandwidth.

$$\frac{250\text{ bytes}}{1\text{ second}} \times \frac{1\text{ message}}{100\text{ bytes}} = 2.5\text{ messages per second, or}$$

$$\frac{2.5\text{ messages}}{1\text{ second}} \times \frac{3600\text{ seconds}}{1\text{ hour}} = 9000\text{ messages per hour.}$$

By the same token, 5% background traffic was modeled by a Poisson process with rate 450 messages/hour, while 20% background traffic works out to 1800 messages/hour. Finally, the attackers were modeled as sending out packets at a much higher rate than legitimate nodes. Messages were generated by attackers at a rate of 90,000 per hour on average, but remember, the attacker could only use all of its available bandwidth to send messages. A generation rate of 90,000 messages per hour would only guarantee that there were usually messages ready to be sent.

A complete description for these models can be found in Appendix A, but the SANs for the two network configurations are shown in Figures 3 and 4, respectively.

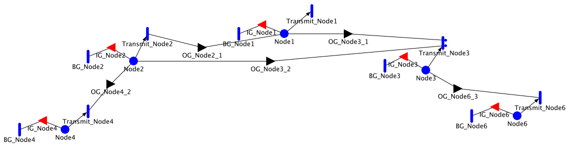


Fig. 3. 5-Node SAN Model

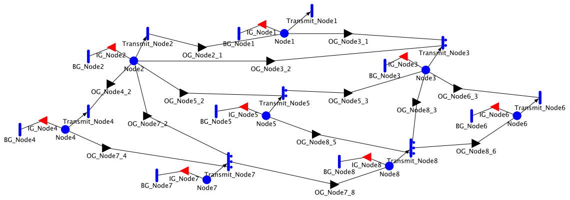
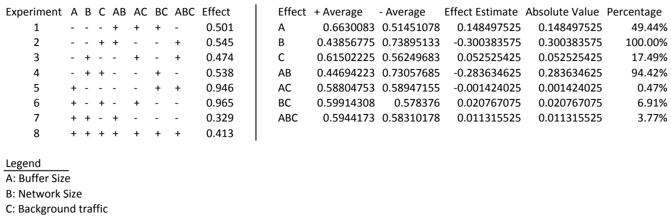


Fig. 4. 8-Node SAN Model

## IV. Results

The full outputs of the SAN modeling are attached in Appendix B. With these models, the following results were seen:



| Experiment | A | B | C | AB | AC | BC | ABC | Effect |
|---|---|---|---|---|---|---|---|---|
| 1 | - | - | - | + | + | + | - | 0.501 |
| 2 | - | - | + | + | - | - | + | 0.545 |
| 3 | - | + | - | - | + | - | + | 0.474 |
| 4 | - | + | + | - | - | + | - | 0.538 |
| 5 | + | - | - | - | - | + | + | 0.946 |
| 6 | + | - | + | - | + | - | - | 0.965 |
| 7 | + | + | - | + | - | - | - | 0.329 |
| 8 | + | + | + | + | + | + | + | 0.413 |

| Effect | + Average | - Average | Effect Estimate | Absolute Value | Percentage |
|---|---|---|---|---|---|
| A | 0.6630083 | 0.51451078 | 0.148497525 | 0.148497525 | 49.44% |
| B | 0.43856775 | 0.73895133 | -0.300383575 | 0.300383575 | 100.00% |
| C | 0.61502225 | 0.56249683 | 0.052525425 | 0.052525425 | 17.49% |
| AB | 0.44694223 | 0.73057685 | -0.283634625 | 0.283634625 | 94.42% |
| AC | 0.58804753 | 0.58947155 | -0.001424025 | 0.001424025 | 0.47% |
| BC | 0.59914308 | 0.578376 | 0.020767075 | 0.020767075 | 6.91% |
| ABC | 0.5944173 | 0.58310178 | 0.011315525 | 0.011315525 | 3.77% |

Legend
A: Buffer Size
B: Network Size
C: Background traffic

Fig. 5.

It is important to note that the *effect* above is the percentage of time the egress node spent with a completely full buffer (unable to accept new legitimate traffic). Again, the simulation was over a 15 minute period. This sign table helps us to determine which factors affect the attack the most. By separating the contribution of each factor into groups, we can more accurately determine the individual impact of each metric.

Somewhat unsurprisingly, the size of the network impacts the effectiveness of the attack the most. A larger network means that the egress node is overwhelmed a much smaller percentage of the time. This is because the other nodes of the network can more effectively mitigate the attack by the random spreading of messages throughout the network.

Secondly, varying buffer size and network size together seems to mitigate against an attack almost as well. With a big network and a big buffer, messages are again spread throughout the network rather than overwhelming a smaller group of nodes. A bigger buffer with each node means that each node (as well as the egress node) has a little bit more room for fluctuation.

Finally, buffer size alone also has a moderate impact on the effectiveness of the attack. A *smaller* buffer actually helps mitigate the attack somewhat well. Although this may seem counterintuitive at first, it actually makes quite a bit of sense. With a small buffer, messages are very readily dropped. This means that any attempt to overwhelm the network with messages is effectively cut off at the first node downstream, since it doesn't have the ability to hold on to a whole string of messages. The egress node isn't near as overwhelmed with congestion because each other node so readily drops messages. Although this may be an effective method to mitigate against such an attack, it is not recommended. A smaller buffer size means that the reliability of genuine message delivery will also be greatly affected.

Perhaps the most surprising result to be gleaned from the data lies in the techniques that aren't effective. A significant fluctuation in background traffic (a factor of four) has little bearing on how effective this attack is. While the attack is ever-so-slighty more effective with more background traffic, it doesn't make an appreciable difference. This is good from a design standpoint: the network only has to be designed to account for a reasonable amount of background traffic. Since the amount of background traffic isn't an important consideration in light of this attack, the network doesn't have to be designed to much higher specifications in order to get a really low level of background traffic. That simply isn't necessary.

## V. Conclusion and Future Work

In this project, I demonstrated the effects of a DDoS attack scenario on various parameters in an AMI network. I believe that understanding the behavior of the attack is essential to building a secure AMI system. Instead of simulating a model with assumptions about network topology and bandwidth, I opted to use a SAN model to help give some insight into the more general behavior of the attack. Finally, I indicated some ways in which the network infrastructure could be designed to best and most efficiently help mitigate against this attack.

## References

[1] S. Rana, H. Zhu, C. W. Lee, D. M. Nicol and I. Shin, *The Not-So-Smart Grid: Preliminary Work on Identifying Vulnerabilities In ANSI C12.22*, GC'12 Workshop, 2012.

[2] D. Jin, C. Lee, D. Nicol, I. Shin, and H. Zhu, *Simulation-based Study of Distributed Denial-of-Service Attacks in Advanced Metering Infrastructure*, INFORMS Annual Meeting, Charlotte, NC, USA, November 2011.

[3] D. Jin, Y. Zheng, H. Zhu, D. M. Nicol, and L. Winterrowd, *Virtual Time Integration of Emulation and Parallel Simulation*, Proceedings of the 26th Conference on Principles of Advanced and Distributed Simulation (PADS), Zhangjiajie, China, 2012.