A Mechanism for Detecting Gray Hole Attacks on Synchrophasor Data

Seemita Pal, Huijiang Li, Biplab Sikdar and Joe Chow
Department of Electrical, Computer and Systems Engineering
Rensselaer Polytechnic Institute, Troy, NY, 12180

Abstract—**The use of synchrophasor data for observation and control is expected to enhance the operation and efficiency of the next generation of power transmission systems. The synchrophasor measurement data is usually transferred over public domain networks such as the Internet, thereby making it susceptible to a number of attacks. This paper focuses on packet dropping or gray hole attacks on networks carrying synchrophasor data and develops a mechanism to detect such attacks. Our solutions is based on exploiting the patterns and correlation between packet delays and packet losses due to congestion in order to differentiate naturally occurring packet drops in the Internet from packet drops by gray hole attacks. The effectiveness of the proposed mechanism has been verified using simulations.**

I. Introduction

THE addition of synchrophasor measurements is expected to provide a number of important features in smart grids [1]. Phasor measurement unit (PMU) or synchrophasor data serves to facilitate a number of applications while enhancing others, such as real-time monitoring of the system, state estimation, disturbance monitoring, instability prediction, wide area protection and control, etc. [1], [2]. Given their importance in the maintenance and control of the power generation and distribution system, monitoring and manipulation of PMU data are particularly attractive avenues for malicious attackers that intend to disrupt and damage the power infrastructure [3]. Additionally, the synchrophasor measurement data is usually transferred over public domain networks such as the Internet, thereby making it susceptible to a number of attacks.

This paper addresses the problem of securing PMU data against packet dropping or gray hole attacks in the networks [4], [5]. In gray hole attacks, the adversary gains control of one or more routers in the network and then arbitrarily drops some or all packets that are forwarded through the compromised routers. The data measured and reported by the PMUs includes frequencies, phasors, analog values and digital values [6]. Synchrophasor measurements enable the direct measurement of the state of the power system. However, packet drops in the network on PMU data can easily lead to the loss of observability of the system and render useless a number of power system control and maintenance applications that rely on the timely and reliable delivery of PMU data. The focus of this paper is to develop an end-to-end strategy for detecting the presence of gray hole attacks.

Existing literature on the analysis and prevention of gray hole and other forms of packet dropping attacks has focused mainly on wireless ad hoc networks [4], [5], [7], and defending against them in wired networks remains an open problem. The solutions for detecting gray hole attacks in wireless networks are based on the inherent ability of nodes to overhear all transmissions in their neighborhood. However, such techniques are not applicable in wired networks which are used to carry PMU data. A proposal to detect malicious drops in wired networks is presented in [8]. The scheme proposed in [8] assumes that the routers in the network cooperate with the detection mechanism and provide real time data related to the queue lengths at their interfaces. In contrast, the methodology proposed in this paper does not require any network support. This is important since during an attack, the data provided by a compromised router cannot be trusted.

The main challenge in detecting a gray hole attack is to distinguish the malicious packet drops from the packet drops that occur due to congestion. In addition, it is desirable that the developed solution does not depend on any explicit feedback from the network elements. Finally, the overhead of the proposed solution should be low, both in terms of the processing requirements and the additional packets that it introduces in the network. To address these issues, we propose an end-host based mechanism for detecting gray hole attacks on PMU data. The proposed detector uses the observed values of the one-way network delay experienced by the packets carrying the PMU data, and does not introduce any overheads in terms of network traffic or support from routers in the network. By observing the trend in the one-way packet delays before and after a loss event, the proposed detection mechanism isolates losses due to congestion from the losses due to gray hole attacks. The proposed detection mechanism has been validated through extensive simulations in a number of settings.

The rest of this paper is organized as follow. In Section II, we present an overview of gray hole attacks and our system model. Section III presents our mechanism for detecting gray hole attacks on synchrophasor data. Section IV presents simulation results to validate the proposed detection mechanism. Finally, Section V concludes the paper.

II. Background and Assumptions

In this section, we first present a brief overview of gray hole attacks. Next, we present our system model and the assumptions on the attacker.

This work was supported primarily by the ERC Program of the National Science Foundation and the Department of Energy under NSF Award Number EEC-1041877 and the CURENT Industry Partnership Program.

A. Gray Hole Attacks

Gray hole attacks fall in the category of active attacks. During a gray hole attack, the attacker causes the drop of packets in the network. However, if all the packets at a router or link are dropped, the attack is easily detected [9]. In contrast to black hole attacks where all packets in the network or on a link are dropped, a gray hole attack drops only a subset of the packets and is thus more difficult to detect. In addition, the attacker may drop the packets arbitrarily or according to any distribution.

Detecting malicious packet drops is very challenging in wired networks because packets may be dropped naturally in the network due to congestion. In a multi-hop network with a large number of diverse, stochastic traffic sources, it is difficult to distinguish random packet drops caused by a gray hole attack from those caused by congestion. In addition, in a compromised network, neither senders nor receivers can trust the explicit feedback from the network about why and where packets are dropped. Because of the challenges in detecting and defending against packet drop attacks, attacks on routers and other network infrastructures leading to packet losses are one of the popular cyber attacks and are an important threat.

B. Network Model

We consider a network with an arbitrary topology and arbitrary number of flows. The path from a PMU to its receiving end point (typically a Phasor Data Concentrator (PDC)) may pass through a number of routers, some of which may have been compromised by an adversary. The data from the PMUs is periodic. Since the number of measurements during a given interval is constant, each PMU data packet is of the same length. Since many of the applications that use the PMU data do so in real time (for example, state estimation), we assume that the data is transferred using the User Datagram Protocol (UDP) as the transport layer protocol. The use of UDP is also motivated by the fact that unlike Transmission Control Protocol (TCP), UDP does not stop to recover lost packets or slow down its transmissions in response to congestion. If TCP were used for transferring the PMU data, in the event of a packet loss, the PDC would not receive any new data till the lost packet is recovered. For real time applications with strict deadlines on the data arrival time, such delays may be unacceptable.

In addition to the flows corresponding to the data packets being sent by the PMUs to the PDC, the network also carries other traffic flows. These flows may use either TCP or UDP as their transport layer protocol and may enter and leave the network at arbitrary times. The PMU flows share the bandwidth with a possibly different set of flows on each hop of its path and any congestion on any of these links affects all flows passing through these links. The bandwidth of each link and its propagation time may be different.

C. Threat Model

The threat model assumed in this paper is that the adversary has compromised one or more routers in the network that carries PMU traffic. At each of the compromised routers, the adversary is assumed to have the ability to arbitrarily drop the packets that pass through the router. In addition to dropping packets carrying PMU data, the adversary may also drop packets from other flows in order to make the attack harder to detect. The PMU data is assumed to be encrypted and the adversary does not alter the contents of the packets.

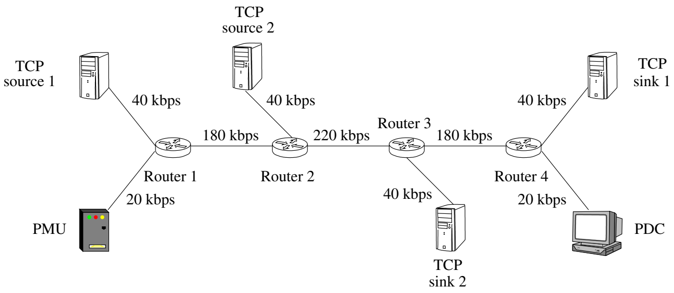


Fig. 1. Example Network Topology: one PMU flow and two TCP flows.

Under the adversary model described above, the paper considers the following gray hole attack: Given that a PMU data flow passes through a network with an arbitrary topology and traffic characteristics, the adversary compromises a set of routers in the network and arbitrarily drops packets that pass through these routers. To maximize the damage to these applications, the objective of the adversary is to drop the largest possible number of packets from the PMU flow without getting detected. Our objective is to develop a mechanism to detect packet drops due to gray hole attacks and the primary concern is to distinguish packets that are dropped due to congestion from the packets that are dropped by the adversary.

III. Mechanism for Detecting Gray Hole Attacks

In this section, we present our strategy to detect gray hole attacks. We first motivate our approach to developing the classifier and then present the details of the detection mechanism which is based on this classifier.

A. Correlation Between Congestion and Delay

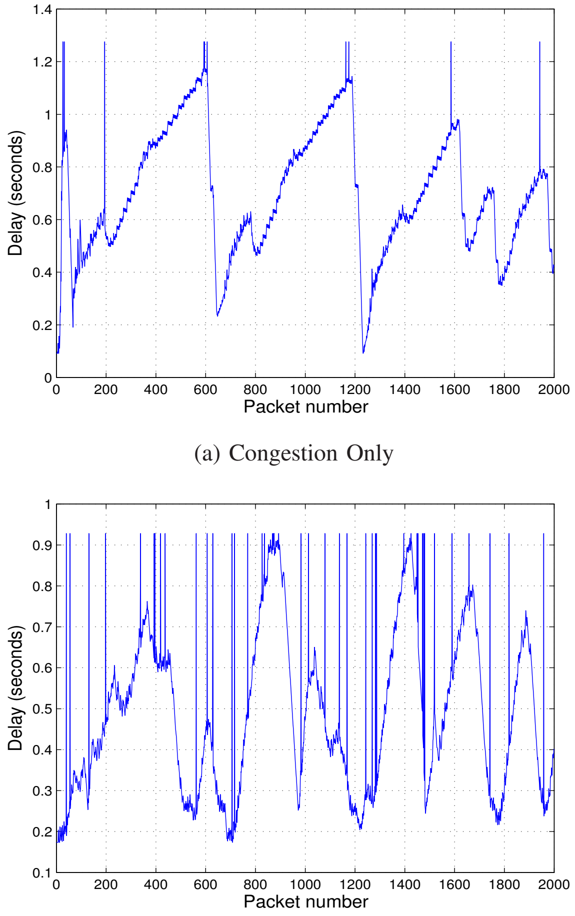
The main challenge in detecting a gray hole attack in a wired network is to differentiate between malicious packet losses and congestion related losses. Congestion related packet drops that occur in the Internet are caused by overflowing buffers at the routers. As the buffer occupancy of the routers increases during the onset of congestion, a corresponding increase in the queuing delay may also be observed. On the other hand, such correlations are unlikely to occur when an attacker maliciously drops randomly selected packets from the PMU data flow. This observation is the basis of the proposed mechanism for detecting gray hole attacks. Our strategy is to develop a technique that can filter out malicious packet drops based on passive observation of the stream of PMU data packets arriving at the flow's end point.

To illustrate the correlation between the congestion related packet drops and the delays in the network, consider the topology in Figure 1. In this example scenario, the network has one PMU flow that shares the network with two TCP flows. Figure 2 shows the PMU data packet delays and packet losses at the PDC end. In this figure, the vertical spikes represent packet drops. Figure 2(a) corresponds to the case where congestion is the only cause of packet losses (i.e., there is no gray hole attack). It is evident that packet drops occur only when the packet delays have increased to some point and after packet drops, the packet delays decrease sharply. This is because when the network is congested, TCP packets are also dropped. As a result, TCP clients trigger their congestion control mechanism, thereby reducing the length of the queues at the routers and thus the delays experienced by the packets. Figure 2(b) corresponds to a scenario where packets may be dropped by a gray hole attack, in addition to packet drops due to congestion and full queues. For these results, we assumed that the attacker has control of Router 1 and the gray hole attack randomly selects and drops packets arriving at the router with probability 0.01. In this figure, we see that there are some losses that fit the pattern in Figure 2(a). These losses were caused due to congestion. In addition, we also have losses that occur during a period where the delay continues increasing even after the packet loss. These packet drops were caused by the gray hole attack. From Figure 2, it is evident that there is a different relationship between the delays experienced by packets before and after a loss event, when one considers packets that are dropped by attackers and drops caused by congestion. The proposed gray hole attack detection mechanism exploits the presence of such correlations in the delays and cause of attacks in order to classify the cause of each packet drop.

B. Classification and Detection Mechanism

In order to develop a detection mechanism that can accurately detect the presence of an attacker dropping PMU data packets, we first need to classify the cause of a packet loss as either due to congestion or due to a gray hole attack. This classification is challenging due to the time-varying nature of Internet traffic and the reactive nature of protocols such as TCP in the presence of congestion. However, there are some salient features in the behavior of queues during congestion that may be passively monitored and used for inferring the cause of packet losses.

In general, congestion occurs in a link or a router when the rate of incoming packets exceeds the rate at which they can be handled. As a result, packets need to be buffered at the router and the delays experienced by the packets also increases. This increase in the queue lengths and packet delays continues till the buffer overflows, resulting in packet loss. TCP flows infer the onset of congestion in the network when it detects packet losses and react to congestion by reducing the rate at which they send packets into the network. The reduction in the TCP traffic in reaction to congestion now leads to a reduction in the traffic in the network. Consequently, the queue lengths at the routers decrease and a corresponding reduction in the packet delays are also observed. The duration for which the queue stays congested depends on a number of factors such as the number of flows, the round trip times of the flows etc..



(a) Congestion Only

(b) Congestion and Gray Hole Attack

Fig. 2. Packet delays and losses. Gray hole attack occurs at Router 1 and 1% data packets from all sources are dropped randomly.

Thus, an indication of a congestion loss is the presence of increasing delays immediately preceding the lost packet and decreasing delays shortly after the lost packet. On the other hand, if packet drops occur but the delays of previous packets did not show an increasing trend, or if packet drops occur continuously or closely while the delays in the packets before and after the drops keep increasing, it is unlikely that the losses were caused due to congestion. Therefore, to detect a gray hole attack packet drop, our approach is to monitor the packet delays in the network and track the gradient in the delays of packets before and after a drop.

We now apply the proposed methodology for distinguishing packet drops due to gray hole attacks from those due to congestion. The mechanism does not use any network support and is executed at the receiving end point of a PMU flow (typically a PDC). Each PMU data packet is timestamped by the source and we assume that the PDC uses the GPS assisted timing information to monitor the network latency of each arriving packet.

In general, the first or an isolated occurrence of a packet loss that is classified as an attack is not sufficient to declare the onset of an attack with a high level of confidence (due to

Algorithm 1 Gray Hole Attack Detection Algorithm

```
initialize $x_n = 0$
function CLASSIFY(i)
    if $slope_I(i) > \alpha$ AND $slope_I(i) - slope_F(i) > \beta$ then
        $cause = congestion$;
    else if $slope_I(i) < \alpha$ AND $slope_I(i) - slope_F(i) < \beta$ then
        $cause = attack$;
    else
        if $slope_F(i) < \gamma$ then
            $cause = congestion$;
        else
            $cause = attack$;
        end if
    end if
    if $cause == attack$ then
        ALERT()
    end if
end function

function ALERT()
    if $x_n = 0$ then
        start $timer$ for value $t$;
    end if
    update $x_n = x_n + 1$;
    if $timer$ has expired then
        if $x_n > \eta$ then
            generate alarm for “GRAY HOLE ATTACK”;
        end if
        $x_n = 0$;
    end if
end function

loop
    for each packet arrival $i$ do
        calculate delay $D_i$;
        consider $N$ previous arrivals;
        update $slope_I(i) = (D_i - D_{i-N})/N$;
        if out-of-sequence packet then
            {/* packet loss detected */}
            wait for $M$ new arrivals;
            update: $slope_F(i) = (D_{i+M} - D_i)/M$;
            CLASSIFY(i)
        end if
    end for
end loop when session is terminated
```

non-zero false positive rates of the classifier). Thus the attack detection mechanism relies on testing whether the number of dropped PMU packets classified as attack drops over a given interval of time exceeds a particular threshold. If this threshold is exceeded, only then a gray hole attack alarm is generated.

The proposed gray hole attack detection algorithm is shown in Algorithm 1. The proposed detection mechanism first quantifies the trends in the delays before and after a loss by calculating the *slope* of the delay over a given window. Let N and M denote the window sizes for calculating the slopes before and after the loss. The slopes before ($slope_I$) and after ($slope_F$) the loss are then defined as

$$slope_I = \frac{D_i - D_{i-N}}{N} \tag{1}$$

$$slope_F = \frac{D_{i+M} - D_i}{M}. \tag{2}$$

For each new packet arrival, the algorithm calculates the slope of the delay values associated with the previous N values. In case a packet loss is detected (i.e. an out of sequence packet is received), the algorithm calculates $slope_I$ and waits for the next M packets to arrive and uses the delay values associated with these packets to calculate the trend in the delays ($slope_F$) after the loss. Based on the calculated value of $slope_I$ and the difference $slope_I - slope_F$, the classifier considers three cases.

In a normal network scenario without an attacker, the onset of congestion is accompanied by an increase in the delays experienced by packets. Thus in the event of a loss, a positive $slope_I$ indicates that the delay seen by the packets was increasing. The measured value of $slope_I$ may be compared against a threshold (α) to confirm with some confidence that the loss was due to congestion. When TCP flows lose packets, they react by slowing down the rate at which they send packets into the network. Consequently, the delays seen by the subsequent packets start to decrease and the value of $slope_F$ becomes lower than $slope_I$ and thus the difference in the slopes $slope_I - slope_F$ becomes positive. The value of the difference of the two slopes may be compared against a threshold (β) to get an indication that the delays after the loss are lower than the delays before the loss and thus the loss was due to congestion. Thus $slope_I$ and the difference between the two slopes $slope_I - slope_F$ may be used as reliable features when classifying a loss event as a drop due to either congestion or attack.

When both $slope_I$ and the difference in the slopes consistently indicate congestion or attack the classification may be done without the need for any additional information. However, when $slope_I$ indicates congestion but the difference in the slopes does not, or vice-versa, then additional information is required for accurately classifying the cause of the loss. In these cases, the algorithm also looks at the value of $slope_F$ for additional information. Since the delay decreases after a drop due to congestion, a value of $slope_F$ lower than a certain threshold (γ) indicates that the loss was due to congestion.

Based on the values of $slope_I$ and the difference in the slopes, we thus have have the following cases:

1) If $slope_I > \alpha$ AND $slope_I - slope_F > \beta$ then the cause of the packet loss is marked as congestion.
2) If $slope_I < \alpha$ AND $slope_I - slope_F < \beta$ then the cause of packet loss is marked as attack.
3) If $slope_I > \alpha$ AND $slope_I - slope_F < \beta$ or $slope_I < \alpha$ AND $slope_I - slope_F > \beta$ then the algorithm considers the value of $slope_F$ for further information. If $slope_F <$

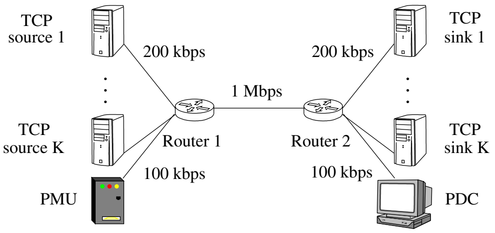


Fig. 3. Network topology with a single bottleneck: one PMU flow and multiple TCP flows.

γ then the decrease in delay after the drop matches with congestion cases and the packet loss is classified as a drop due to congestion. Otherwise, it is classified as an attack.

Thus, based on the computed values of the slopes we classify the cause of each of the lost PMU packets as congestion or attack. On the observation of the first packet classified as attack, the system goes in the *alert mode*. In this alert mode, the system counts the total number of packet drops that are classified as attack drops for the next t minutes. Towards this end, a timer of t minutes is first started and the number of lost packets that are classified as packet drops due to attack in the next t minutes, denoted by x_n, is then counted. An alarm signifying the presence of a gray hole attack is generated if $x_n > \eta$, where η is the alarm threshold. If the threshold is not exceeded when the timer expires, then the classifier resets x_n, keeps monitoring packet drops, and repeats the entire process on observation of packet drop classified as due to an attack.

IV. Simulation Results

In this section, we present simulation results to evaluate the effectiveness of the proposed gray hole attack detection mechanism. The simulations were conducted using the Network Simulator 2 (NS2) simulation tool. For our results, we consider two topologies: a dumbbell network topology and a mutihop network topology. For both of the topologies we vary the number of flows in the network to create different levels of congestion. In addition, we consider attacks of different intensities where the adversary drops a different fraction of the packets that traverse the compromised router. Each simulation scenario consists of one PMU flow and a number of TCP flows. The PMU flow uses UDP as the transport layer protocol and generates 20 packets per second and each packet is of 100 bytes. The length of each simulation run was kept at 1000 seconds and each reported result is for the average of 10 different runs for the same scenario. In these simulations, we assume that the adversary drops packets from the PMU as well as the TCP flows in order to make the detection of the attack more difficult. The simulations used $M = 7$, $N = 7$, $\alpha = 0.0008$, $\beta = 0.0033$, and $\gamma = -0.0003$ for the detection algorithm and these values were determined empirically.

For each topology, we evaluate the performance of the proposed classification mechanism in terms of its accuracy, false positive rates, and false negative rates. The false positive rate is the probability that a packet drop is categorized as a gray hole attack drop when the real cause of the drop is congestion. The false negative rate is the probability that the cause of a packet drop is categorized as congestion in the network when the actual cause is the gray hole attack. In addition, we also evaluate the accuracy of the proposed detection scheme. The accuracy of the system is defined as the fraction of packet losses whose cause is correctly classified.

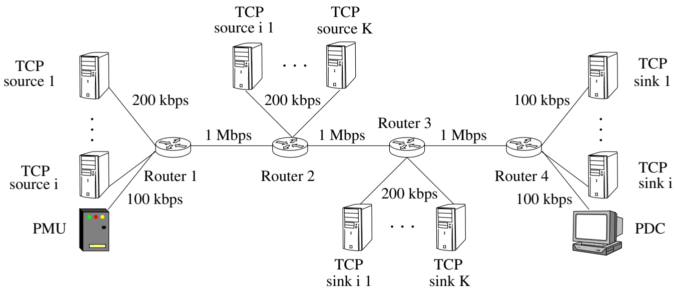


Fig. 4. Network topology with multiple bottlenecks: one PMU flow and multiple TCP flows.

For the first set of simulations, we consider the topology shown in Figure 3 where there is a single bottleneck link. In this topology, we assume that Router 1 is compromised. For this topology, we varied the number of TCP flows (K in the figure) from 4 to 10 to simulate networks with different levels of congestion. Furthermore, gray hole attacks of different intensities were simulated by using attacker drop rates of 0.005, 0.0075, 0.01, 0.015 and 0.02, and also the scenario when there is no attacker (i.e. an attacker drop rate of 0). The attack detection results for the 10 TCP case under various attack intensities and different values of the alarm clustering timer t are shown in Table I. The propagation time of all links in the network was 10ms and each router had a buffer capacity of 60Kbits. It is evident that the accuracy of the proposed mechanism is high for all scenarios. We obtain similar results for the cases where the congestion level is varied by increasing or decreasing the number of connected TCP sources and these results are not shown to avoid repetitive results.

The second simulated network corresponds to a network with multiple bottlenecks and is shown in Figure 4. In this topology it is assumed that Router 2 is compromised and the attacker drops packets from all the flows that pass through it. The propagation time of all links in the network was 10ms, and each router had a buffer capacity of 60 Kbits. As in the single bottleneck case, we consider scenarios with different levels of congestion by choosing the total number of TCP flows in the network (K in the figure) as 4, 6, 8, 10 and 12, and the corresponding number of long TCP flows (i in the figure) were 3, 4, 5, 6 and 7, respectively. In addition, we simulated different intensities of of gray hole attacks by simulating attacker drop rates of 0.005, 0.0075, 0.01, 0.015 and 0.02, and also the scenario when there is no attacker.

For the multihop topology, Table II presents the results of the detector for the case of 10 TCP flows in the network, for different values of the alarm clustering timer t. For all cases, we observe that the proposed classification scheme can

TABLE I
ACCURACY, FALSE POSITIVE AND FALSE NEGATIVE PERCENTAGES OF GRAY HOLE ATTACK DETECTION IN A NETWORK WITH SINGLE BOTTLENECK AND 10 TCP FLOWS FOR DIFFERENT PACKET DROP RATES AND DETECTION DELAYS. A: ACCURACY, FP: FALSE POSITIVE, FN: FALSE NEGATIVE

	2 mins ($\eta = 6$)			3 mins ($\eta = 9$)			4 mins ($\eta = 12$)			5 mins ($\eta = 15$)		
Drop rate	A	FP	FN	A	FP	FN	A	FP	FN	A	FP	FN
0.00	100	0	0	100	0	10	100	0	0	100	0	0
0.005	95	0	10	95	0	10	100	0	0	100	0	0
0.0075	100	0	0	100	0	0	100	0	0	100	0	0
0.01	100	0	0	100	0	0	100	0	0	100	0	0
0.015	100	0	0	100	0	0	100	0	0	100	0	0
0.02	100	0	0	100	0	0	100	0	0	100	0	0

TABLE II
ACCURACY, FALSE POSITIVE AND FALSE NEGATIVE PERCENTAGES OF GRAY HOLE ATTACK DETECTION IN A NETWORK WITH MULTIPLE BOTTLENECK AND 10 TCP FLOWS FOR DIFFERENT PACKET DROP RATES AND DETECTION DELAYS. A: ACCURACY, FP: FALSE POSITIVE, FN: FALSE NEGATIVE

	2 mins ($\eta = 6$)			3 mins ($\eta = 9$)			4 mins ($\eta = 12$)			5 mins ($\eta = 15$)		
Drop rate	A	FP	FN	A	FP	FN	A	FP	FN	A	FP	FN
0.00	100	0	0	100	0	10	100	0	0	100	0	0
0.005	95	0	10	95	0	10	100	0	0	100	0	0
0.0075	100	0	0	100	0	0	100	0	0	100	0	0
0.01	100	0	0	100	0	0	100	0	0	100	0	0
0.015	100	0	0	100	0	0	100	0	0	100	0	0
0.02	100	0	0	100	0	0	100	0	0	100	0	0

TABLE III
OVERALL DETECTION RESULTS IN SINGLE AND MULTIPLE BOTTLENECK NETWORKS FOR DIFFERENT DETECTION DELAYS. A: ACCURACY, FP: FALSE POSITIVE, FN: FALSE NEGATIVE

Detection	Single Bottleneck			Multiple Bottlenecks		
delay (mins)	A	FP	FN	A	FP	FN
2 ($\eta = 6$)	98.33	2	1.6	99.27	0	0.89
3 ($\eta = 9$)	99	2	0.8	99.64	0	0.44
4 ($\eta = 12$)	99.33	0	0.8	99.64	2	0
5 ($\eta = 15$)	99.67	0	0.4	100	0	0

classify, with a high level of accuracy, the cause of any packet drop in a network. The attack detection scheme based on this classification mechanism thus yields very accurate results. It is seen that as we increase the time window of the detection mechanism, i.e. the detection delay, we get better results. Similar results were obtained for the scenarios with other numbers of TCP flows and these results have been omitted.

The overall results of the detector for all the different TCP cases and attack intensities for the dumbbell topology and the multihop topology are presented in Table III. These results correspond to the averaged results for all the choices of K (the number of TCP flows) and the attacker drop rates. It is seen that the accuracy is 100 percent when the detection delay is 5 mins. For lower detection delay cases, the accuracies are still greater than 99 percent.

V. CONCLUSIONS

This paper presents an mechanism to detect packet dropping or gray hole attacks in networks carrying synchrophasor data. The proposed methodology is based on exploiting the correlation between packet delays and packet losses due to congestion. The proposed methodology is based on passive observations of the one way network delay experienced by the packets and can be implemented without any additional overhead or support from the network. Simulation results are presented to verify the performance of the proposed algorithm.

REFERENCES

[1] S. Horowitz, A. Phadke and B. Renz, "The Future of Power Transmission," *IEEE Power and Energy Magazine,* vol.8, no.2, pp.34-40, March-April 2010.

[2] R. Burnett, M. Butts and P. Sterlina, "Power system applications for phasor measurement units," *IEEE Computer Applications in Power,* vol. 7, no. 1, pp. 8-13, January 1994.

[3] H. Khurana, M. Hadley, N. Lu and D. Frincke, "Smart-Grid Security Issues," *IEEE Security and Privacy,* vol. 8, no. 1, pp. 81-85, January-February 2010.

[4] D. Djenouri, L. Khelladi and A. Badache, "A survey of security issues in mobile ad hoc and sensor networks, *IEEE Communications Surveys and Tutorials,* vol. 7, no. 4, pp. 2-28, 2005.

[5] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks, *IEEE Wireless Communications,* vol. 14, no. 5, pp. 85-91, October 2007.

[6] A. Armenia and J. Chow, "A Flexible Phasor Data Concentrator Design Leveraging Existing Software Technologies," *IEEE Transactions on Smart Grid,* vol. 1, no. 1, pp. 73-81, June 2010.

[7] J. Cai, P. Yi, J. Chen, Z. Wang and N. Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network," *Proc. of IEEE AINA,* pp. 775-780, Perth, Australia, April 2010.

[8] A. Mizrak, S. Savage and K. Marzullo, "Detecting Malicious Packet Losses," *IEEE Transactions on Parallel and Distributed Systems,* vol. 20, no. 2, pp. 191-206, February 2009.

[9] X. Zhang, S. F Wu, Z. Fu, and T-L Wu, " Malicious Packet Dropping: How It Might Impact the TCP Performance and How We Can Detect It,"*Proc. of ICNP,* pp. 263-272, November 2000.