A Cyber-Insurance Scheme for Water Distribution Systems Considering Malicious Cyberattacks

Yunfan Zhang, Lingfeng Wang, *Senior Member, IEEE,* Zhaoxi Liu, *Member, IEEE*, and Wei Wei

***Abstract*— As one of the national critical infrastructures, the water distribution system supports our daily life and economic growth, the failure of which may lead to catastrophic results. Besides the uncertainty from the system component failures, cyberattacks are vital to the secure system operation and have great impacts on the reliability of the water supply service. Malicious attackers may intrude into the supervisory control and data acquisition (SCADA) system of pump stations in the water distribution networks and interrupt the water supply to the customers. Cyber insurance is emerging as a promising financial tool in system risk management. In this paper, cyber insurance is proposed for the cyber risk management of the water distribution system. A semi-Markov process (SMP) model is devised to model the cyberattacks against pump stations in the water distribution system. Both the impacts of the independent cyber risks in the individual distribution network and the correlated cyber risks shared across different water distribution networks are evaluated and modeled. A sequential Monte Carlo Simulation (MCS) based algorithm is developed to evaluate the system loss. Cyber insurance premiums for the water distribution networks are designed based on the actuarial principles and potential system losses. Case studies are also performed on multiple representative water distribution networks, and the results demonstrate the validity of the proposed cyber insurance model.**

***Index Terms*—Cybersecurity, cyber insurance, premiums, water distribution system, reliability evaluation.**

I. Introduction

Widespread applications of the information and communication technology (ICT) introduce higher risks on cybersecurity in modern cyber-physical systems. The real-time monitoring and communication systems are commonly used in the regular operation of water systems. The systems control and data acquisition (SCADA) systems in the water systems are extensively applied to control the automated physical processes which are essential to the drinking water treatment and water distribution systems. It has become a standard for the operation of medium to large scale drinking water systems and even some small water utilities. With the improvement of operational efficiency, the vulnerabilities of the water system to malicious cyberattacks are increasing at the same time. A successful cyberattack on the water network can lead to very serious damage on both the supply side and demand side. Consequently, the SCADA system in the water distribution network has become the primary target of several cyberattacks in the past two decades [1][2]. According to the Water Sector Cybersecurity Brief for States [3] given by the U.S. Environmental Protection Agency (EPA), successful cyberattacks on the controls systems like the SCADA system in the water network have significant impacts on the system performance, such as upsetting the treatment and conveyance processes by opening and closing valves, overriding alarms and disabling pumps or other equipment, deface the utility's website, compromise the email system, install malicious programs like ransomware to disable the process control operations, etc. The cyberattacks to the critical infrastructures are becoming more serious in recent years and cybersecurity threats continue to grow across the water utilities. A recent example of cyberattack against the water sector is the City of Atlanta ransomware attack in 2018. The Atlanta Department of Watershed Management could not turn on the working computers for normal operation within one week, and Atlanta had to completely close its official water department website for two weeks after the cyberattack. This cyberattack takes several months to address and the approximate cost is up to 5 million dollars [4]. In 2016, the system of Lansing Board of Water & Light (BWL) was totally locked by the unidentified foreign hacker. The attacker demanded a $25,000 ransom to unlock the system. In addition, BWL had to pay the cyber forensics fee, clean and test hundreds of computers and replace the infected servers, which incurred the total cost to around $2.4 million dollars [5]. Another example of cybersecurity threats to the water utilities is that an American water authority was hacked between November 2016 and January 2017. According to the intelligence briefing on this cyberattack published by the Department of Homeland Security (DHS), after successfully intruding into the system, the cyberhackers took control of all the cellular routers in the water utility and stole valuable internet service for other uses, which cost the utility $45,000 in December and $53,000 in January respectively. Fortunately, the cyber intrusions did not damage the utility infrastructure and lead to any loss of the water service. Or else, more severe damage and system losses could have been caused by the cyberattacks.

Cybersecurity is considered as one of the most critical factors that has a great impact on the reliable performance of the critical systems. Cyber attackers may compromise the major function of the water distribution networks in delivering clean water, pollute the environment, and eventually lead to financial and legal liabilities for the water utilities. The Executive order 13636 Improving Critical Infrastructure Cybersecurity issued in 2013 [6] pointed out the urgent need of a framework to provide a cost-effective approach to help the critical infrastructure owners and operators to reduce the overall cyber risks while maintaining the reliable system performance. Cyberattacks can bring potential threats to the water systems. Some existing studies on cybersecurity characterization have mostly

This work was supported by US National Science Foundation (NSF) under award ECCS1739485.

Y. Zhang, L. Wang, and Z. Liu are with Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA.

W. Wei. is with Department of Mathematical Sciences, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA.

considered the cybersecurity from a qualitative perspective. So far, very few studies have considered the quantitative assessment of cybersecurity. Therefore, it is of great importance to evaluate the impacts of the cyberattacks on the water distribution network in a quantitative manner. From the systems analysis perspective, there are some similarities between the failures caused by accidental faults such as system components failures or human errors and the failures due to cyberattacks. Therefore, we can fully utilize the proposed model and available research in the literature about reliability analysis of critical infrastructures to develop cybersecurity quantification analysis.

Reliable water supply is of critical importance to support the economic development and human life. Based on the predictions from report of [7] and [8], water supply will become one of the most serious national problems by 2025. With the increasing risks of substantial economic losses due to cyberattacks, additional tools to manage the cybersecurity risks are strongly urged. An integrated risk evaluation of the water system incorporating the impact of cyberattacks is very meaningful in enabling more informed decision making. One efficient way is to adopt the recently developed cyber insurance policies, which are the policies that provide coverage against the overall system losses from network related issues in cybersecurity. From the business perspective of cybersecurity, the visions of cyber-insurance as a risk management tool were formulated. Some existing studies have considered the cyber insurance as an effective tool for cyber risk management [9, 10, 11]. The authors of [12] demonstrated the insurability of cyber risks. By analyzing the statistical properties of hundreds of cyber losses cases, it is proved that the cyber risks can be insured but a sustainable cyber insurance market is needed. A framework by considering the possible operating principles of insurance companies to quantitatively assess the overall cyber risks on critical infrastructures is developed in [13]. By applying the proposed approach, the optimal levels of investment for both cybersecurity and insurance can be formulated to minimize the cyber risks. The authors of [14] analyzed the risk management strategies of companies when the risks are interdependent. The study shows how the interdependence of cyber risks reflects on the incentives to invest in security technologies and to buy insurance coverage. A new classification of correlation properties of cyber-risks based on a twin-tier approach was proposed in [15]. The study shows how the two-step risk arrival process for cyber risks can be incorporated in an economic model. A framework used to model the cyber insurance considering the information asymmetry between insurer and insured, the interdependent and correlated nature of cyber risks is studied in [16]. In [17], a new optimal insurance model is developed based on the traditional cyber-insurance model to assess the case where both the insurable and non-insurable risks exist. The studies in [18] indicate how the competitive cyber-insurers would impact the overall network security and the welfare of the networked society.

Some recent efforts have been made toward developing effective detection mechanisms against cyber-attacks launched on an operational water treatment plant in real-time [19], [20]. Various approaches have been proposed to study the cyber-physical system security problem and summarized in [21]. For different cyber-physical systems, the physical configuration of the system is varying, but they do share some similar potential risks from the cybersecurity perspective. In [22], a framework is proposed to formulate how the cyber-physical attacks on water distribution network would affect the system hydraulic performance. A *MATLAB* toolbox named *epanet*CPA [23] was developed to help the researchers formulate different attack scenarios on the water system. The authors also pointed out that the system components in a water network such as sensors, PLC, and SCADA system are vulnerable to cyberattacks. In 2019, the authors of [24] improved the *epanet*CPA toolbox by extending the capabilities of conducting pressure-driven simulations of the cyber-physical attacks on water distribution systems. The authors of [25] introduced a new cyber-physical stress testing platform named *RISKNOUGHT*, which allows users to simulate the water distribution systems as cyber-physical systems. However, cyber insurance was rarely linked to the quantitative risk analysis of cybersecurity on water distribution system in the existing literature.

The scope of this paper focuses on developing a quantitative risk management framework to incorporate cyber insurance for water distribution system owners and operators to manage the cyber risks. The major contributions of this paper are summarized as follows:

- A modified semi-Markov process (SMP) model incorporating a stochastic cyber risk correlation model is proposed to evaluate the potential cybersecurity threats against the SCADA system in the water distribution network. Based on the proposed model, both the independent cyber risk within the individual water network and the correlated common cyber risks shared across different water networks can be considered and evaluated.
- A Monte Carlo simulation (MCS) based quantitative risk assessment approach is developed to estimate the impact of malicious cyberattacks on water distribution system reliability.
- A cyber-insurance framework including several actuarial insurance principles is built to manage the risks of water distribution systems considering the financial consequences of cybersecurity risks.

The remainder of this paper is organized as follows. In Section II, an overview of the system reliability assessment is presented. In Section III, the reliability model of the water distribution system considering cyberattacks is described. In Section IV, how the cyber insurance premiums are calculated based on the actuarial principles is introduced. In Section V, case studies are performed to illustrate the effectiveness of the proposed model. Section VI draws the conclusion of the paper.

II. Cyber-insurance for system Risk management

Various probabilistic reliability evaluation algorithms have been developed [26] and applied to critical infrastructures [27]. When performing system-level reliability evaluation, a wide spectrum of factors may lead to a system failure. In most traditional reliability evaluation algorithms, only the physical N-1 or N-k contingencies of system components is considered. The physical component failures could be triggered and consequently lead to an overall system failure. However, for modern critical infrastructures, more factors or uncertainties such as cyberattacks should be taken into consideration when designing effective protection mechanisms to ensure reliable performance of the systems. Due to the wide deployment of ICT in the system operations of the critical infrastructure sectors, cybersecurity threats may have more significant impacts on the system performance than physical failures. Cyberattacks against the water system can not only affect the system individually but also interact with the physical failures to lead to more complex failures. More severe system faults in the related physical and cyber failures could be caused. Cyberattacks and physical failures may happen simultaneously to trigger more significant impacts on the overall system. This kind of combinational

failures could directly result in the interruption of water services. Therefore, in this paper the impact due to cybersecurity threats against the water distribution system is considered in performing the reliability assessment.

When a successful cyber intrusion is performed on the control network of the system, the physical infrastructure could be directly affected [28]. For example, when certain critical components in the water supply network (e.g., pumps) are disabled by a cyberattack on the control system, the high interdependency between the cyber and physical portions of the modern water network could result in higher risks of system performance degradation or entire failure. Failures in the cyber infrastructure (e.g., the wrong control signals or false system information) could mislead the system operator to make uninformed decisions which may result in system failures. Abnormal operations of the physical components due to cyberattacks may increase the stress of the system operator as well, so that human errors are more likely to happen in such cases.

According to existing studies [7, 8], it is predicted that the water supply will become a national problem within 5 to 6 years. Thus, it is of great importance to ensure a reliable and secure water distribution system in the presence of various uncertainties including the cybersecurity threats. Cyberattacks have become an increasingly severe threat so that cyber insurance policies are recently being developed in some industry sectors to cover the potential losses from a variety of cyber incidents, including data breaches, business interruption, network damage, etc. Cyber insurance policies can also provide incentives for security investments that reduce cyber risks [29]. In [30], the authors have traced the evolution of cyber-insurance from the traditional insurance policies to the early stage of the cyber-risk insurance policies. The authors of [31] summarized the available background knowledge about cyber insurance in the literature from both market and scientific perspectives, and then pointed out a series of possible directions for future studies on cyber insurance. The DHS National Protection and Programs Directorate (NPPD) has also become aware of the cyber insurance in its role in helping manage potential cybersecurity threats to the critical infrastructures [32]. However, through the findings from NPPD, it shows that the first-party cybersecurity insurance market is still nascent, particularly when it comes to coverage for cyber-related critical infrastructure loss. This is mainly due to the lack of actuarial data; aggregation concerns; and the unknowable nature of all potential cyber threat vectors. The authors of [33] pointed out the insurance market should incentivize the vendors to strengthen the security level of their products. Reference [34] shared the insight that a balanced mix of perspectives on threats, organizational approaches, and protective measures is essential to protect the critical infrastructures from potential cybersecurity threats.

Due to the increasing deployment of information and communication technologies (ICTs), the water system infrastructure is exposed to more potential cyberthreats than before. The attackers may gain access to the critical monitoring and control systems through cyber intrusions. Then they may directly send fabricated operation commands to the critical system components. These behaviors may eventually impact the overall performance and reliability of the water distribution system. The development of cyber insurance, with its strong reliance on risk metrics, can be an efficient tool for promoting the development of cyber risk guidelines and better manage the increasing cyber risks. This paper aims to model and analyze the impact of cyberattacks on the water distribution systems quantitatively and develop suitable cyber insurance premiums based on insured's level of reliability and self-protection.

III. Reliability Model of Water Distribution System Considering Cyberattacks

Modern water distribution systems are highly dependent on the information systems to ensure their performance and functions. The Supervisory control and data acquisition (SCADA) system can largely help the water utility operators to monitor and control the distribution process that may be distributed across several remote sites. However, the SCADA systems in the water distribution network are vulnerable to potential cyberattacks. A successful cyberattack on the water distribution system can lead to severe consequences. The most direct consequence is the system failures that may result in immediate loss of water service. The overall loss of a water distribution system can be evaluated and quantified by the amount of the loss of water service and the duration of the fault event in the system from the reliability perspective. In order to take the potential cybersecurity threats into consideration, both the independent and correlated cyber risks are modeled in this section. And a high-fidelity hydraulic flow-based reliability evaluation procedure is proposed to quantify the overall system loss of the water network under malicious cyberattacks.

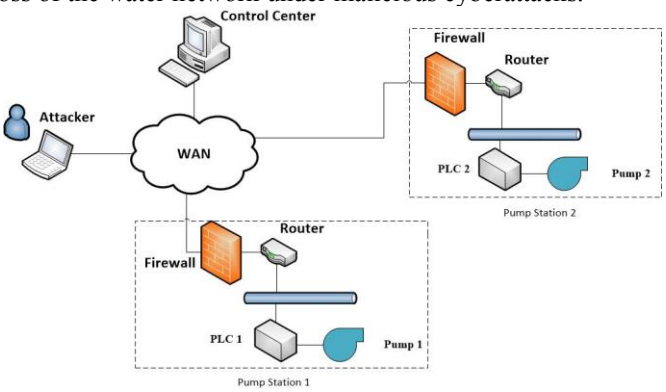

Fig. 1. An Example of SCADA Architecture in Water Distribution System

Fig. 1 illustrates an example of the cyber structure of SCADA system in the water distribution network, which is used to control and monitor the distribution of the water. The control center and the geographically distributed pump stations are connected through a complex wide area network (WAN). The operators in the control center monitor the statuses of the field devices and send out operation commands. From the intruder's perspective, he/she may launch cyberattacks on either the control center or the distributed pump stations in the network. Once the attacker successfully intrudes into the control network, various malicious actions can be possibly done, such as shutting down pumps, sending out false operation commands, and interrupting the information systems. All these malicious actions will possibly result in serious system failures.

A. Cyberattack Model

The SCADA systems are among the primary targets of potential cyberattacks on the critical infrastructures. Even if a high-level defense strategy is deployed, it is still possible for the attacker to intrude into the SCADA system if some critical vulnerabilities of the system are exploited, and significant losses would be caused by the attack. In this study, a successful cyber intrusion means the attacker gains the control of pump stations in the water distribution network, which will consequently lead to the undesired loss of water service. The Lockheed Martin researchers have applied the concept of kill chain to define the

Cyber Kill Chain (CKC) in [2]. The CKC models the life cycle of an intrusion process with several steps. The CKC model focuses on the analysis from the attacker's perspective, as the attackers need a series of malicious activities to compromise the final target, and the attackers will adjust each step based on the success or failure of the previous step. On the contrary, the SMP model [35] is utilized in this paper to formulate the process of cyberattacks on the water system, which focuses on the interactions between the cyberattack and the defense of the system, and captures the stochastic characteristics of the cybersecurity performance of the system under the attacks. With the implementation of more advanced intrusion tolerance techniques, the SCADA system in critical infrastructures is more resilient to cyberattacks. The SMP model can sufficiently formulate the dynamics between the cyberattack and the response of the system, especially when the SCADA system has gained some degree of intrusion tolerant capability. Define SMP $X = \{X(t);\ t \geq 0\}$ consisting of a stochastic process with discrete state space S. The transition rate in the process is only relevant to the current state, and the state transitions are determined by the transition probability matrix. After identifying the absorbing states in the SMP model, the mean sojourn time of the transient states can be measured and the mean time to compromise can be further estimated.

In this study, two types of attack scenarios are considered that may occur in the SCADA system of the water distribution network: normal attack and penetration attack [36]. For the normal attack scenario, the intrusion processes are less advanced when compared to the penetration attack, and the impacts are limited within the pump station level network, which means that the normal attacks can only intrude into the human-machine interface of the pump station, and a successful normal attack can only affect the attacked pump station. If the attacker has successfully intruded into one pump station, the assaulted pumps in the pump station will be shut down. Meanwhile, there is no impact on other pump stations that have not been attacked. The penetration attack is one of the Advanced Persistent Threats (APT) attacks, which requires more intrusion processes and it is more difficult to be detected. In the penetration attack scenario, the attackers are assumed to launch cyberattacks on the control center in the water distribution network. When the control center is compromised, the attacker can send malicious control demands to any pump stations in the water distribution system, such as shutting down any pumps on their choice. In brief, a successful penetration attack could result in serious system-level failures. In this study the attacker is assumed to shut down only one pump station when the penetration cyber intrusion succeeds, and the target of penetration attack is chosen based on a criticality analysis. This means we assume that the attackers have gained some knowledge of system reliability and will choose to control the most critical pump station in the distribution network.

The SMP model for the normal attack is illustrated in Fig. 2. The initial state of the normal attack scenario is the good state G, which indicates that the system is operated in the normal condition. In most cases, defense strategies will be deployed to detect and block the cyberattacks against the SCADA system. Once the defense strategies fail to fully cover the SCADA system and vulnerabilities of the system are exposed, the system is not in a secure situation anymore, and the state of the system in the SMP model will transit from good state to the intrusion process. The procedure of transition from state V to state A implies the intrusion process to SCADA system. The vulnerable state V indicates that the vulnerabilities of the SCADA system are found by the attacker. After that, the host state H will be reached if the attacker successfully exploited at least one vulnerability of the SCADA system and the attacker is able to acquire the host privilege of the system. Then the active attack state A is reached when the targeted device is exploited by the attacker who can then launch the attack on the destination device. During the intrusion process, if the cyber intrusion attempt is successfully detected and the defensive mechanism is triggered, the system can be brought back to the good state G. The state of system will transit from state A to masked compromised state MC when the SCADA system is able to provide normal service under the attack with proper protection strategy. Then the state of system will be brought back to good state G later when the attack is cleared. Or else, the state of system goes to the triage state TR if the cyber intrusion is not able to be masked. In this state, all the defense strategies and protection mechanisms will be applied to reduce the overall loss that may be caused by the attack. Then the diagnostic and recovery strategies will be generated to track the cyberattack location and recover the SCADA system from the abnormal situation in the failed secure state FS. If the type of attack is accurately identified and corresponding protection mechanism can deal with the current situation, the system will be restored in a short period and eventually come back to the good state. However, in the worst-case scenario, the state of the system reaches the failed state F, which means the applied defense strategies and protection mechanisms lose efficacy, and the cyberattack is successfully launched which will lead to significant damage on the water distribution system.

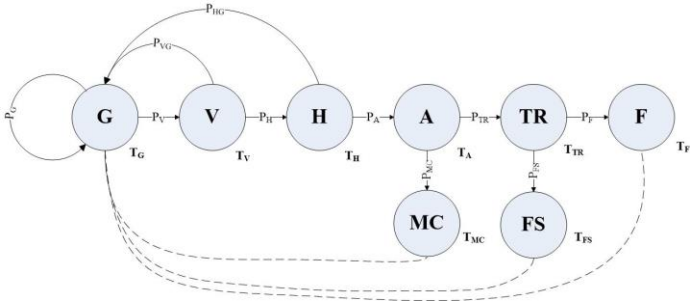

Fig. 2. SMP Model of Normal Attack on SCADA System

The SMP model of the penetration attack is presented in Fig. 3. When compared to the pump station level network, the system-level control cantor generally deploys more comprehensive defense strategies and protection mechanisms. Consequently, it will take more effort to launch a successful cyberattack, and more advanced intrusion technologies are needed from the attacker side. However, more severe damage may be caused if the attacker manages to penetrate the control center of the water distribution network. To control the whole network, the attacker should acquire the privileges of all the servers in the SCADA network. Thus, after exploiting the potential vulnerabilities of the SCADA system in state H, the attacker would try to connect all the servers in the SCADA network. If the attacker has successfully connected all the servers, the state of the system in the SMP model will transit to the connection state C. After that, the state of system shifts to the network state N when the privileges of all the connected servers are acquired by the attacker. Then the state of the system is brought to the attack state A when the targeted devices are exploited by the attacker.

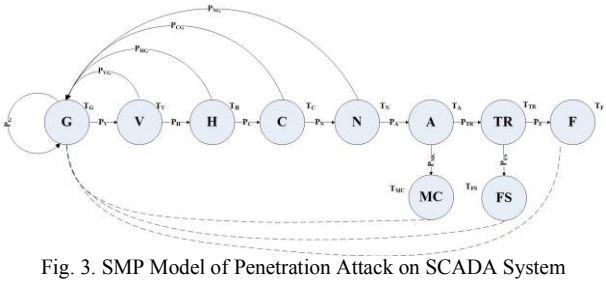

Fig. 3. SMP Model of Penetration Attack on SCADA System

To evaluate the impact of cyberattacks on the reliability of the water distribution systems, one critical issue is the frequency of successful cyberattacks on the SCADA system. Thus, the measurement of the MTTC in the SMP model of the SCADA system is needed for the reliability evaluation. In the SMP model, the MTTC estimates the mean time that the state of the system become the failed or security-compromised states, which are considered as the absorbing states. For the SMP models of two types of cyberattacks, the good state and other states in the intrusion process are transient states, the remaining states are absorbing states in the model. For the normal attack, the set of transient states is represented as $S_{TN} = \{G, V, H, A, TR\}$, while the set of absorbing states is $S_{AN} = \{MC, FS, F\}$. For the penetration attack, the set of transient states is denoted as $S_{TP} = \{G, V, H, C, N, A, TR\}$, and the absorbing state space is denoted as $S_{AP} = \{MC, FS, F\}$. Thus, the two types of attack scenarios share the same absorbing state space which can be combined as $S_A = \{MC, FS, F\}$. For the absorbing SMP models of the two attack scenarios, Q_{KN} and Q_{KP} represent the Markov kernel of normal attack and penetration attack respectively and are given as follows.

$$Q_{KN} = \begin{bmatrix} P_G & P_v & 0 & 0 & 0 & 0 & 0 & 0 \\ P_{VG} & 0 & P_H & 0 & 0 & 0 & 0 & 0 \\ P_{HG} & 0 & 0 & P_A & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & P_{TR} & P_{MC} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & P_{FS} & P_F \end{bmatrix} \quad (1)$$

$$Q_{KP} = \begin{bmatrix} P_G & P_v & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ P_{VG} & 0 & P_H & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ P_{HG} & 0 & 0 & P_C & 0 & 0 & 0 & 0 & 0 & 0 \\ P_{CG} & 0 & 0 & 0 & P_N & 0 & 0 & 0 & 0 & 0 \\ P_{NG} & 0 & 0 & 0 & 0 & P_A & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & P_{TR} & P_{MC} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{FS} & P_F \end{bmatrix} \quad (2)$$

In this study, the concept of mean time to compromise (MTTC) is applied to reflect the cybersecurity of the system. MTTC is commonly used when evaluating the cybersecurity level of a system. The MTTC of successful normal attack or penetration attack is represented as

$$MTTC = \sum_{i \in S_{TN} \text{ or } S_{TP}} v_i T_i \quad (3)$$

where T_i is the mean sojourn time of state i, and v_i is the average number of times that state i is visited before the absorbing states are reached.

The visit count element v_i is formulated as

$$v_i = p_i + \sum_{j \in S_{TN} \text{ or } S_{TP}} v_j p_{ji} \quad (4)$$

where p_{ji} is the transition probability from state j to state i in the SMP model, and p_i is the probability that the initial state of the SMP is state i. For any transition probability in the SMP model, it should follow the following constraint:

$$\sum_{j \in S_A \cup S_{TN} \text{ or } S_A \cup S_{TP}} p_{ij} = 1, \quad i \in S_{TN} \text{ or } S_{TP} \quad (5)$$

Then the visit count elements v_i for normal attack can be derived and calculated as

$$V_G = \frac{1}{P_V P_H P_A (1-P_{MC})}, \quad V_V = \frac{1}{P_H P_A (1-P_{MC})}$$
$$V_H = \frac{1}{P_A (1-P_{MC})}, \quad V_A = \frac{1}{1-P_{MC}} \quad (6)$$
$$V_{TR} = \frac{P_{TR}}{1-P_{MC}}$$

Similarly, the visit count elements v_i for each states of the penetration attack are represented as follows:

$$V_G = \frac{1}{P_V P_H P_C P_N P_A (1-P_{MC})}, \quad V_V = \frac{1}{P_H P_C P_N P_A (1-P_{MC})}$$
$$V_H = \frac{1}{P_C P_N P_A (1-P_{MC})}, \quad V_C = \frac{1}{P_N P_A (1-P_{MC})} \quad (7)$$
$$V_N = \frac{1}{P_A (1-P_{MC})}, \quad V_A = \frac{1}{1-P_{MC}}, \quad V_{TR} = \frac{P_{TR}}{1-P_{MC}}$$

With the formulation from (3) to (6), the MTTC of both attack scenarios can be calculated. Based on the equations given above, increasing any sojourn time of any transient states will directly increase the MTTC of the SCADA system. By applying the described SMP model, the two cyberattack scenarios on the SCADA system of water distribution network can be simulated.

B. Correlations of Cyber Risks

Effective management of the cybersecurity risk of critical infrastructures is still a challenging task. One major reason is that the cybersecurity threats are not independent for each individual water distribution network, though water utilities usually have physically isolated distribution networks. Due to the significant homogeneity and the presence of dependencies in the operation systems and software across different water utilities, their cyber risks are highly correlated. For example, a vulnerability may arise in the operation software in the control system of a water distribution network. When the same operation software stack is installed on another distribution network, the software vulnerability is shared among them. These shared vulnerabilities can lead to correlated cyber risks of multiple water networks and result in greater loss. What's more, the information technology infrastructure of various water utilities is dominated by a few similar technologies that may also leave these utilities with the same potential vulnerabilities, which means although the water utilities are not physically connected to each other, they may share correlated common cyber risks. This kind of cyber risk correlations across various water utilities cannot be modeled through the traditional algorithm of risk analysis. Consequently, a stochastic model is highly needed to identify and formulate the correlation among different water distribution networks due to the similar potential cyber risks they shared.

The Markov kernel and the sojourn time in the absorbing SMP model mentioned in subsection III-A can be used to develop a stochastic model that takes both the independent and correlated cyber risks into account. The Markov kernel and the sojourn time in the SMP model can reflect the SCADA system statuses under cyberattacks. Therefore, for the purpose of developing a stochastic model, the Markov kernel and mean sojourn time in this study are set to be stochastic variables instead of constants, which is different from the common SMP model. For each individual water utility in the distribution systems, the transition probabilities of the Markov kernel and the mean sojourn time of each transient state are modified and formulated as follows.

$$p_{ij}^N = \hat{p}_{ij}^N u + \hat{p}_{ij}(1-u), \quad i \in S_{TN} \text{ or } S_{TP}, \; j \in S_A \cup S_{TN} \text{ or } S_A \cup S_{TP} \tag{8}$$

$$T_i^N = \hat{T}_i^N u + \hat{T}_i \; (1-u), \quad i \in S_{TN} \text{ or } S_{TP} \tag{9}$$

where $\hat{p}_{ij}^N$ indicates the stochastic transition probabilities of a water utility under the independent cybersecurity threats; $\hat{p}_{ij}$ is the stochastic transition probabilities of the water utility under the common cyber risks – both $\hat{p}_{ij}^N$ and $\hat{p}_{ij}$ are assumed to follow the Beta distributions; $\hat{T}_i^N$ and $\hat{T}_i$ are stochastic mean sojourn time of transient state i under the independent and correlated common cyber risks respectively. They are assumed to follow the Gaussian distributions. u is a stochastic variable that follows a Bernoulli distribution $u \sim Bernoulli(\varsigma)$, where ς is the mean value of the Bernoulli distribution. It is used to represent the degree of cyber correlation across different water utilities in the stochastic model. When $\varsigma = 1$, it indicates that all the water utilities are totally independent with each other. Each individual water utility in the distribution network only has independent cyber risks, and they don't share any common cyber risks. When $\varsigma = 0$, it is the completely opposite case, which means the water utilities are largely dependent on each other, similar potential vulnerabilities and common cyber risks are shared across various water utilities in the distribution network. When $\varsigma = 0.5$, it is the most common case, which means the dependence across the water utilities is not that strong, but they do share some common cyber risks.

C. Hydraulic Analysis Integrated Model

For the hydraulic analysis in the proposed model, a powerful software tool called EPANET is incorporated to perform the reliability evaluation of the water distribution network. EPANET is a widely used software for water flow analysis. It can be adopted to analyze the water flow within a period consisting of multiple time steps. In this study, a hydraulic flow-based reliability evaluation considering the component failures due to cyberattacks is performed, and the statuses of system components in the distribution system are simulated in the corresponding procedure.

The method used to solve the flow continuity and head loss equations is termed the 'Gradient Method', which is developed by Pilat and Todini [37]. A hybrid node-loop approach will be employed to simulate the hydraulic state of the pipe network. The detailed formulation of this method is given in [37]. When applying the Gradient method, initial flow values should be set for all the pipes in the network – these values may violate the flow continuity constraints at the first iteration. But after running several iterations, the new nodal heads can be determined by solving the following matrix equation:

$$\boldsymbol{AH} = \boldsymbol{F} \tag{10}$$

where $\boldsymbol{A}$ is an N-dimensional Jacobian matrix, $\boldsymbol{H}$ is an N by one vector of the unknown nodal heads, and $\boldsymbol{F}$ is an N by one vector of the right-hand side terms.

The diagonal elements and off-diagonal terms of the Jacobian matrix are given by

$$A_{ij} = \sum_j p_{ij} \tag{11}$$

$$A_{ij} = -p_{ij} \tag{12}$$

where p_{ij} represents the inverse derivative of the head loss between two points with respect to the flows going through the pipeline. For pipes,

$$p_{ij} = \frac{1}{nr|Q_{ij}|^{n-1} + 2m|Q_{ij}|} \tag{13}$$

For pumps, it is given by

$$p_{ij} = \frac{1}{n\omega^2 r\left(\frac{Q_{ij}}{\omega}\right)^{n-1}} \tag{14}$$

The MCS method is employed to sample the system states. For each sampled system state, the hydraulic simulator EPANET is integrated for performing the water flow analysis. The performance of the water distribution system is mainly dictated by the pressure. Insufficient pressure may lead to water demand losses. For each node, the water that is supplied can be obtained based on the pressure, which is expressed as [38]

$$D_{ai} = \begin{cases} D_{ri} & \text{if } P_{ci} \geq P_{min} \\ D_{ri}\frac{\sqrt{P_{ci}}}{\sqrt{P_{min}}} & \text{if } P_{ci} < P_{min} \end{cases} \tag{15}$$

where D_{ai} is the actual amount of water supplied to the node; D_{ri} is the water demand required at each load point; P_{ci} is the calculated pressure at each node point; and P_{min} is the threshold pressure within the system.

If the threshold pressure cannot be satisfied at any load point, the loss of water demand can be calculated based on (16):

$$D_{lossi} = \left(1 - \frac{\sqrt{P_{ci}}}{\sqrt{P_{min}}}\right) D_{ri} \tag{16}$$

D. Modeling of System Loss

The reliability assessment of the water distribution system is performed based on the Monte Carlo simulation (MCS) considering the cyberattacks against pump stations in the water distribution networks. The proposed algorithm can be used to determine the amount of the loss of water service and the duration of each failure event in the system. The simulation procedure is depicted in Fig. 4 and the detailed process are described as follows.

1) Model the reliability of all physical components in the system, which are composed of the pumps, pipes, and water demands at each junction. The physical reliability of the pumps and pipes are modeled by the parameters including MTTF and MTTR. The sequential MCS is performed to randomly sample physical failures of system components. If there is any physical failure, hydraulic analysis is conducted to evaluate the physical system state to determine the loss of water service during the failure event.
2) Model the cyberattacks against the system. The MTTCs of two attack scenarios are determined based on the proposed SMP considering both the independent and correlated cyber risks. The attack target is the SCADA system in the water distribution network. When the SMP model of any pump station enters the failed secure state FS or failure state F, the failures of pump stations will occur for the attack scenario.
3) Check whether a successful cyberattack occurs. If so, update the statuses of pumps which are affected by the cyberattacks. For example, when one pump station is successfully attacked, its status will be changed to the down status. Then the simulation goes back to step 2.
4) If the stopping criterion is not satisfied, go to step 2). In this paper, the time interval of the simulation process is set to be one hour and the hourly resolution based MCS is performed for 1,000 years, which turns out to be sufficient to achieve the MCS convergence and derive the reliability indices needed for insurance premium calculation.
5) Calculate the final reliability indices and overall system loss.

To evaluate the overall system loss due to cyberattacks, the monetary loss of the water distribution system caused by cyberattacks is estimated by applying the concept of annual interruption cost (AIC) [26], which is commonly used to estimate the reliability worth. Based on the amount of the loss of water service and the duration of all the failure events, the overall expected system loss due to cybersecurity threats K is

obtained by removing the AIC caused by physical contingencies from the AIC considering the interruptions due to both physical failures and cyberattacks:

$$\mathrm{K} = \sum_{i=1}^{N} L_i \cdot d_i \cdot \varepsilon - \sum_{j=1}^{M} L_j \cdot d_i \cdot \varepsilon \qquad (17)$$

where K is the total annual system loss caused by cyberattacks; L_i and L_j are the amounts of losses of water service considering cyberattacks and without considering cyberattacks respectively; d_i and d_j are the durations of failure events considering cyberattacks and without considering cyberattacks respectively; and ε is the reliability worth coefficient of the system interruptions. The first term in (24) $\sum_{i=1}^{N} L_i \cdot d_i \cdot \varepsilon$ is the overall system loss considering both physical failures and cyberattacks, and the second term $\sum_{j=1}^{M} L_j \cdot d_i \cdot \varepsilon$ is the system loss due to system component failures without considering cyberattacks.

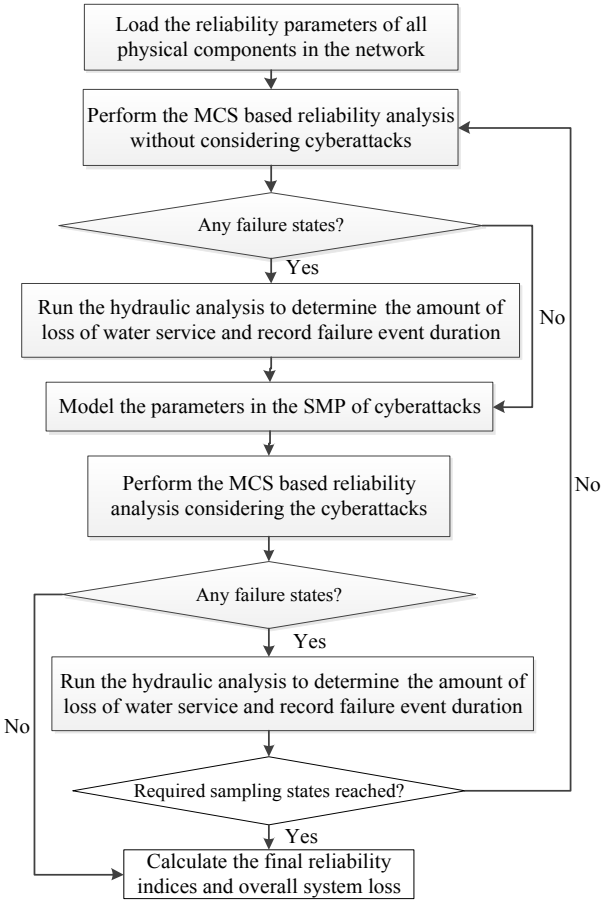

Fig. 4. Flowchart of Reliability Evaluation Considering Cybersecurity

IV. Cyber Insurance Principles and Premium Calculation

Cyber insurance is a risk management technique via which network users' risks can be transferred to an insurance company in return for the insurance premium. With the increasing cyber security risk of critical infrastructures, and in combination with the need for compliance with recently enforced corporate regulation, the demand for cyber insurance has significantly increased. While the critical infrastructures are becoming more and more dependent on their networked operation systems, more potential vulnerabilities are exposed to the cyberattacks than before. The cyber attackers could get access to the monitoring and control system through cyber intrusions. When a successful cyber intrusion is executed, the malicious attacker would be able to send fabricated operation commands to critical components, which could directly lead to a serious system failure. With the development of cyber insurance policies and its strong reliance on risk metrics, cyber insurance is promising to become an efficient tool for critical system owners and operators to manage the increasing cyber risks.

More recently, cyber-insurance policies have become more comprehensive as the insurers have developed a better understanding of the cyber risk landscape. Cyber insurance becomes a powerful tool to align the market incentives to improve the cybersecurity. With the improvement of cyber-insurance, the supporters believe that cyber-insurers would have a better estimation of the overall cybersecurity threats by covering various types of risks. As a result, it would entail the design of cyber-insurance contracts that would place appropriate amounts of self-defense liability on the clients, and consequently make the critical infrastructures more robust against cyberattacks. From the insurer's perspective, cyber insurance represents an opportunity since there is a growing demand to protect the core components in the system, such as network infrastructure and control system. If the insurance companies could accurately quantify the cyber-risks and propose attractive premiums, this opportunity can be translated into considerable profits. However, if the insurance company fails to precisely quantify the cyber risks, it may suffer significant losses. Quantifying cyber-risks for the purpose of insurance pricing is still a challenging task since cyberthreats are difficult to be addressed comprehensively and risk landscapes change frequently.

The expected value premium principle is commonly used in premium calculations. Under this principle, the premium for a risk X can be formulated as $\pi(X) = (1+\rho)E[X]$, where ρ is called the safe loading coefficient. This safe loading coefficient should be carefully determined to ensure the total premium collected by the insurer is sufficient to cover all the potential losses, especially when the pool is relatively large. Most existing premium principles including the expected value premium principle are developed based on the assumption that the individual risks are independent. However, this assumption is violated in the case of cyber-insurance. As explained in the previous section, cyber risks across different water distribution networks are not independent. Therefore, it is necessary to develop new premium principles which consider the correlated cyber risks among different water distribution networks.

In order to control the insolvency risk, that is, the risk that the total loss would exceed the total premium, the total premium in this study is determined based on the VaR or TVaR of the total system loss, and then allocated to the individual water utilities. Value at risk (VaR) is a statistic that is widely used to quantify the level of financial risk within a firm, portfolio or position over a specific time frame. VaR can be applied to measure and control the level of risk exposure. One can apply VaR calculations to specific positions or whole portfolios or to measure firm-wide risk exposure. Let $X_i, i = 1, 2, \ldots, n$ represent the potential losses from different water utilities, then the total loss is represented as $loss = \sum_i^n X_i$. The total premium can be calculated as follows.

$$P_1 = VaR_\alpha(loss) = VaR_\alpha\left(\sum_{i=1}^{n} X_i\right) \qquad (18)$$

where $\alpha \in (0,1)$ represents the confidence level and is set to be close to 1.

Tail Value at Risk (TVaR) is another widely used risk measure in insurance area [39]. When compared to VaR, TVaR is a more conservative way to quantify the premiums. The premiums based on TVaR can be formulated by

$$P_2 = TVaR_\alpha(loss) = \frac{1}{\alpha}\int_{1-\alpha}^{1} VaR_p(loss)d_p \quad (19)$$

By applying the TVaR principle, the premium is higher than the premium calculated based on the VaR principle at the same confidence level, which means the probability that the overall system loss exceeds the collected premiums is lower. Mathematically, based on the VaR premium principle, the probability that the system loss will exceed the collected premiums is equal to 1- α, that is $Pr(loss > P_1) = 1 - \alpha$. While for the TVaR principle, the probability that the overall system loss exceeds the total premium is $Pr(loss > P_2) \leq 1 - \alpha$.

The total premium could be determined based on either the VaR principle or TVaR principle. After that the total premium needs to be allocated to each utility with regard to its risk level. Two principles are proposed to respectively allocate the total premiums defined in (20) and (21) to the individual utilities as follows.

$$\pi_1(X_i) = E[X_i] + \frac{VaR_\alpha(X_i')}{\sum_{i=1}^{n} VaR_\alpha(X_i')} VaR_\alpha(loss') \quad (20)$$

$$\pi_2(X_i) = E[X_i] + \frac{TVaR_\alpha(X_i')}{\sum_{i=1}^{n} TVaR_\alpha(X_i')} TVaR_\alpha(loss') \quad (21)$$

where $X_i' = X_i - E[X_i]$ indicates the centralized version of risk X_i for all i=1, 2, …, n, and similarly, $loss' = \sum_1^n (X_i - E[X_i])$ is the centralized total loss for all i=1, 2, …, n. It is obvious to see that

$$\sum_{i=1}^{n} \pi_1(X_i) = VaR_\alpha(loss) = P_1 \quad (22)$$

$$\sum_{i=1}^{n} \pi_2(X_i) = TVaR_\alpha(loss) = P_2 \quad (23)$$

Another way to allocate the total TVaR premium is based on the individual contributions to the TVaR of the total risk. It is a modification of the original TVaR premium principle. The premium for each water utility can be calculated as follows:

$$\pi_3(X_i) = E\left[X_i \mid \sum_{i=1}^{n} X_i > VaR_\alpha\left(\sum_{i=1}^{n} X_i\right)\right] \quad (24)$$

For the premium calculation, π_2 and π_3 present different ways to allocate the total TVaR premium. In this sense, the numerical outcomes based on π_2 and π_3 should be relatively close. Generally, π_2 premiums are relatively easier to calculate, while π_3 is anticipated to possess better theoretical properties.

V. CASE STUDY

Generally, for most water utilities, the water distribution networks they own are physically isolated from each other. Industrial control systems (ICS) are commonly used in the operation of water system. However, due to the significant similarity in the operation systems and software across different water utilities, the potential cyber risks are highly correlated for water utilities. Due to the high correlation between ICS system and information system and the uniform standard of ICS [40], the SCADA systems in the water distribution network are facing not only the independent cyber risks but also the common cyber risks [41]. The similar vulnerabilities they share could result in correlated cyber risks of multiple water networks and lead to significant system loss. In this sense, although the water utilities are not physically connected to each other, they may share correlated common cyber risks.

Case studies will be presented in this section to illustrate the application of the proposed insurance scheme and premium principle on different water utilities. Case studies are performed on four representative water distribution networks. Each water distribution network is assumed to be owned and operated by a single water utility.

For the four independent water distribution networks, there are 1, 2, 3, 4 pump stations in networks 1, 2, 3, 4, respectively. And the overall system sizes of the distribution networks from 1 to 4 are in an ascending order. The detailed information about each test distribution work is given as follows. Network 1 comprises 40 pipes, 35 junctions and 1 tank, with a total nodal demand of 322.78 gpm (or 169.65 MG) per year. Network 2 comprises 117 pipes, 92 junctions, 2 pumps, 2 reservoirs and 3 tanks, with a total nodal demand of 3,052.11 gpm (or 1,604.19 MG) per year. Network N1 and N2 are built and given by EPANET in the test system files. In order to demonstrate the efficiency of the proposed scheme, two larger test networks N3 and N4 are developed with EPANET and deployed in the case study. Network 3 comprises 121 pipes, 95 junctions and 3 pump stations, with a total nodal demand of 4125.84 gpm (or 2168.54 MG) per year. And Network 4 is the largest system which comprises 154 pipes, 107 junctions, 4 pumps, 2 reservoirs and 3 tanks, with a total nodal demand of 5036.37 gpm (or 2647.12 MG) per year. Some of the junction points in the test water distribution networks have specified water demands, but some junction points do not have water demands. The monetary loss of the water distribution system due to the malicious cyberattacks is evaluated based on the annual interruption. The threshold pressure P_{min} is set to be 40 psi in the case studies.

All the distribution networks are assumed to be physically independent with each other and totally isolated from other water grids. The water demand and parameters are kept constant in the simulation period. The topological diagrams of the tested water distribution networks are given in Fig. 5.

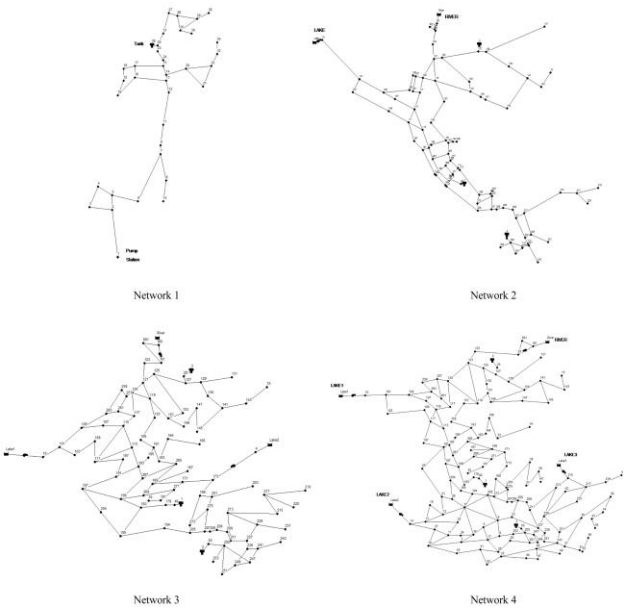

Fig. 5. Test Water Distribution Networks

In this paper, the parameter settings of the sojourn time and transition probabilities of each state in the SMP model are presented in Table I.

TABLE I
PARAMETERS SETTING OF THE TWO CYBERATTACK SCENARIOS

Parameters	Normal Attack	Penetration Attack
T_G	25 days	30 days
T_v	5 days	15 days
T_H	1 day	1 day
T_C		2 days
T_N		1 day
T_A	2 days	4 days
T_{TR}	0.5 day	0.5 day
P_V	1	1
P_H	0.5	0.4
P_C		0.4
P_N		0.4
P_A	0.5	0.5
P_{MC}	0.2	0.3
P_{TR}	0.8	0.7
P_{FS}	0.4	0.3
P_F	0.6	0.7

Based on the formulation described in previous sections, the proposed approach is tested on the four water distribution networks under three different cases, where $\varsigma = 1, \varsigma = 0.5,$ and $\varsigma = 0$, respectively. The value of ς indicates the degree of correlation between cyber risks of the water distribution networks. The expected values of the system annual loss for the three different scenarios and corresponding standard deviations are calculated, and the results are presented in Table II. The coefficients of variation (CoV) are also shown in Table II, which are commonly used to evaluate and reflect the riskiness of marginal losses of the networks. The CoV of all the distribution networks are below 1.3 in this study, which is typical in the insurance field. The marginal distributions of the losses of the four water distribution networks are shown in Fig. 6. For the three different scenarios, the pattern of the marginal distributions of water networks follows a similar fashion.

TABLE II
EXPECTED VALUE, STANDARD DEVIATION AND COEFFICIENT OF VARIATION OF ANNUAL LOSS OF WATER NETWORKS

Network	N1	N2	N3	N4
$\varsigma = 1$				
Expected Values ($)	51288	116548	167238	195604
Standard Deviations ($)	62571	138692	192324	228857
CoV	1.22	1.19	1.15	1.17
$\varsigma = 0.5$				
Expected Values ($)	55462	132245	176964	211315
Standard Deviations ($)	69328	161339	224744	264144
CoV	1.25	1.22	1.27	1.25
$\varsigma = 0$				
Expected Values ($)	53468	137396	191936	223478
Standard Deviations ($)	64696	163501	238001	272643
CoV	1.21	1.19	1.24	1.22

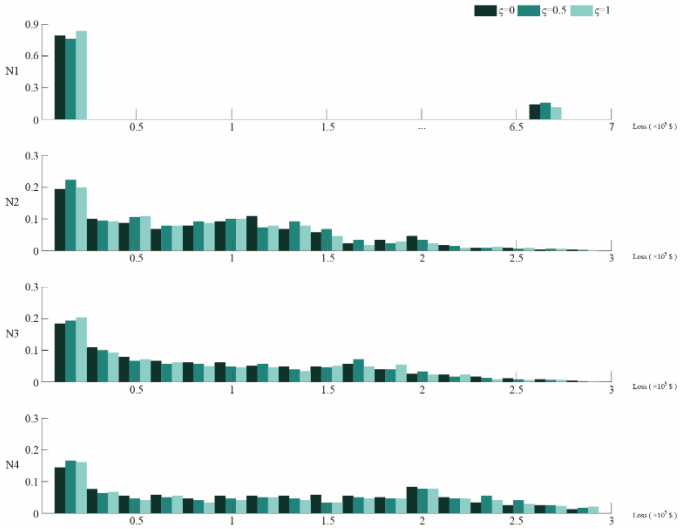

Fig. 6. Marginal Distributions of Loss of Water Distribution Networks.

The cyber risks correlation model proposed in this study will have a great influence on the cyber-insurance premium for each water distribution network while the marginal property of the loss distribution of each distribution network remains unaffected. Table III clearly presents the strength of dependence of the utility losses across various water distribution networks with different values of ς in the case studies. As mentioned in the previous section, ς indicates the degree of dependence across different water distribution networks. When $\varsigma = 0$, it indicates the strongest dependence case. On the contrary, when $\varsigma = 1$, it represents the weakest dependence case. The case when $\varsigma = 0.5$ represents an intermediate strength of dependence across the water grids. The results in Table III illustrate that the dependency of the cybersecurity threats across the four water distribution networks can be accurately reflected by the correlation model.

TABLE III
CORRELATION OF LOSSES OF WATER NETWORKS

	Network	N1	N2	N3	N4
$\varsigma = 1$	**N1**	1	0	0	0
	N2	0	1	0	0
	N3	0	0	1	0
	N4	0	0	0	1
$\varsigma = 0.5$	**N1**	1	0.27	0.28	0.28
	N2	0.27	1	0.26	0.23
	N3	0.28	0.26	1	0.28
	N4	0.28	0.23	0.28	1
$\varsigma = 0$	**N1**	1	0.54	0.56	0.57
	N2	0.54	1	0.53	0.52
	N3	0.56	0.53	1	0.55
	N4	0.57	0.52	0.55	1

The individual premiums allocated for the four water utilities based on the three proposed premium principles are listed in Table IV. In the case study, the confidence level is set to as $\alpha = 10\%$, which means there is only 10% chance that the total loss would exceed the total premium. The risk loading coefficients are calculated by (25), and the risk loading for different cases are presented in Table V.

$$\rho_i = \frac{\pi(X_i)}{E[X_i]} - 1 \qquad \text{for i=1, 2, …, n.} \qquad (25)$$

TABLE IV
PREMIUM FOR EACH INDIVIDUAL DISTRIBUTION NETWORK

Premium ($)	N1	N2	N3	N4
$\varsigma = 1$				
π_1	69365	165498	232461	267978
π_2	79770	188808	267581	316879
π_3	81125	191139	269253	320791
$\varsigma = 0.5$				
π_1	76322	202335	265446	312746
π_2	91923	243331	316766	369801
π_3	93625	244653	320305	371914
$\varsigma = 0$				
π_1	83266	232258	314775	366504
π_2	106159	277540	385791	438017
π_3	112635	280288	387711	442486

TABLE V
RISK LOADING OF EACH INDIVIDUAL DISTRIBUTION NETWORK

Risk Loading ρ	N1	N2	N3	N4
$\varsigma = 1$				
ρ for π_1	0.35	0.42	0.39	0.37
ρ for π_2	0.55	0.62	0.60	0.62
ρ for π_3	0.58	0.64	0.61	0.64
$\varsigma = 0.5$				
ρ for π_1	0.37	0.53	0.50	0.48
ρ for π_2	0.65	0.84	0.79	0.75
ρ for π_3	0.68	0.85	0.81	0.76
$\varsigma = 0$				
ρ for π_1	0.55	0.69	0.64	0.64
ρ for π_2	0.98	1.02	1.01	0.96
ρ for π_3	1.11	1.04	1.02	0.98

In this study, the ratio γ is calculated to represent the cyber insurance premiums as a percentage of the overall operating revenue based on the designed cyber insurance principle. γ is the ratio between the annual premium and the annual revenue of the water utility. The detailed results are shown in Table VI.

$$\gamma = \frac{\text{Annual premium cost}}{\text{Annual revenue of the water utility}} \times 100\% \quad (26)$$

TABLE VI
PREMIUM TO REVENUE RATIO FOR EACH DISTRIBUTION NETWORK

Ratio γ	N1	N2	N3	N4
$\varsigma = 1$				
γ for π_1	13.63%	3.44%	3.57%	3.37%
γ for π_2	15.67%	3.92%	4.11%	3.99%
γ for π_3	15.94%	3.97%	4.14%	4.04%
$\varsigma = 0.5$				
γ for π_1	14.99%	4.20%	4.08%	3.94%
γ for π_2	18.06%	5.06%	4.87%	4.66%
γ for π_3	18.40%	5.08%	4.92%	4.68%
$\varsigma = 0$				
γ for π_1	16.36%	4.83%	4.81%	4.61%
γ for π_2	20.86%	5.77%	5.93%	5.52%
γ for π_3	22.13%	5.82%	5.96%	5.57%

The cyber-insurance premium to revenue ratio for the water utilities is relatively higher when compared to the traditional insurance practice. This premium to revenue ratio on one hand illustrates that severe system losses can be caused by cyber-attacks against the SCADA system in water distribution network. Meanwhile, it also implies the importance of enhance the reliability of water network considering potential cybersecurity threats. One major difference between the water distribution system and other critical infrastructures is that the distribution networks for most water utilities are physically isolated. As a result, when a system failure occurred in one distribution network, there is minor impact on other distribution networks. The loss due to the system failure will remain in its own region. The results in Table VI show that Network 1 has the highest premium to revenue ratio, while Network 4 has the lowest premium to revenue ratio among the four distribution networks. The differences are mainly due to the network configuration, as Network 1 only has one pump station. Once the pump station is compromised by the cyber attackers, it will directly lead to a complete shutdown of the entire water distribution system. In other words, its system reliability considering cyber-attacks is relatively lower than the other water networks. Consequently, the cyber-insurance premium for Network 1 with regards to its risk level will be much higher than the other water networks. The simulation results imply that the cybersecurity level will have a significant impact on the premium of the water distribution network, and the water utilities will benefit more by enhancing its cybersecurity in the long run.

In order to show how the security level of the system can affect the cyber insurance premium, a comparative study is performed with the degree of dependence across different water distribution networks ς=0.5. Two scenarios are designed and compared to the basic case. The security level of the water distribution system can be indicated by the parameters setting in the SMP model. P_H, P_C, P_N are decreased from 0.4 to 0.3 in scenario 1, which indicates that the system cybersecurity level is strengthened as more advanced and efficient detection and protection mechanisms are applied. As a result, the system has lower probabilities to be compromised by the cyber-attacks. On the contrary, P_H, P_C, P_N are increased from 0.4 to 0.5 in scenario 2, which means that the cybersecurity level of the system is reduced. So the system is more vulnerable to the potential cyber risks, and the system has higher probabilities to be compromised by the cyber-attacks.

TABLE VII
THE IMPACT OF SYSTEM SECURITY LEVEL ON PREMIUM

		N1	N2	N3	N4
Basic case	**Expected value**	$55462	$132245	$176964	$211315
	Premium (VaR)	$76322	$202335	$265446	$312746
***Scenario* 1** Security level strengthened	**Expected value**	$41256	$106178	$132167	$158794
	Premium (VaR)	$64823	$163280	$203824	$234715
***Scenario* 2** Security level weakened	**Expected value**	$66238	$149854	$205317	$257386
	Premium (VaR)	$98274	$242418	$326855	$398572

The detailed comparative case study results are presented in Table VII. The results in scenario 1 imply that the premiums for all the four water utilities are significantly reduced when the overall system cybersecurity is strengthened. In other words, the premium of cyber insurance can indicate the level of the cyber

protection. All the water utilities could benefit from lower premiums by enhancing their cybersecurity level. Therefore, the proposed cyber insurance scheme encourages the stakeholders to increase their investments on cybersecurity so that the annual insurance premiums will be reduced. While for scenario 2, if the cybersecurity of water utility is weakened, the premiums for the four utilities all experience dramatic increase. Both the expected value of the loss and the corresponding premium increase significantly. This implies that the water utilities will be financially penalized in terms of cyber insurance premiums with the degradation in cybersecurity.

VI. CONCLUSION

This paper proposes a modified semi-Markov process (SMP) incorporating a cyber risk correlation model to evaluate the potential cybersecurity threats against the SCADA system in the water distribution network. By applying the proposed approach, both the independent cyber risks within one individual water network and the correlated cyber risks across different water utilities can be considered. A sequential Monte Carlo simulation-based algorithm is also developed to assess the overall system loss and the failure event duration considering two types of cyberattack scenarios against the water distribution networks. The total cyber-insurance premium can be estimated based on the designed actuarial principles. After that, the premium allocation for each individual water utility is further determined with regards to its individual risk level. The results of the case studies indicate that higher system reliability and more advanced self-protection mechanism can reduce the cyber-insurance premium of the water utilities with the proposed actuarial principles. Lack of research in this area may be a major reason why the cyber-insurance market has not been established yet. A detailed analysis of cybersecurity outcomes considering the correlation among different utilities will be instrumental in stipulating market-friendly cybersecurity coverage policies. Besides the cybersecurity threats on the water distribution system, the power supply reliability may affect the performance of water distribution system as well. In this sense, the cascading effect from one critical infrastructure to another critical infrastructure can be modeled. However, this cascading effect is not covered in the scope of the current work and left for the future work. Furthermore, in future studies, there are several areas where this research can be extended, such as developing a more comprehensive model which can tackle massive water utilities. Also investigating the cyberattacks on the SCADA system of the real water distribution networks will be instrumental in designing a more detailed and practical cyber insurance framework based on the emerging features of cybersecurity threats in practice.

REFERENCES

[1] S. Amin, X. Litrico, S. Sastry and A. M. Bayen, "Cyber Security of Water SCADA Systems—Part I: Analysis and Experimentation of Stealthy Deception Attacks," in *IEEE Transactions on Control Systems Technology*, vol. 21, no. 5, pp. 1963-1970, Sept. 2013.

[2] A. Hassanzadeh, A. Rasekh, S. Galleli, M. Aghashahi, R. Taormina, A. Ostfeld, and M. Banks, "A review of cybersecurity incidents in the water sector." Journal of Environmental Engineering 146.5 (2020): 03120003.

[3] U.S. Environmental Protection Agency (EPA) *Water Sector Cybersecurity Brief for States*. EPA. (2018)

[4] J.H. Germano, *Cybersecurity risk & responsibility in the water sector*. American Water Works Association. (2018)

[5] S. Reed, *Was BWL prepared for a ransomware attack?* Lansing State Journal. (2016)

[6] B. Obama, "Executive order 13636: Improving critical infrastructure cybersecurity." Federal Register 78.33 (2013): 11739.

[7] S. Diop, P. M'mayi, D. Lisbjerg, and R. Johnstone, "Vital water graphics: an overview of the state of the world's fresh and marine waters," vol. 1: UNEP/Earthprint, 2002.

[8] E. J. Lee and K. J. Schwab, "Deficiencies in drinking water distribution systems in developing countries," Journal of water and health, vol. 3, pp. 109-127, 2005.

[9] W. Yurcik, and D. Doss, "Cyberinsurance: A market solution to the internet security market failure," in *Workshop on Economics and Information Security* (WEIS), Berkeley, CA. 2002.

[10] L.A. Gordon, L.P. Martin, and T. Sohail "A framework for using insurance for cyber-risk management." *Communications of the ACM* 46.3 (2003): 81-85.

[11] B. Schneier, "Hacking the business climate for network security." *IEEE Computer* 37.4 (2004): 87-89.

[12] C. Biener, M. Eling, and J. H. Wirfs, "Insurability of cyber risk," Newsletter on Insurance and Finance, vol. 14, pp. 1–4, 2014.

[13] D. Young, J. Lopez, M. Rice, B. Ramsey, and R. McTasney, "A framework for incorporating insurance in critical infrastructure cyber risk strategies," International Journal of Critical Infrastructure Protection, vol. 14, pp. 43–57, 2016.

[14] H. Ogut, N. Menon, and S. Raghunathan, "Cyber insurance and IT security investment: Impact of interdependent risk," in *Workshop on the Economics of Information Security* (WEIS), Cambridge, MA, 2005.

[15] R. Bohme and G. Schwartz, "Models and Measures for Correlation in Cyber-Insurance." in *Workshop on the Economics of Information Security* (WEIS). 2006.

[16] R. Bohme and G. Schwartz, "Modeling cyber-insurance: Towards a unifying framework. in *Workshop on the Economics of Information Security* (WEIS). 2010.

[17] R. Pal, L. Golubchik, and K. Psounis, Aegis: A novel cyber-insurance model. In IEEE/ACM *GameSec*, 2011.

[18] N. Shetty, G. Schwarz, M. Feleghyazi, and J. Walrand. Competitive cyberinsurance and internet security. In *Workshop on Economics and Information Security* (WEIS), 2009.

[19] S. Shrivastava, S. Adepu, and A. Mathur, "Design and assessment of an Orthogonal Defense Mechanism for a water treatment facility." Robotics and Autonomous Systems 101 (2018): 114-125.

[20] S. Adepu, and A. Mathur, "Assessing the effectiveness of attack detection at a hackfest on industrial control systems." IEEE Transactions on Sustainable Computing (2018).

[21] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey." IEEE Internet of Things Journal 4.6 (2017): 1802-1831.

[22] R. Taormina, S. Galelli, N.O. Tippenhauer, E. Salomons, and A. Ostfeld, "Characterizing cyber-physical attacks on water distribution systems." Journal of Water Resources Planning and Management 143.5 (2017): 04017009.

[23] R. Taormina, S. Galelli, H.C. Douglas, N.O. Tippenhauer, E. Salomons, and A. Ostfeld, "A toolbox for assessing the impacts of cyber-physical attacks on water distribution systems." Environmental modelling & software 112 (2019): 46-51.

[24] H.C. Douglas, R. Taormina, and S. Galelli, "Pressure-driven modeling of cyber-physical attacks on water distribution systems." Journal of Water Resources Planning and Management 145.3 (2019): 06019001.

[25] D. Nikolopoulos, G. Moraitis, D. Bouziotas, A. Lykou, G. Karavokiros, and C. Makropoulos, "Cyber-Physical Stress-Testing Platform for Water Distribution Networks." Journal of Environmental Engineering 146.7 (2020): 04020061.

[26] R. Billinton and R. N. Allan, *Reliability evaluation of engineering systems*: Springer, 1992.

[27] R. N. Allan, *Reliability evaluation of power systems*. Springer Science & Business Media, 2013.

[28] D. Kirschen and F. Bouffard, "Keeping the lights on and the information flowing," *IEEE Power Energy Mag*., vol. 7, no. 1, pp. 50–60, Jan. 2009.

[29] W. S. Baer, and A. Parkinson, "Cyberinsurance in *IT* security management." *IEEE Security & Privacy* 5.3 (2007): 50-56.

[30] R. P. Majuca, W. Yurcik, and J. P. Kesan, "The evolution of cyberinsurance." *arXiv preprint cs/0601020* (2006).

[31] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey." *Computer Science Review* 24 (2017): 35-61.

[32] National Protection and Programs Directorate (NPPD), "Insurance for cyberrelated critical infrastructure loss: Key issues," Department of Homeland Security (DHS), Washington, DC, Tech. Rep., July 2014.

[33] R. Anderson, and T. Moore, "The economics of information security." *Science* 314.5799 (2006): 610-613.

[34] G. Gluschke and M. H. Cain, Cyber Security Policies and Critical Infrastructure Protection, M. Macori, Ed. Potsdam, Germany: Institute for Security and Safety (ISS) Press, 2018.

[35] B. B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes

of intrusion tolerant systems," *Performance Evaluation*, vol. 56, no. 1-4, pp. 167–186, 2004.
[36] Y. Zhang, L. Wang, and Y. Xiang, "Power system reliability analysis with intrusion tolerance in SCADA systems." *IEEE Transactions on Smart Grid* 7.2 (2015): 669-683.
[37] L. A. Rossman, "EPANET 2: User's Manual," 2000.
[38] A. Ostfeld, D. Kogan, and U. Shamir, "Reliability simulation of water distribution systems–single and multiquality," Urban Water, vol. 4, pp. 53-61, 2002.
[39] S. A. Klugman, H. H. Panjer, and G. E. Willmot, *Loss Models: From Data to Decisions.* John Wiley & Sons, 2012.
[40] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to industrial Control Systems (ICS) Security," NIST Special Publication 800-82, pp. 1–68, 2015.
[41] W. Shim, "Interdependent risk and cyber security: An analysis of security investment and cyber insurance," Ph.D. Dissertation, Michigan State University, East Lansing, MI, 2010.