Survey of Attack Projection, Prediction, and Forecasting in Cyber Security

Martin Husák, Jana Komárková, Elias Bou-Harb, and Pavel Čeleda

***Abstract*—This paper provides a survey of prediction, and forecasting methods used in cyber security. Four main tasks are discussed first, attack projection and intention recognition, in which there is a need to predict the next move or the intentions of the attacker, intrusion prediction, in which there is a need to predict upcoming cyber attacks, and network security situation forecasting, in which we project cybersecurity situation in the whole network. Methods and approaches for addressing these tasks often share the theoretical background and are often complementary. In this survey, both methods based on discrete models, such as attack graphs, Bayesian networks, and Markov models, and continuous models, such as time series and grey models, are surveyed, compared, and contrasted. We further discuss machine learning and data mining approaches, that have gained a lot of attention recently and appears promising for such a constantly changing environment, which is cyber security. The survey also focuses on the practical usability of the methods and problems related to their evaluation.**

***Index Terms*—Cyber security, intrusion detection, situational awareness, prediction, forecasting, model checking.**

I. Introduction

CYBER security is a broad field of research, and the detection of malicious activities on the network is among the oldest and most common problems [1]. However, intrusion detection is mostly reactive and responses to specific patterns or observed anomalies. The intuitive next step is taking a proactive approach, in which there is a need to preemptively infer the upcoming malicious activities so that we could react to such events before they cause any harm [2]. Research efforts and progress in predictions and forecasting in cyber security are not as prominent as attack detection. However, it is gaining more attention, and a breakthrough in this field would benefit the whole discipline of cyber security [1].

Before we can start making predictions about cyber security, there is a need to examine what can actually be predicted and what obstacles are there that make this problem hard. First, if there is an attack taking place, it is possible to predict its next steps. Such a task is called attack projection [3]. A similar task is intention recognition [4], in which we also estimate what is the ultimate goal of an adversary, which can also help us in predicting adversary's next moves. Another task is predicting cyber attacks that are going to happen. In this case, we talk about intrusion prediction [5], although we can use similar approaches to predict also vulnerabilities. Finally, we might be interested in overall statistics of attacks, the presence of threats, and other pieces of information that together form a network security situation. In this context, we talk about network security situation forecasting [6]. Numerous methods and system were proposed to approach these problems, and as we point out in this survey, they often share a common theoretical background, which makes the particular tasks and use cases similar to each other.

To summarize the open problems, we emphasize the following research challenges of predictions and forecasting in cyber security:

- What can be predicted in a cyber security domain? Is it the next move of an adversary, appearance of a new attacker, or cyber security situation from a global perspective?
- How usable are the predictions in cyber security? Can they be used to effectively mitigate an attack or to get prepared for an upcoming security threat?
- How to evaluate predictions in cyber security and what metrics should be used? Is it sufficient to rely on evaluation using datasets and testbeds or can the actual prediction accuracy be measured in a live network setting?

To this end, such research challenges impact both theoretical and practical perspectives. In this survey, we postulate if predictions and forecasts are possible, and we are also interested in the applicability and evaluation of the theoretical results.

A. Paper Organization

This paper is divided into nine sections. Section II introduces the main use cases of predictive and forecasting methods in cyber security. Taxonomy of attack prediction methods is presented in Section III. A literature review of methods of cyber attack prediction is presented in Sections IV–VII with a detailed explanation of the methods. Section VIII discusses evaluation of attack prediction and lessons learned. Finally, Section IX concludes the paper and provides an outlook on future research.

Manuscript received February 2, 2018; revised July 31, 2018; accepted September 5, 2018. Date of publication September 24, 2018; date of current version February 22, 2019. This work was supported by ERDF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" under Grant CZ.02.1.01/0.0/0.0/16_019/0000822. *(Corresponding author: Martin Husák.)*

M. Husák, J. Komárková, and P. Čeleda are with the Institute of Computer Science, Masaryk University, 602 00 Brno, Czech Republic (e-mail: husakm@ics.muni.cz; komarkova@ics.muni.cz; celeda@ics.muni.cz).

E. Bou-Harb is with the Cyber Threat Intelligence Laboratory, Florida Atlantic University, Boca Raton, FL 33431 USA (e-mail: ebouharb@fau.edu).

Digital Object Identifier 10.1109/COMST.2018.2871866

This paper is intended for an audience familiar with computer networks and cyber attacks. Nevertheless, the tasks and use cases of attack prediction, projection, and forecasting are defined in Section II, so the reader does not need to be an expert in the field. Probably the most interesting part of this survey can be found in Sections III–VII. A taxonomy in Section III provides a high-level view of the discussed methods. Sections IV–VII contain theoretical background and list of recent literature for each group of methods. There is also a table included in each of the four sections (Tables II–V) that summarizes all the prediction method. If a paper listed in the table is discussed in the text, it is distinguished by the author name(s) in *italic*. Selected papers are highlighted with a gray background in the table and announced in the text as recommended reading. Practitioners are advised to read Section VIII that contains practical implications and open problems in the field.

B. Literature Search Methodology

A literature search for this survey covered many journals and conference proceedings. Although the discussed problems are studied in the field of cyber security, the topics are often addressed in journals and conferences on computer networks and communications. Due to the specific nature of this work, we also had to go through journals and conferences dedicated to formal methods in computer science, such as expert systems and their applications, which appeared to be an important source of papers for this survey.

First, we reviewed survey-oriented journals like IEEE Communication Surveys and Tutorials and ACM Computing Surveys, although no survey was found to discuss predictions in cyber security. Subsequently, we used Google Scholar, IEEE Xplore, and ACM Digital Library to search for related papers using the queries *"cyber security" AND "prediction"*, *"cyber security" AND "attack projection"*, *"cyber security" AND "forecasting"*. Further, we looked for publications citing or cited by already found works or having the same author. The publications are presented in chronological order from 2012 to 2018. Papers published prior to 2012 are not included in this survey unless they pose fundamental contribution or are still highly relevant. The numbers of citations assessed by Google Scholar and Scopus were used to identify the most influential research papers.

C. Existing Surveys

To the best of our knowledge, prediction and forecasting methods in cyber security were not surveyed in such scope yet, although several surveys of particular tasks and use cases were published in recent years. Wei and Jiang [7] in 2013 analyzed the problem of network security situation prediction and compared predictions of NSSA using neural networks, time series, and support vector machines, although mostly to illustrate the limitations of the available methods. Yang *et al.* [3] formalized the task of attack projection and surveyed literature on the topic in 2014. Three categories are listed, prediction based on attack plans, estimates of attackers capabilities and intentions, and predictions by learning attack patterns and attacker's behavior. Leau and Manickam [6] in 2015 surveyed several existing techniques of network security situation forecasting. They grouped them into three categories by their theoretical background: machine learning, Markov models, and Grey theory. In 2016, Gheyas and Abdallah [8] surveyed detection and prediction of insider threats. Although this topic is still of interest, the predictive approaches do not seem to be studied in recent years. Ramaki and Atani [2] surveyed early warning systems, which often use predictive analytics, although these are not discussed much in details. A simple yet usable taxonomy of intrusion prediction methods can also be found in a paper by Abdlhamed *et al.* [9]. The authors first split related work into two groups, predictions methods and intrusion detection enhancement. The prediction methods are categorized into three groups, methods using Hidden Markov models, methods based on Bayesian networks, and genetic algorithms. Subsequently, they classify artificial neural networks, data mining, and algorithmic methodologies as three enhancements for intrusion detection, which enhance the effectiveness of prediction systems. The same authors later published a survey of intrusion prediction [5], in which they categorize prediction methodologies and prediction systems. Prediction methodologies can be based on alert correlation, sequences of actions, statistical and probabilistic methods, and feature extraction. Prediction systems are then categorized as based on hidden Markov models, Bayesian networks, genetic algorithms, neural networks, data mining, and algorithmic methods. Recently, Ahmed and Zaman [4] surveyed methods of attack intention recognition, a field dominated by methods based on graphical models. The authors recognize four categories: causal networks, path analysis, graphical models, and dynamic Bayesian networks. Methods based on causal networks were evaluated as the most effective.

II. Use Cases of Prediction and Forecasting in Cyber Security

From the surveyed research papers, we distilled several tasks that pose a use case of prediction or forecasting in cyber security. The tasks are summed up in Table I. Historically, the first such use cases are the attack projection [3] and the attack intention recognition [4], which are closely tied to intrusion detection. The task is to predict what is an attacker (in an already observed attack) going to do next, and what is attacker's ultimate goal [4]. In practice, these two tasks use very similar methods, and can often be used interchangeably. Later, the task of predicting attacks emerged [5]. This task is more general as it does not require observation of a preceding activity. The expected outcome is a prediction of an attack before it actually occurs, not predicting a continuation of an observed series of events. Finally, the task of forecasting a security situation [6] is a highly generic use case related to cyber situational awareness. The task is not to predict an attack, but rather forecast the situation in the whole network [2]. The outcomes may be a forecast of increase or decrease in the number of attacks or vulnerabilities in the network. The following subsections discuss the use cases in more details.

TABLE I
USE CASE CHARACTERISTICS

Use case	Task description	Previous surveys
Attack projection	What is an adversary going to do next?	Yang et al. [3]
Attack intention recognition	What is an ultimate goal of an adversary?	Ahmed and Zaman [4]
Attack / Intrusion prediction	What type of attack will occur, when, and where?	Abdlhamed et al. [5]
Network security situation forecasting	How is the overall situation going to evolve?	Leau and Manickam [6]

A. Attack Projection and Intention Recognition

The initial idea of attack projection dates back to 2001 when Geib and Goldman [10] proposed attack projection as an extension of attack plan recognition and identified its prerequisites and possible problems, such as a need to work with unobserved actions, failure to observe, and consideration of multiple concurrent goals. First methods started to appear around 2003 [11], [12] and the research in this field is still active, including literature reviews [3], [4].

To project the continuation of an attack and predict the upcoming events, we typically need to document the behavior of the attackers and establish a description of an attack for later use. Sample anatomy of a cyber attack was given by Bou-Harb *et al.* [13]. The anatomy consists of the following steps:

i. Cyber scanning
ii. Enumeration
iii. Intrusion Attempt
iv. Elevation of Privilege
v. Perform Malicious Tasks
vi. Deploy Malware/Backdoor
vii. Delete Forensic Evidence and Exit

Many types of cyber attacks follow this simple sequence of events, which can be observed either in the network traffic or on the target system, where intrusion detection systems may be found. The projection of an ongoing attack is, in essence, very simple. If we see a sequence of events that fit an attack model, we may assume that the attack will continue according to the model. Thus, we predict the adversary's next step. Nevertheless, vague description of an attack is not usable for algorithmic predictions and, thus, more formal description of an attack is required, e.g., in the form of an attack graph [11]. Further, many different types of attacks exist, so there is a need to create a model for all the attacks that are going to be projected. Historically, the first methods depended on attack libraries [12] that had to be manually filled, which requires substantial effort and continuous updates [3]. Thus, modern methods more often rely on data mining to automatically generated attack patterns for attack projections [14], [15].

A basic idea behind attack intention recognition is similar to attack projection; the difference is in motivation. In attack projection, we are not that interested in an attacker's intentions. If an ultimate goal of an adversary is estimated, the predictions of future malicious events may be suited more to the particular attack. Attacker's intention recognition is studied in network forensics [4], where it was originally performed over historical data. However, novel approaches are focused on real-time intention recognition and are becoming more and more similar to attack projection.

B. Intrusion Prediction

A more general task predicting cyber attacks, mostly intrusions [5]. Instead of projecting an already observed attack, we are interested in predicting novel attacks. Minor variations of the task also include predictions of vulnerabilities, attack propagation and multi-stage attacks, and other cyber security events. There is also a significant overlap with research on early warning systems [2], which pose a practical use case for prediction in cyber security in general.

Due to the task being too generic, there are not many common elements in the proposed approaches. While attack projection mostly relied on discrete models of cyber attacks, there is a plethora of methods and models used for attack prediction ranging from discrete models, e.g., attack graphs, to continuous models, e.g., time series. Thus, one may predict the attacks using the same discrete models that used for attack projection, with only a small variation in prediction start. For example, the prediction may not start with an already observed malicious event, but rather with a probability that a particular vulnerability in the network will be exploited. An example of an approach based on a continuous model is a time series representing a number of attacks on a certain system or network in time. The time series may then be used to predict if an attack is going to happen or not. Advanced methods may calculate with types of attacks and characteristics of attackers and victims, so that they may estimate what type of attack is going to happen, who is going to an attacker, and who is going to be the victim. Recent approaches often include non-technical data sources in the predictions so that we may see methods based on sentiment analysis on social networks [16], [17] or changes in user behavior [18], thus overcoming the "unpredictability" of cyber attacks.

C. Network Security Situation Forecasting

The last main use case of predictions and forecasting in cyber security is the forecasting of a global security situation. Instead of focusing on an individual attacker or an ongoing attack, there is a need to know what is a holistic state of an information system or a network under our control. This use case of cyber security prediction was briefly surveyed by Leau and Manickam [6].

A key concept of a holistic view on cyber security is often referenced as *cyber situational awareness* (CSA) or *network security situational awareness* (NSSA). Both terms originate in the general term *situational awareness* that originates in military research. One of the most widely used definitions of situational awareness is the one by Endsley [19]: "Perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in near future." The definition itself emphasizes three levels, perception, comprehension, and projection, as illustrated on Figure 1 [20]. When applied in the cyber security field, perception corresponds to monitoring of cyber

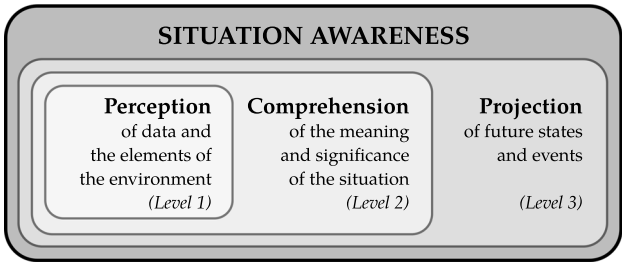

Fig. 1. Levels of situational awareness [20].

systems as well as intrusion detection. Comprehension corresponds to the understanding of the cyber security situation, in our case represented by modeling of cyber threats or correlating security alerts. Finally, projection, as understood in the context of this paper, is an action of predicting the changes in a cyber security situation [3]. As we can see, the importance of projection is rooted deep in the theoretical background of the situational awareness [21] and thus, motivates the research on predictions in cyber security. The motivation is stronger than in attack projections presented earlier, where the projection is seen only as an extension of intrusion detection.

Most of the works use quantitative analysis to describe the network security situation at a point in time. The resulting values are then projected into the future. Such an approach does not provide any information about the exact nature of future attacks. However, it can supply warnings about general increase or decline of network security in future. The quantitative approach allows for efficient application of methods for analysis and projection that have been thoroughly researched in the context of other fields. The quantitative analysis requires a measure for evaluation of a network security situation. There is no established canonical measure for assessing network security situation. However, there are two prevalent approaches: hierarchical method with additive weights and attack intensity estimation method. The hierarchical method evaluates the network security situation bottom up. Initially, a security situation is measured for each host. Subsequently, the values for each host are multiplied by a weight of the host and summed up to compute the overall security of the network. The actual method for estimating host security varies by author. The weight usually expresses the importance of the host. The attack intensity approach fuses information about the ongoing attacks from diverse sources and estimates an overall attack intensity. The overall intensity is derived from the number and severity of attacks against the whole network. The prediction can then give a warning about incoming increase or recess of attacks. Note that since the input, as well as the predicted value, are numeric, most of the models used for prediction of network security situation falls into the category of continuous models.

III. Taxonomy and Metrics of Prediction Methods in Cyber Security

This section presents a taxonomy of attack prediction methods. There are several approaches for categorizing the methods, ranging from use cases to mathematical background. Related surveys were mostly focused on a single use case, such as attack projection or network security situation forecasting. We decided not to categorized the methods by their use case but instead on their theoretical background, thus highlighting the similarities between the methods solving different tasks. Nevertheless, the use cases of particular research works are explained in their descriptions. The resulting taxonomy of attack prediction methods is illustrated in Figure 2.

First, we categorize the methods by the theoretical background they use as a basis for prediction. Typically, a predictive method in cyber security uses a model to represent an attack or network security situation. Clear examples are graphical models of attack progression or game-theoretical representation of attacker-defender interaction. Approaches based on these discrete model formed the first category of methods. In contrary, the network security situation might be represented via a continuous mathematical model, e.g., a time series or a grey model, that are excellent for forecasting. The second category of methods thus contains methods based on continuous models. Both categories contain several subcategories, each representing a particular model. The third category of predictive and forecasting methods contains the methods based on machine learning and data mining. A common characteristic of such methods is that they include the learning phase, i.e., creating the knowledge base for further predictions. It is worth noticing that several model-based approaches used data mining to create a model before making predictions [14], [15]. However, data mining plays only a supporting role in such cases so that these methods do not qualify for the machine learning and data mining category. Finally, the fourth category contains methods that are either very specific or otherwise hard to categorize. For example, predictions of DDoS attack volume and predictions based on sentiment analysis on social media are very specific and use unique methods in the context of this work. The fourth category further includes a group of similarity-based approaches, which are unfortunately highly fragmented, and a group of methods based on evolutionary computing, which emerged very recently and thus it is too soon to properly categorize it.

Apart from the theoretical background, we are interested in the input data that are used for predictions. There are multiple available data sources with different levels of abstraction. A method can work with raw data, such as network traffic and system logs, or with the abstract data, such alerts generated by intrusion detection systems or numerical representation of network security situation. Further, for the needs of evaluation of the methods, the data can be either available as a dataset or gathered from a live environment. Such information are contained in taxonomy but can be found in the Tables II–V.

IV. Methods Based on Discrete Models

The first group of cyber attack prediction methods is using discrete models. In this section, we discuss methods using graph models, such as attack graphs, Bayesian networks, and Markov models. An alternative approach is based on game theory. A summary of methods and research papers discussed in this section can be found in Table II.

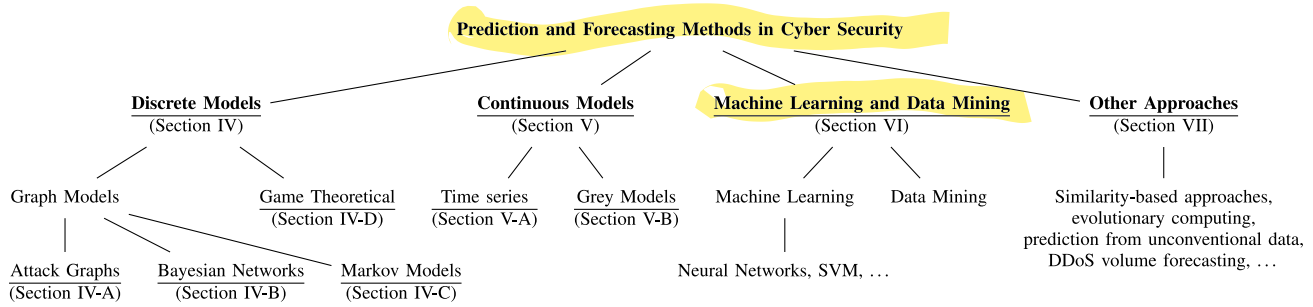

Fig. 2. Taxonomy of attack prediction and forecasting methods.

TABLE II
COMPARISON OF PREDICTION METHODS, PART I – APPROACHES BASED ON DISCRETE MODELS

Attack Graphs (Section IV-A)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Hughes and Sheyner [11]	2003	Attack graph	Proof-of-concept	The first proposed methods
Chung et al. [22] (NICE)	2013	Attack graph	Testbed	Part of countermeasure selection tool
Kotenko and Chechulin [23] (CAMIAC)	2013	Attack graph	Proof-of-concept	Part of impact assessment tool
Cao et al. [24], [25]	2014-2015	Attack graph	Live	75 % accuracy, factor graph
Ramaki et al. [26] (RTECA)	2014	Attack graph	DARPA 2000	95 % accuracy
GhasemiGol et al. [27], [28]	2016	Attack graph	Proof-of-concept	Scalable for large-scale networks
Polatidis et al. [29], [30]	2017-2018	Attack graph	Proof-of-concept	Recommender system
Bayesian Networks (Section IV-B)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Qin and Lee [12]	2004	Causal network	DARPA GCP	Fundamental work on attack projection
Wu et al. [31]	2012	Bayesian network	-	Only model extensions
Ramaki et al. [32]	2015	Bayesian attack graph	DARPA 2000	92.3–99.2 % accuracy, real-time
Okutan et al. [33]	2017	Bayesian network	Live	63%–99% accuracy, non-conventional signals
Huang et al. [34]	2018	Bayesian network	Testbed (cyber-physical)	Application in a larger framework
Markov Models (Section IV-C)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Farhadi et al. [15]	2011	Hidden Markov model	DARPA 2000	81.33 %–98.3 % accuracy, data mining, illustrative example of a real-time attack projection framework
Sendi et al. [35]	2012	Hidden Markov model	DARPA 2000	Prediction of next step in multi-step attack
Shin et al. [36] (APAN)	2013	Markov chain	DARPA 2000	Improving intrusion detection by predictions
Zhang et al. [37]	2014	Hidden Markov model	DARPA 2000	Improvements in theoretical background
Kholidy et al. [38], [39], [40]	2014	Hidden Markov model, Variable-order Markov model	DARPA 2000	Timing metric – predicts an attack coming in 39 minutes
Abraham and Nair [41]	2015	Markov model	Testbed	Exploitability analysis, vulnerability life-cycle
Bar et al. [42], [43]	2016	Markov chain	Live (honeypot)	Large-scale attack propagation models
Game Theory (Section IV-D)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Lisý et al. [44]	2012	Game theory	Virtual attacks	38.6 % accuracy
Píbil et al. [45]	2012	Game theory	Comparison with naive algorithms	Extensions of previous works
Abdlhamed et al. [9]	2016	Game theory, time series	DARPA 1999	Combined approach

A. Attack Graphs

An attack graph is a graphical representation of an attack scenario that was introduced in 1998 by Phillips and Swiler [46] and quickly became a popular method of formal representation of attacks. Thus, the first attack prediction methods were based upon attack graphs. The attack graphs also served as a basis for other model-checking approaches, e.g., methods using Bayesian networks and Markov models and game-theoretical methods.

1) Method Description: An *attack graph* (often abbreviated as AG) is a tuple $G = (S, r, S_0, S_s)$, where S is a set of states, $r \subseteq S \times S$ is a transition relation, $S_0 \subseteq S$ is a set of initial states, and $S_s \subseteq S$ is a set of success states [47]. The initial state represents the state before the attack starts. Transition relations represent possible actions of an attacker. These are usually weighted, e.g., by the probability that the attacker will choose the action. If an attacker takes all the actions to transition from the initial state to any of the success states, the attack is successful, as the success state represents a system compromise.

As stated earlier, an attack graph is constructed either manually or automatically; a popular approach is using data mining to generate attack graphs [14]. An example of an attack graph is shown in Figure 3. In the nodes, we can see possible events

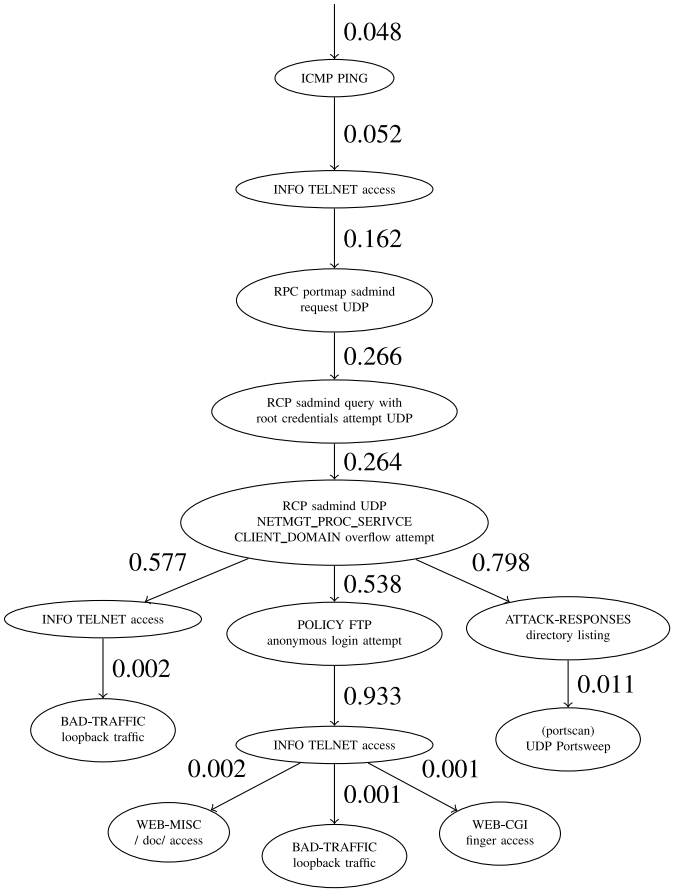

Fig. 3. Example of exploit-oriented attack graph with predictability values (inspired by [14]).

that comprise an attack. Edge values represent a probability, by which the event associated with the end node will happen. The edge value is referred to as predictability.

The predictions using attack graphs are based on traversing the graph and searching for a successful attack path, or on probability values of edges in the graph. Assuming a current attack is in a certain state according to the model, the node is marked as an initial state. From the initial state, all the possible paths may be traversed, e.g., using breadth-first search, and the ones leading to successful system compromise are selected as possible attack paths. The weights might be used to predict the most probable path. Alternatively, the most probable action of an attacker may be considered in each node, which might predict the immediate action of the attacker, but there the attack path may not lead to a successful compromise.

2) Literature Review: Attack graphs were the first method proposed for predicting cyber attacks, dating back to an essay by Hughes and Sheyner published in 2003 [11]. Many research papers that propose using the attack graphs, mostly for attack projection and intent recognition, were published in years 2005-2008. Recent additions are listed in this section.

In 2013, two alert correlation frameworks, in which prediction is involved, were proposed. Chung *et al.* [22] presented NICE, a system for countermeasure selection in virtual network systems, that uses attack graphs to model and project the attacks. Kotenko and Chechulin [23] presented CAMIAC, a system for cyber attack modeling and impact assessment, where the attack graphs are used in a similar way. However, both systems use attack projection as a part of a larger system, and the research works do not focus on it.

Another variant of attack graphs is a factor graph proposed by Cao *et al.* [24], [25] in 2014. A factor graph is a probabilistic graphical model consisting of random variables and factor functions. The authors compare it to Bayesian networks and Markov random fields and evaluate the use of factor graph for predicting attacks over a large dataset of real security incidents (several years of reports) with a promising accuracy of 75 %.

Ramaki *et al.* [26] in 2014 proposed RTECA (Real Time Episode Correlation Algorithm) for multi-step attack scenarios detection and prediction. The paper describes in details the theoretical and practical implications of designing such a tool. Although they propose leveraging attack graph, the authors extensively use causal correlations in their approach. Thus, in their later work, Ramaki *et al.* [32] dropped the attack graphs in favor of Bayesian networks (see Section IV-B for more details).

GhasemiGol *et al.* [27] in 2016 introduced an uncertainty-aware attack graph to evaluate network security state and a forecasting attack graph to estimate the risk of future attacks. The forecasting attack graph is built using several other graphs - uncertainty-aware attack graph, hyper-alerts graph (for alert correlation as in [48]), dependency graph, and response graph. Although the attack graphs and probabilities have to be predefined, they are continuously updated in reaction to incoming alerts. The authors describe the process of graph generation in details and provide an impressive amount of examples, illustrations, and algorithms, which makes the paper very interesting as an introductory paper to the field. The authors also used many tools proposed in earlier works to assess their usability. The same authors also proposed attack graph-based attack prediction as a part of their work on incident response management [28].

Polatidis *et al.* [29], [30] proposed an approach to cyber attack prediction using attack graphs and recommender systems. First, an attack graph is built using the information about infrastructure. Subsequently, a recommender system is used to predict cyber attacks using a collaborative filtering approach that the authors proposed earlier [49]. The papers include a case study of attack graph generation in critical infrastructure, specifically maritime supply chain.

B. Bayesian Networks

Another group of model-checking approach to attack prediction is using Bayesian networks. These methods are closely related to model-checking approaches based on attack graphs because a Bayesian network is typically constructed from an attack graph. The distinct feature of Bayesian networks are the conditional variables and probabilities that are reflected in the model. In some cases, further restrictions are set on Bayesian networks. For example, the requirement on the causality of events leads to using causal networks instead of generic Bayesian networks.

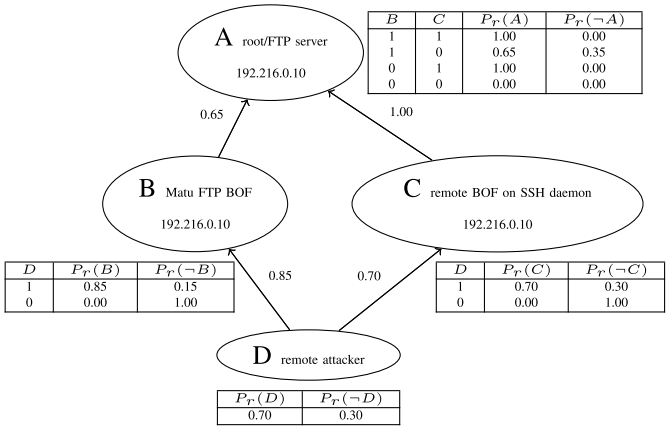

Fig. 4. Simple Bayesian Attack Graph illustrating probability computations (inspired by [50]).

1) Method Description: A Bayesian network is a probabilistic graphical model that represents the variables and the relationships between them. The network is a directed acyclic graph with nodes as the discrete or continuous random variables and edges as the relationships between them. The nodes maintain the states of the random variables and conditional probability form.

There are several equivalent definitions of a Bayesian network. Bayesian network is usually represented as a directed acyclic graph (DAG). Each node represents a variable that has a certain set of states. The edges represent the causal relationships between the nodes. Formally, let $G = (V, E)$ be a DAG, and let $X = (X_v)vV$ be a set of random variables indexed by V. A Bayesian Network consists of a set of variables and a set of direct edges between variables. Each variable has a finite set of mutually exclusive states. The variable and direct edge form a DAG. To each variable A with parents $B_1, B_2 \cdots B_n$, there is attached a conditional probability table $P(A|B_1, B_2 \cdots B_n)$.

An example of a Bayesian attack graph is shown in Figure 4 [50]. We can derive that the Bayesian network models an activity of an attacker (D), who is likely to use one of the buffer overflow exploits (B, C) to get access to a server (A). Probability tables are attached to each node informing us about the probability related to the exploit that the attacker will likely use and what is the probability of a successful exploit.

Further extensions or constraints are used for specific purposes, including cyber security. For example, Bayesian attack graphs is an attack graph in the form of the Bayesian network [32]. A causal network is a special case of a Bayesian network which explicitly requires the relationships in the network to be causal [12].

In order to create a Bayesian network or a Bayesian attack graph, the list of events, causal dependencies between events, and the probability of transitions between events are required. Building the model requires either expert knowledge, or it can be trained using data mining or machine learning. Typically, the probability tables are calculated from the training datasets or historical records. Structure learning, parameter learning, and unobserved variable inference are the main tasks of building the network.

Alert prediction using Bayesian networks or Bayesian attack graphs uses probabilities depicted in the model. The event with the highest posterior probabilities is the most probable to appear in the future. For practical purposes, a threshold is required to filter out predicted alerts with low probability. If the probability of the predicted event is higher than the threshold, the predicted event can be reported, and appropriate defense mechanisms can be set.

2) Literature Review: A fundamental contribution is research work by Qin and Lee from 2004 [12], which remain a recommended reading even today. The authors presented an approach to attack plan recognition and prediction of upcoming attacks based on predefined attack plans. According to their proposal, a causal network is constructed from low-level alerts. Subsequently, probabilistic inference is conducted to evaluate the likelihood of the next attack step. Their approach was evaluated using DARPA's Grand Challenge Problem datasets. However, only limited results are presented. A drawback of their work is that it requires a library of attack plans, from which the causal network is derived. Thus, input from a human expert is needed. The authors acknowledge this as a challenge for future work. They also stated that there is a need to distinguish between the deceptive plan and the real goal of the attack and also attacks conducted by one attacker and a group of collaborating attackers. These issues remain open research problems even today.

Similarly to the situation with attack graphs, methods based on Bayesian networks peaked in late 2000' and are not getting that much attention lately. Wu *et al.* [31] in 2012 proposed minor updates to building Bayesian networks from attack graphs for attack predictions. The authors propose to include the presence of vulnerabilities and three environmental factors into the Bayesian networks to reflect the potential impact of predicted attacks. The environmental factors are the value of assets in the network, the utilization of the host in the network, and the attack history. However, the research work only outlines the work and does not include any results.

Ramaki *et al.* [32] proposed a real-time alert correlation and prediction framework in 2015. The framework has two modes, online and offline. In the offline mode, a Bayesian attack graph is constructed from low-level alerts. In the online mode, the most probable next step of the attacker according to BAG is predicted. The authors evaluated their approach using the DARPA 2000 dataset. The accuracy of prediction was observed to be increasing with the length of the attack scenario. Thus, accuracy ranged from 92.3% when processing the first attack step to 99.2% when processing the fifth attack step.

Recently, Okutan *et al.* [33] included signals unrelated to the target network into the attack prediction method based on the Bayesian network. The signals are mentions of attacks on Twitter or the current number of attacks from Hackmageddon [51]. The results show that the prediction accuracy ranges from 63 % to 99 %, which makes it a promising approach.

Huang *et al.* [34] in 2018 involved attack prediction using the Bayesian network in their framework for assessing cyber attacks in cyber-physical systems. However, there are no

improvements to the prediction method itself; it is more of an application.

C. Markov Models

Another common approach to predicting attacks based on model-checking prediction methods is using Markov models. Markov models form a popular category of models, including well-known examples of Markov chains and Hidden Markov Models (HMM). Markov models are often represented as a graph, which makes methods based on them similar to the methods based on attack graphs and Bayesian networks. Contrary to previously described approaches, Markov models operate well in the presence of unobservable states and transitions, which removes the dependency of intrusion detection and attack prediction methods on possessing complete information. This allows for successful intrusion detection and attack prediction even if some attack steps were undetected or cannot be completely inferred.

1) Method Description: There are several variants of Markov models used for attack prediction, Hidden Markov models (HMM), Variable-length Markov models (VLMM), and Variable-order Markov models (VOMM). In this section, we show how to construct the model and predict an attack using an HMM. VLMM and VOMM, however, share the same theoretical background and their utilization for attack prediction is very similar. HMM is a statistical model where the system being modeled is assumed to be a Markov process with unobserved (hidden) states. Hence, we can not observe the state of a model directly, but only the outputs dependent on the current state.

Consider having attack sequences consisting of classes such as enumeration, host and service probing, exploitation, etc. These events may be detected by an IDS, and thus the alerts will be raised. From the perspective of HMMs, the alerts are observable outputs of attack classes. Keep in mind that not all the events can be detected by an IDS. In order to construct an HMM from the attack sequences, we need to determine the number of states in the model, the number of distinct observation symbols per state, the state transition probability distribution, and the initial state distribution [15]. The number of states is the number of attack classes. The observation symbols represent IDS alerts. State transition and observation probabilities are extracted from historical records or by an expert.

HMMs are often visualized as graphs. In cyber security, attack classes are the nodes, observation symbols are the edges, and the probabilities are weights of the edges. Figure 5 shows an example of HMM used for attack prediction [35]. We can see four states representing the attacker's progress from a normal state (nothing is happening) to a successful compromise.

When having a sequence of attack classes, there is a need to predict the next activity of an attacker, i.e., the next element in the sequence. Intuitively, there is a need to find the most likely path from the current state node. The most likely path provides a sequence of attack classes that are the predicted actions of the attacker. To eliminate false positives, it is recommended to set a probability threshold so that lower probabilities are discarded, and such paths are not considered for further actions [15].

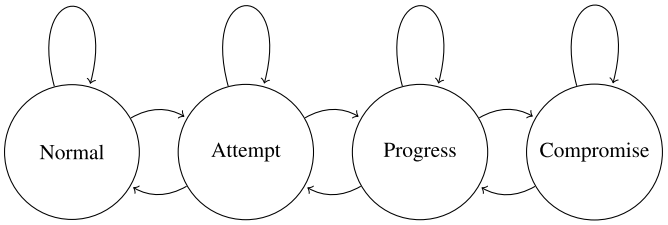

Fig. 5. Hidden Markov Model states for predicting cyber attacks (inspired by [35]).

2) Literature Review: The methods based on Markov models appeared along with the methods based on attack graphs and Bayesian networks in late 2000'. Farhadi *et al.* [15] in 2011 proposed a complex framework for alert correlation and prediction. In this work, sequential pattern mining is used to extract attack scenarios, which are then represented using a Hidden Markov model that is used for attack plan recognition. Authors claim that their work is the first to use an unsupervised method of attack plan recognition. Research works like this one are part of a trend in research on predictions in cyber security that overcomes a major drawback of previous works. Instead of relying on a predefined model constructed or supervised by a human expert, it incorporates unsupervised methods of data mining or machine learning. Thus, we selected this work as a recommended reading to illustrate this transition.

Sendi *et al.* [35] in 2012 proposed a method of intrusion prediction in real time that uses HMMs. The multi-step attacks are the prime interest in this work. An experimental evaluation shows how their method can predict multi-step attacks, which is especially useful for preventing the attacker from gaining control over more and more hosts in the network.

Shin *et al.* [36] in 2013 proposed an advanced probabilistic approach for network-based IDS (APAN), which uses a Markov chain to model unusual events in the network traffic and to forecast intrusion. Contrary to other methods based on Markov models, this method processes network anomalies and, thus, is not aiming at predicting the next move of an attacker like other model-checking approaches.

Zhang *et al.* [37] in 2014 discussed differences between trained and untrained Markov models as applied to detection and prediction of multi-step attacks. The authors first train the HMM by Baum-Welch algorithm. Consequently, attack scenario corresponding to an alert is found using a Forward algorithm. Finally, the next possible attack sequence is predicted using the Viterbi algorithm. The approach was evaluated using DARPA 2000 dataset. Trained HMMs scored better than their untrained counterparts in both recognition and prediction.

Kholidy *et al.* published a series of three papers on attack predictions in cloud systems in 2014. First, attack prediction models for intrusion detection systems in the cloud are proposed [38]. Subsequently, the utilization of finite state HMMs for predicting multi-stage attacks in the cloud is discussed [39]. Finally, the intrusion prediction model with finite context with a probabilistic suffix tree is described [40].

Abraham and Nair [41] proposed predictive cybersecurity framework based on Markov models for exploitability analysis. The authors use CVSS data to assess the lifecycle of vulnerabilities and predict their impact on the network.

Most recently, Bar *et al.* [42], [43] in 2016 used data from honeypots for complex modeling of attack propagation using Markov chains. Several frequent patterns of attack propagation were observed and described in details. However, the prediction of the next attacked honeypot is only briefly mentioned and left for future work.

D. Game Theory

Game-theoretical approaches to attack prediction are similar to the graphical model-checking approaches discussed earlier. The game is used as a model of interaction between an attacker and a defender. Contrary to the graphical model-checking approaches, game-theoretical methods aim to find the best strategy for the players instead of the most frequent attack progression observed in historical data. Thus, game-theoretical approaches seem promising especially for prediction of advanced attacker's activity.

1) Method Description: Game theory is a mathematical tool designed for analysis of an interaction between subjects with often conflicting objects. The basic assumptions in game theory are that participants are rational (they pursue their objectives) and that they reason strategically (they take into account their knowledge or expectations of other participants).

A game is a model of strategic interaction. The game consists of 1) a finite set N of players (usually attacker and defender/administrator in context of network security), 2) a nonempty set of actions A_i for each player $i \in N$, 3) a payoff function u_i for each player $i \in N$, that assigns each outcome $a \in \times_{j \in N} A_j$ a utility of player i.

A strategy of a player is a function that provides a player's action for each situation in which the player should make a decision. We distinguish between two types of strategies. Pure strategies provide a single action for each situation. By contrast, a mixed strategy assigns each situation a probability distribution over the set of player's actions. The concept of a *game solution* in game theory is not explicit. The most commonly used solution concept is a *Nash equilibrium* [52]. In Nash equilibrium, both players have chosen such strategies, which neither of them would benefit by deviating from his strategy. Finding the Nash equilibria of a game is often computationally intractable [53]. However, algorithms with lesser computational complexity approximating the Nash equilibria are available for some types of games [54], [55].

There are various classes of *game models* that can be used for attack prediction. One such classification distinguishes *extensive* vs. *strategic games*. In a game in strategic form, each player chooses his action only once, and the actions of all players are made simultaneously. By contrast, in games in extensive form, the players make the choice of action multiple (possibly infinitely many) times simultaneously or in turns and the players may include all available information in their decision at the time the decision is made.

Alternatively, we distinguish *games with imperfect vs. perfect information*. In extensive games with perfect information, at any stage of the game, all players are informed about each other's moves in previous turns. Contrary, if all information about past moves is not available to all player, the extensive form game is said to have imperfect information.

2) Literature Review: Lisý *et al.* [44] used a zero-sum game in extensive form with imperfect information to infer the attacker's plan in situations when the attacker tries to actively mislead the defender about his goals. They assume the targets and their respective value for the attacker are known as well as the set of all attack scenarios. Every round of the game, the attacker chooses an action, and the defender chooses a sensor from a given set of sensors. Each sensor has given the capability of detecting various attacker's actions. The attacker tries to reach the most valuable target while avoiding detection and misleading the defender about the ultimate goal. The defender tries to guess as many of the attacker's moves as possible. They present an algorithm to compute an approximation of the Nash equilibria. Another presented algorithm each turn identifies the most probable scenarios, thus enabling the defender to guess not only the attacker's next action but also his ultimate goal.

Píbil *et al.* [45] focus on predicting the target of the attacker rather than his next move. They consider the zero-sum finite game in extensive form with imperfect information between the attacker and defender. The defender selects the deployment of honeypots, mainly how valuable they appear to the attacker. The attacker chooses which target to attack. They consider two scenarios; in the first scenario, the attacker has no information other than the perceived value of the target, while in the second scenario the attacker can probe a few targets and receive noisy information of their type. The Nash equilibria of this game help the defender to best disguise the honeypots and the attacker to select which targets will he attack.

Abdlhamed *et al.* [9] in 2016 proposed a system for intrusion prediction in a cloud computing environment. Their system is designed to leverage the problem that theoretic models such as game theory can be highly unreliable with insufficient or uncertain input data. Their system first tries to match the situation to build attack models and scenarios. If the match is sufficient, the system assumes the situation is covered by the theoretical game theory based model and applies the model's prediction. In case the input data are not sufficient, statistical methods are applied for prediction. Thus, this work poses as an example of using a combination of different approaches.

V. Methods Based on Continuous Models

The second group of methods is using continuous models, namely time series and grey models, as discussed in appropriate subsections. Such approaches are in most cases suitable for forecasting network security situation. Common results are forecasts of the numbers, volumes, and composition of attacks in the network and their distribution in time. Alternatively, spatiotemporal patterns in time series may be used to predict cyber attacks. A summary of methods and research papers can be found in Table III.

TABLE III
COMPARISON OF PREDICTION METHODS, PART II – APPROACHES BASED ON CONTINUOUS MODELS

Time series (Section V-A)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Park et al. [56] (FORE)	2012	Time series and linear regression	Live	1.8 time faster reaction to worms
Zhan et al. [57]	2013	Time series (FARIMA)	Live (honeypot)	Attack predictions up to 5 hours ahead
Silva et al. [58]	2014	Time series (PBRS/EWMA)	Live (honeynet)	up to 57.8 % accuracy, limited to burst attacks (brute-forcing and DDoS)
Abdullah, Pillai et al. [59], [60]	2015	Time series (GARMA + ARMA)	Live data (honeynet)	Limited set of atack types considered
Freudiger et al. [61]	2015	Time series (EWMA)	Dshield	Collaborative blacklisting
Chen et al. [62]	2015	Spatiotemporal patterns	Live (honeynet)	Discussison of found attack patterns
Zhan et al. [63]	2015	Time series (FARIM + GARCH) + Extreme values	Live (honeypot)	70 %–87.9 % accuracy
Sokol et al. [64]	2017	Time series (AR(1))	Live (honeynet)	95 % certainty, finding simple models
Werner et al. [65]	2017	Time series (ARIMA)	Hackmageddon	14.1 %–21.2 % accuracy
Dowling et al. [66]	2017	Temporal variances	Live (honeynet)	Attack type predictability
Okutan et al. [67]	2017	Time series (ARIMA)	Live data (anonymized)	Unconventional resources (Twitter, etc.)
Grey Models (Section V-B)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Lin et al. [68]	2014	Grey models	DARPA 1998	Supported by immunity model
Leau and Manickam [69], [70]	2016	Grey models	DARPA 1999 & 2000	More robust than standard grey models

A. Time Series

Time series pose a very interesting tool for predictive analysis, that is used in various fields, including cyber security. It is worth mentioning that time series are commonly used in anomaly detection. A time series represent common network traffic patterns. Subsequently, the deviations that do not match with the expected values of network traffic in a given moment is proclaimed as an anomaly. Although the terminology and methods of anomaly detection are similar to attack prediction, the two use cases are substantially different. Hence, research on anomaly detection is not presented here.

1) Method Description: A time series is a set of consecutive data points indexed in time order, often plotted in line charts. A time series is constructed from historical records of an observed phenomenon; in our case, it can be attacker's activity or a network security situation state represented in a numerical value. There are a plethora of methods for dealing with time series analysis that can be used to predict the values of a time series in the near future. A significant number of approaches employ moving average, a calculation to analyze the data by creating a series of averages of subsets of the time series. Variants of moving average analyses include simple moving averages (SMA) [9] or exponential weighted moving average (EWMA) [58], [61]. The weights and exponential smoothing allow a prediction method to better reflect the nature of the input time series, e.g., seasonality of network traffic (day-night differences, etc.). A recent trend is using autoregressive moving averages (ARMA, ARIMA) [65], [67]. See Figure 6 for an example of time series forecasting with moving average and forecasting confidence limits.

2) Literature Review: Using time series for cyber attack prediction and forecasting is a somewhat recent idea, compared to other approaches. A precursor to time series methods appeared in 2012 when Park *et al.* [56] proposed FORE, a mechanism for predicting "cyber weather" using regression analysis. The tasks of FORE is to forecast unknown Internet worms by analyzing the randomness in the network traffic. The concept of the work is that the presence of work in the network

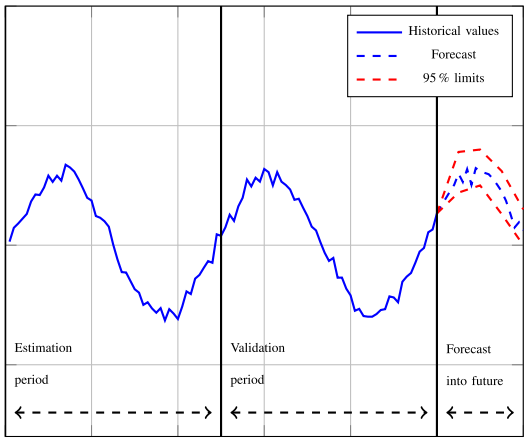

Fig. 6. Time series forecasting with moving average.

traffic increases network traffic randomness. The forecasts are based on time series analysis and linear regression.

From there on, Zhan *et al.* [57] proposed a statistical framework based on time series analysis of honeypot data in 2013. In 2014, Silva *et al.* [58] created a model for predicting burst attacks, i.e., brute-forcing and DoS, that is based on time series. The authors compared pseudo-random binary sequences (PBRS) and exponential weighted moving average (EWMA) to predict the beginning of bursts. In an evaluation using a honeynet, it was shown that the attacks could be predicted with an accuracy ranging from 17.4 % to 57.8 % with a moving average of around 5-10 hours. Many research papers appeared in 2015. Abdullah *et al.* [59] and Pillai *et al.* [60] proposed using GARMA and ARMA time series evaluated on live data from a honeynet. Freudiger *et al.* [61] worked on controlled data sharing that would lead to collaborative predictive blacklisting. Part of this contribution proposed the use of EWMA time series for predictions and evaluation on Dshield data. Chen *et al.* [62] relied on time series in their work on predicting cyber attacks using spatiotemporal patterns. Zhan *et al.* compared long-term and short-term predictions of cyber attacks

using time series (FARIMA and GARCH) and extreme values with interesting results, up to 87.9 % prediction accuracy was achieved 1 hour ahead of time of an attack. In 2017, Werner *et al.* [65] used ARIMA time series to predict the intensity of cyber attacks, i.e., expected number of attacks in the next day. Sokol and Gajdoš [64] used AR(1) model to predict attacks against a honeynet. A similar yet simplistic method using random sampling in temporal variance was proposed by Dowling *et al.* [66] to attack type predictability. Recent work by Okutan *et al.* [67] uses a broad range of unconventional signals, such as Twitter events, to improve forecasting of security incidents using a time series and ARIMA model.

Time series were already mentioned in Section IV-D, where a combined approach using game theory and supported by time series analysis was presented [9]. Machine learning methods (see Section VI) may also use time series to train classifiers [71].

B. Grey Models

The Grey Models are typically used for predicting cyber security situations and define yet another example of methodologies which employ a continuous mathematical model. The Grey Theory was first presented by Ju-Long in 1982 [72]. In a grey theory terminology, a situation with no information is defined as black and a situation with complete information as white. Since both options are idealized, the real world problems are somewhere in the middle, in a situation defined as grey. Thus, a grey situation can be modeled using a Grey Model (GM).

1) Method Description: The most widely used grey forecasting models are *GM*(1, 1) and its modification Grey-Verhulst model. The forecasting ability of these models is limited to predicting next members of a time series. It is most suitable for short-term prediction based on a small sample of data. In network security, authors usually measure the network security situation and predict its next value.

Let $X^0 = \{x^0(1), \ldots, x^0(n)\}$ be a sequence of length n whose next value will be predicted, usually a time series. First the Accumulating Generation Operation (1-AGO) is applied and new sequence $X^1 = \{x^1(1), \ldots, x^1(n)\}$ is created, where $x^1(k) = \sum_{i=1}^{k} x^0(i)$. By applying accumulation operation, the influence of random fluctuations present in the original sequence is weakened. Moreover the original sequence can be easily reconstructed as $x^0(k) = x^1(k) - x^1(k-1)$ for $k > 1$, $x^0(1) = x^1(1)$.

The model is created for the sequence X^1. Different modifications use different models. The original *GM*(1, 1) model assumes the data satisfy the differential equation

$$\frac{dx^1(k)}{dk} + ax^1(k) = b.$$

The model works best for data with exponential growth. The Grey-Verhulst model, which is more appropriate for data following S-curve [73] assumes a differential equation

$$\frac{dx^1(k)}{dk} + ax^1(k) = b\left[x^1(k)\right]^2$$

The model parameters a, b are estimated using least squares method from the sample data. The solution of the differential equation $\widehat{x}^1(k)$ is computed and the future values of the sequence X^0 are predicted as $\widehat{x}^0(k+1) = \widehat{x}^1(k+1) - \widehat{x}^1(k)$ for $k \geq n$. The various methods based on Grey model usually use modified model or extend the model on error prediction.

2) Literature Review: Preliminary work on network security situation forecasting using Grey models from 2006 to 2014 is covered in a survey by Leau and Manickam [6]. Thus, we only surveyed later research works.

In 2014, Lin *et al.* [68] introduced their definition of the network security situation. They claim the network defense is similar to an immunity system; the severity of a situation is proportional to the strength of the response. The authors compute the network security situation based on the number of defensive measures currently in place. They improve the prediction by considering various factors, that influence network security situation. The most influential factors are selected using the method of grey entropy correlation analysis, and the Kalman filter is applied to improve the prediction.

In 2016, Leau and Manickam [69] endeavor to overcome the limitations of *GM*(1, 1) and Grey-Verhulst models, namely that they are accurate only for specific input series. In their work, they introduce an adaptive Grey-Verhulst model that is robust as applied to wider types of time series. The modification consists of an extension of the underlining Grey-Verhulst model. While the original model from which the differential equation is derived assumes that $x^0(k) + az^1(k) = b(z^1(k))^2$, where $z^1(k) = \frac{1}{2}x^1(k) + \frac{1}{2}x^1(k-1)$, the modified version assumes $z^1(k) = x^1(k-1) + \frac{1}{2}x^0(k) + \frac{1}{6}x^0(k-1) - \frac{1}{6}x^0(k-2)$. The value of $z^1(k)$ is derived so that the error due to different shapes of the original time series is reduced as much as possible. The same authors also introduce [70] an adaptive Grey-Verhulst-Kalman prediction model, which utilizes the adaptive Grey-Verhulst model from their previous work and improves it by applying the Kalman filter to predict the next residuum, thus increasing the prediction accuracy.

VI. Machine Learning and Data Mining Methods

Machine learning (ML) is gaining popularity in the research community in wide areas of exploration, and cyber security is no exception [89]. It contains a vast landscape of approaches and methods, such as neural networks and support vector machines, which makes it difficult to properly categorize machine learning in terms of attack prediction methods. Machine learning is closely tied to data mining [89], which was already mentioned several times in this work. Typically, data mining was exploited to create a model used in attack prediction, e.g., an attack graph [14] and a Markov model [15]. The utilization of data mining in this context is intended to overcome a major drawback of model-based attack prediction models, i.e., the dependency on models provided by a security expert [3]. However, data mining does not directly influence the method itself. Thus, in this section, we only list approaches that make direct use of machine learning. Methods that are only supported by machine learning or data mining are discussed in other sections.

TABLE IV
COMPARISON OF PREDICTION METHODS, PART III – APPROACHES BASED ON MACHINE LEARNING AND DATA MINING

Neural Networks (Section VI-B1)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Zheng et al. [74]	2012	BP neural network	KDD99	Modular system, very brief discussion
Chen et al. [75]	2013	Recurrent neural network	Live (honeypot)	Old data (2000-2001)
Zhang et al. [76]	2013	BP and RBF neural networks	Custom dataset	84.2-85.42 % accuracy, BP faster than RBF
Xing-zhu [77]	2016	RBF Neural network	DARPA 1998	Intrusion prediction
Zhang et al. [78]	2016	Wavelet neural network	Testbed	Optimized by genetic algorithms
He et al. [79]	2017	Wavelet neural network	DARPA (not specified)	Minor improvements, discusses drawbacks
Support Vector Machines (Section VI-B2)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Cheng and Lang [80]	2012	Support Vector Machine	Live	Alternative to NSSA forecasting based on neural networks
Jayasinghe et al. [81]	2014	Support Vector Machine	Live (webpages)	Limited to drive-by download attacks
Uwagbole et al. [82], [83]	2017	Support Vector Machine	Custom dataset	Limited to SQL injection attacks
Data Mining (Section VI-B3)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Fachkha et al. [84]	2012	Frequent pattern mining, association rule mining	CAIDA network telescope	Global scope given by CAIDA's network telescope size
Kim and Park [85] (CARMA)	2014	Sequence mining	Live	Thorough reasoning behind the results
Husák and Kašpar [86]	2018	Sequential rule mining	Live (alert sharing platform)	Collaborative environment, timing discussed
Other Machine Learning Methods (Section VI-B4)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Soska and Christin [87]	2014	Decision-tree classifiers	Live	detects websites that will turn malicious, 66 % TP and 17 % FP rate
Liu et al. [71]	2015	Random forest classifier	VERIS database, Hackmageddon, Web Hacking Incident Database	data breach forecasting, 258 features, 90 % TP and 10 % FP rate
Shao et al. [18]	2016	Rule mining, clustering	Proof-of-concept	User behavior analysis, identification of potentially problematic user groups
Veeramachaneni et al. [88] (AI^2)	2016	Combination of supervised and unsupervised methods	Live	Improved detection rates compared to unsupervised methods alone

A. Method Description

There is a number of approaches and methods of machine learning that can be used to predict future events such as cyber attacks. Thus, we describe the basics of neural networks herein as they are the most often used machine learning method derived from the surveyed papers. Neural networks were prominent at the initial rise of machine learning but were later replaced by Support Vector Machines (SVM) that offered lower computational complexity and shorter learning times. However, with the novel findings, the neural networks are once again gaining on popularity [89]. Readers that are interested in more details related to machine learning applications in cyber security are kindly referred to a survey by Buczak and Guven [89].

There are common steps in applying machine learning methods. Usually, it consists of two phases, training and testing. During the training phase, appropriate examples from the learning dataset are learned. Consequently, in the testing phase, new data are processed by the model and the machine learning method produces results, such as predicted continuations of attack sequences. In practice, however, there is also a validation phase between the training and testing. In the validation phase, another dataset is used to evaluate how well was the model trained or which of the models should be used for testing. For example, several neural networks may be constructed in the learning phase, each with a different number of layers and nodes, which differ in the prediction accuracy and effectiveness. An important aspect of machine learning is supervision. Either a model is trained autonomously and thus is referred to as unsupervised *unsupervised*, or the input data are fully or partially labeled by a human expert and thus dubbed as *supervised* or *semi-supervised* learning. The problem of identifying the classes and class attributes in the data, i.e., inputs of the machine learning methods, is known as *feature extraction* [89].

Artificial neural network (ANN) is a form of distributed computing inspired by biological neural networks, i.e., neurons in a brain. It is composed of simple processing units and synapses between them. It is common to visualize ANN in a graph as illustrated in Figure 7, where nodes are units and edges are synapses. A subset of units acts as input nodes and another subset as output nodes. The remaining nodes receive the signals transmitted from their input nodes, process the signals, and transmit it to their output nodes. The nodes can be weighted, and the whole network is typically structured in layers. Further, the nodes may have their own state or a threshold, which retransmits only the signals of a given level. The weights, thresholds, and synapses are established during the learning phase and may vary as the learning proceeds. The inputs are sent as signals to the input nodes, and the output nodes then provide the results.

B. Literature Review

The literature review of machine learning and data mining methods was structured as follows. Three subsections are dedicated to methods that were used in multiple research works. Those are neural networks, support vector machines, and data mining. The remaining research works are discussed after

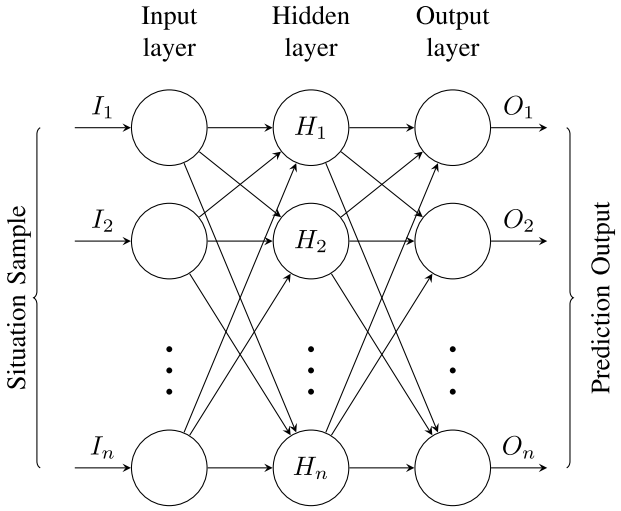

Fig. 7. Artificial neural network for network security situation prediction (inspired by [90]).

that. It is hard to properly categorize this group of methods, because of frequent combinations of approaches or uniquely used approach.

1) Neural Networks: A number of papers deal with the application of machine learning to predict network security situation for the needs of NSSA. These papers are rather short and focus on the theoretical background of NSSA modeling and forecasting, such as the mathematical formalization of the problem. However, the proposed approaches are rarely supported by experimental evaluation and, thus, provide limited value for security practitioners. Nevertheless, the common statement that NSSA is of vital interest is unquestionable. Various types of neural networks are discussed in these papers, and herein, a summary is subsequently provided for completeness purposes. The first papers started to appear in 2008, and the work continues till now. In 2012, Zheng *et al.* [74] discussed using back-propagation neural networks. Zhang *et al.* [76] in 2013 compared back-propagation and radial basis function neural networks and Chen *et al.* [75] proposed using small-world echo state network, which is a kind of recurrent neural network. Zhang *et al.* [78] proposed using wavelet neural networks in 2016. Most recently, He *et al.* [79] proposed using a mixed wavelet-based neural network.

Neural networks were also used for intrusion prediction in 2016 by Xing-Zhu [77]. The research work is, in essence, similar to the works on network security situation forecasting, only the motivation is focused more towards predicting particular intrusion.

2) Support Vector Machine: Cheng and Lang [80] suggested using support vector regression machine to forecast network security situation, although this work mostly presents an alternative to the neural network-based methods. Apart from a different classifier, their work is, in essence, similar to research performed in this field using neural networks.

Support vector machines proved suitable for predicting very specific attacks. Jayasinghe *et al.* [81] in 2014 predicted drive-by downloads by monitoring and analyzing bytecode stream produced by a Web browser. Uwagbole *et al.* [82] in 2017 proposed a predictive system based on machine learning to predict SQL injection attacks. The system uses SVM to classify Web request so that the SQL injection can be predicted before the Web page starts a malicious database query. The work is accompanied by another paper on generating corpus a for the learning phase [83].

3) Data Mining: Fachkha *et al.* [84] in 2012 investigated the data from darknet, a large unassigned IP address space, to profile the darknet traffic and corresponding cyber threats. Frequent pattern mining and association rule mining were used to find hidden correlations between events in darknet traffic. The found patterns and rules are then proposed to be used for predicting events in the darknet traffic and cyber threats in general. Due to the nature of the darknet, in this case, CAIDA darknet that represents 1/256 of the IPv4 address space, the results of such threat prediction have global scope.

Kim and Park [85] in 2014 used data mining to build the attack graph for attack prediction. The authors used sequential association rule mining to reflect the order of events. Although the paper indicates that the mined sequences are used for constructing the attack graph, the paper does not particularly specify how is this actually done but rather focus on the sequence mining. Thus, it was not categorized under attack graph-based models in Section IV-A. Sequence mining was also used in recent work by Husák and Kašpar [86], in which the authors mined sequential rules from cyber security alerts contained in a large-scale alert sharing platform. Contrary to [85], the emphasis was put on analyzing live data from real networks and evaluating the suitability of such an approach in practice.

4) Other Machine Learning Methods: In 2014, Soska and Christin [87] used machine learning to automatically detect vulnerable websites before they turn malicious. Traffic statistics, filesystem structure, and website content were used to train an ensemble of decision-tree classifiers. The authors performed a year-long evaluation with promising results of 66% true positive rate and 17% false positive rate, which is a good result among methods evaluated in practice.

Liu *et al.* [71] in 2015 characterized the extent to which cyber security incidents can be predicted. The research work is focused on data breaches, which are predicted using a random forest classifier against more than 1,000 real data breaches. The number of features used for training the classifier is remarkable, 258 features were collected from organizations' networks. The features either describe mismanagement symptoms (misconfigured DNS, BGP, etc.) or malicious activity time series (spam, phishing, network scans, etc.). The resulting 90% true positive rate and 10% false positive rate only underline the extent of this work. Due to the significant extent of the work, we list this work as a recommended reading.

Veeramachaneni *et al.* [88] in 2016 presented AI^2, a machine learning system for attack prediction that includes human input. First, the first authors use an ensemble of unsupervised outlier detection methods, including principal component analysis and autoencoders. Subsequently, feedback from an analyst is obtained and supervised learning module

TABLE V
COMPARISON OF PREDICTION METHODS, PART IV – OTHER APPROACHES

Similarity-based approaches (Section VII-1)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Jantan et al. [91], Rasmi et al. [92]	2012, 2013	Similarity	Proof-of-concept	Reduced time and cost of intention recognition in network forensics
AlEroud and Karabatis [93], [94]	2014, 2017	Semantic links and similarity, Contextual relationships	Synthetic dataset (IP flows), DARPA (not specified)	Supported by machine learning, missing temporal aspects
Jiang et al. [95]	2016	Similarity	Live (honeynet)	Supported by data mining
AlEroud and Alsmadi [96]	2017	Similarity	Testbed (SDN)	Evaluation limited to DoS prediction
DDoS volume forecasting (Section VII-2)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Kwon et al. [97], [98]	2012, 2017	Regression analysis and other statistical methods	Live (honeypots)	Framework was proposed first, methods were added later
Fachkha et al. [99]	2013	Time series, liner regression	CAIDA network telescope	Backscatter analysis – global scope
Olabelurin et al. [100]	2015	Entropy forecasting	Testbed	Low false positive rate – 22.5%
Evolutionary computing (Section VII-3)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Hu et al. [101], [102], Wei et al. [103]	2016-2017	Belief rule base model, evolutionary computing	Proof-of-concept	Possible alternative to grey models for network security situation prediction
Predictions based on unconventional data sources (Section VII-4)				
Authors	**Year**	**Approach/Model**	**Evaluation**	**Advantages and Limitations**
Mahjoub and Mathew [104] (SPRank)	2015	DNS anomalies	Live	Practical implementation, not a research paper
Hernandez et al. [16]	2016	Twitter sentiment analysis, linear regression	Live (Twitter)	Thorough evaluation on real-world events
Dalton et al. [105]	2017	Information foraging in publicly available data	Hackmageddon	Only suggests improvements to existing methods
Shu et al. [17]	2018	Twitter sentiment analysis, logistic regression	Live (Twitter)	Claims to predict attack, including its type, against a particular target

is used. The model is constantly refined as more feedback is gathered, which leads to promising results. The AI^2 improves the detection rate more than three times on average while reducing false positive rate fivefold, compared to unsupervised methods alone.

Shao *et al.* [18] in 2016 used user behavior analysis to predict cyber attacks with a motivation to include the reasoning behind the attacks. User security rating is derived from his/her consistency (usage patterns), accuracy (frequency of mistakes), and constancy (how long the user displays good online behavior). Rule mining is then used to find hidden relations in the behavior patterns. Finally, unsupervised clustering, such as k-means, and manual filtration of the results are used to identify groups of users that are prone to malicious operations.

VII. OTHER APPROACHES

In this section, we discuss the fourth group of prediction methods, methods that are hard to categorize properly or that are highly specialized in terms of a use case or a method used. The full list of approaches and papers is presented in Table V. There is no common background to these methods, so we only provide the literature review, and briefly explain the background there.

A. Similarity-Based Approaches

The first of the alternative approaches is based on similarity, mostly addressing the problem of attacker's intention recognition by calculating a similarity metric with a previously observed attack. In 2012, Jantan *et al.* [91] and Rasmi and Jantan [92] proposed a model of attack strategy that allows comparisons of the attack strategies. The observed security alerts are expressed numerically, and cosine similarity is applied to infer a similarity between two attack strategies. It is worth mentioning that the same authors have previously developed models based on Bayesian networks [106].

In 2014, AlEroud and Karabatis [93] proposed an approach to detect cyber attacks using semantic link network (SLN), which utilizes contextual information of network flows and alerts raised in response to them. Subsequently, SLN is used to predict and detect malicious flows, focusing on multi-step attacks, using similarity measures. The same authors recently published a novel approach [94] based on contextual relationships between cyber attacks and calculating their similarity.

In 2016, Jiang *et al.* [95] proposed an intrusion prediction mechanism based on honeypot log similarity. System logs from honeypots were first analyzed using association rule mining to find useful implicit information and to select features. Subsequently, the flows are mapped into metric space, and distance calculation is used to identify flows that are most similar to the known malicious flows, thus adding them to the prediction list. This approach aims at reducing false positive alarms and was evaluated in a live environment of a Taiwanese academic network.

Recently, AlEroud and Alsmadi [96] used similarity to predict and mitigate attacks in software-defined networks. The network traffic is aggregated to flows, and the flows' characteristics are subsequently compared to flow signatures of known attacks. If a similarity is found between known malicious flows and current flows, it is possible to predict a continuation of the traffic and mitigate the attack.

B. DDoS Volume Forecasting

Deeply studied topics are the DDoS attacks and predictions related to them. The predictions of DDoS attacks focuses mostly on identifying the initial phase of an attack, in which the volume of bogus network traffic rises, and the prediction of the volume of the attack. The volume of a DDoS attack is the most important feature of such attacks. The metrics for DDoS volume are packet or byte rate per second and the estimated number of compromised machines involved in the attack. Knowing the attack volume in advance tells us whether the target system or the network can withstand the attack or if there is enough capacity for defense, e.g., in scrubbing centers.

Since 2012, several authors have proposed their methods of DDoS forecasting. Kwon *et al.* [97] used honeynets to capture the initial phases of the DDoS attack and predict its size. Later, they used statistical approaches to predict the DDoS volume [98]. Fachkha *et al.* [99] proposed an approach based on analysis of data from darknets. Olabelurin *et al.* [100] improved the forecasting techniques by including entropy in the calculations.

C. Evolutionary Computing

A very recent approach to forecast network security situation is based on belief rule base (BRB) models and evolutionary algorithms, namely CMA-ES. This approach emerged in 2016, and was since then described and continuously improved by Hu *et al.* [101], [102] and Wei *et al.* [103], including the improvements in network security situation assessment [107]. BRB model includes a series of belief rules and can be built from expert knowledge as well as historical data. These might be subjective and inaccurate. Subsequently, the covariance matrix adaption evolution strategy (CMA-ES) is used to optimize the models the parameters of BRB model, which can then forecast network security situation. This novel approach seems very promising and might be a good alternative to grey models, that were used for the same purpose, as discussed in Section V-B. Nevertheless, this method is too novel, so that we cannot compare its impact, e.g., by a number of citations.

D. Unconventional Data Sources

A novel trend in cyber security predictions is using unconventional data sources. For example, using DNS logs for attack prediction is present in work by Mahjoub and Mathew [104] from 2015, who proposed a principle called Spike Rank or SPRank, that detects domains showing a sudden spike in DNS queries issued from millions of clients worldwide towards OpenDNS resolvers. The spikes were able to detect several malware campaigns as well as phishing campaigns.

In addition, even non-technical data sources were considered for cyber attack prediction. Hernández *et al.* [16] in 2016 performed sentiment analysis on Twitter to predict cyber attacks. Sentiment analysis of social networks was also a data source for Shu *et al.* [17] in 2018. Information foraging for improving cyber attack predictions was also discussed by Dalton *et al.* [105] in 2017. The authors, however, discuss various strategies for information foraging and only briefly mention the data sources with which they work.

VIII. Evaluation and Lessons Learned

In this section, we evaluate the findings from the literature review, and we answer the questions stated in the introduction. In the first question, we were interested in what can be predicted in the cyber security domain. Although many use cases were proposed, they can be reduced to several main use cases, namely, attack projection and intent recognition, attack or intrusion prediction, and security situation forecasting. These were already described in details in Section II. The remaining questions are summed up and answered in the following subsection. First, we sum up the practical implications, i.e., how ready are the attack prediction methods to effectively mitigate the attacks. Further, we take a closer look at the evaluation of predictions and forecasts in cyber security. A separate subsection is dedicated to metrics as there appeared to be more approaches to set an evaluating set of metric. Finally, we sum up open and resolved problems in the field.

A. Practical Implications

Regarding the practical implications, the prime issues are the accuracy and efficiency of predictions, but it is hard to evaluate and compare the methods. Even setting the right metrics is a problem as we have discussed further in this section. However, high prediction accuracy is a good indicator of a method's usability in practice. As we inferred in the literature review, there are many approaches that achieved high accuracies of over than 90 % [15], [26], [32]. However, such results were obtained when evaluating the approaches over datasets. When we take a look at methods evaluated on live network traffic, the prediction accuracies drop down to around 60–70 % [25], [33], [58], [63]. Some works show even worse results, which indicates that the prediction accuracy in practice is at the lower bounds.

Other practical aspects of predictions in practice are the time criteria, namely the time needed to predict future events and the time that remains to the predicted event. While older works focused on the computational complexity of the prediction algorithms, the field reports are scarce. However, modern approaches are implemented to operate in real time with minimal time delay [32], which effectively solves the problem. Nevertheless, there is a need to find out how much time there is to react to a predicted attack. Kholidy *et al.* [38]–[40] claim that they can predict an attack forthcoming in 39 minutes, which is a promising result that leaves enough time even for manual inspection of the predicted event. However, there are no other works using the same metrics.

There are two other major issues common to many methods, populating the knowledge base of the attacks and placing attack prediction at the most suitable level of abstraction [3]. First, attack prediction methods require either a library of attack plans completed by experts or a dataset of historical records, from which the attack plans might be constructed. Although both approaches are prone to errors and missing attack descriptions, the use of machine learning and data mining for model construction or direct prediction has prevailed in recent years. However, if an automatically found attack plan is going to be used in practice, one has to be

careful to manually inspect the results. Second, it is computationally demanding to implement attack prediction at the network level, e.g., as part of an IDS. Working with alerts from IDS is much more scalable and flexible than working with packets or network flows. Additionally, it is convenient to combine alerts from multiple IDS, e.g., a network-based and host-based, to get the complete trace of the attack. However, correlating alerts from heterogeneous sources adds additional complexity and stands as a research problem of its own [108].

Suthaharan [109] states that the network intrusion detection and prediction are time sensitive applications requiring highly efficient Big Data techniques to tackle the problem on the fly. Thus, it is proven that the data fall into the category of big data. However, a new definition of big data is provided based on three new parameters, cardinality, continuity, and complexity, instead of traditional volume, variety, and velocity. Further, the suitability of machine learning for big data is discussed. Although methods based on Support Vector Machines provide excellent accuracies, yet they are not suitable for big Data due to their computational complexity. Representational learning might be suitable for big data classification, but Machine Lifelong Learning is recommended to be used.

B. Datasets

During the literature search, we encountered several datasets that were often used for evaluation of the proposed methods. The most popular datasets were produced by MIT Lincoln Labs and are generally recognized as the DARPA datasets [110], [111]. There are three distinct datasets available: DARPA 1998, DARPA 1999, and DARPA 2000. DARPA 2000 further contains two attack scenarios, LLDOS 1.0 and LLDOS 2.0.2; often only LLDOS 1.0 was used in attack prediction method evaluations. Although the dataset is popular and well documented, its main problem is its age; almost 20 years old dataset does not reflect current cyber security threats and network traffic patterns.

ACM SIGKDD announced KDD Cup 1999 [112], a contest on knowledge discovery from the cyber security data. In this contest, DARPA 1998 dataset was used, although many authors referenced the dataset as the KDD 1999 dataset. The KDD Cup 1999 gained a lot of attention from numerous researchers on the problem of intrusion detection as well as attack prediction, thus allowing further comparisons of various methods. However, substantial flaws in the dataset were revealed in a thorough evaluation [113]. Thus, the dataset is now considered unreliable and even harmful by the community, although attempts for improving the dataset quality were made [114]. Still, the dataset is used even in recent works [9], [77].

Other datasets public datasets are used scarcely; the researchers often crafted their own datasets [76] and evaluated their proposed methods using these data. While some data are obtained from real network traffic, which provides fresh data, nevertheless it is quite problematic to publish such data due to the needs of data anonymization. Another common option is to design a testbed [22], [41], [100], which is often laborious to set up, even if a proper description is provided. Thus, custom datasets and testbeds seem suitable for evaluating the proposed methods, but the reproducibility of such research is often disputable.

There is one more common problem related to many datasets used for evaluating methods of attack prediction, and that is that the datasets are not designed for the purpose of evaluating attack prediction. As Fava *et al.* stated back in 2008 [115], commonly known datasets, including the DARPA datasets, are crafted for intrusion detection and, thus, do not have the notion of attack tracks, i.e., there is no information available on the attackers' intentions or correlation of attack steps. Thus, we can only confirm the accuracy of predicting the next attacker's move, but we cannot confirm or discard the predicted attack plan.

C. Evaluation in Live Network

Evaluation of attack prediction in real-life scenarios is challenging. It is hazardous to let the adversary execute an intrusion in a real network only to evaluate the predictions. In large networks, it is also problematic to get access to every host that could be compromised. Nevertheless, several live data sources were used, such as the data from DShield [116], a collaborative database of firewall logs, and Hackmageddon [51], a compilation of cyber attack timelines and statistics. Very often, researchers set up a honeypot to capture cyber security data and use them to evaluate predictions. The main advantage of honeypots is that they typically contain only malicious data. However, they are not useful for studying advanced attackers for the purpose of attack intention recognition. Finally, darknets, large unassigned IP blacks, such as CAIDA network telescope, were used for prediction in a global scale [84], [99].

In addition, the research on attack projection is often accompanied by research on deception and network traffic manipulation. The aim of deception in cyber security is to guide the adversary to the target of defender's choice, typically a honeypot. Several researchers [117] continued their work on attack prediction by proposing a deception system, which prepares an attractive target for an attacker. For example, if an adversary is supposed to exploit a certain service, a honeypot emulating such service is set up in the target network, either as a new target or as a clone of a real system. If the predictions are correct and the honeypot setup is quick enough, the attacker would exploit a honeypot, and the attack can be studied. Manipulating the terrain for the attacker was problematic mostly due to the need for rapid deployment of honeypots and movement of targets as traffic manipulation was too costly. However, recent development in networking, namely in Software Defined Networks (SDN), allowed easy traffic manipulation. The emerging field of SDN thus began producing security-related frameworks focusing on early-stage attack mitigation and traffic redirection, e.g., diverting the attack traffic to a honeypot instead of the original target. AVANT-GUARD [118] is one of the early examples. Combining such framework with attack prediction have been

proposed recently [96], and we expect more work on this topic in near future.

D. Metrics

Setting the metrics to evaluate and compare attack prediction methods is a challenging task. Naturally, we are interested in the prediction accuracy as a prime indicator, but that may rely on a given context and specific use case. In practical setups, we encountered the time criteria, such as prediction efficiency and the time remaining to the predicted event. Specific tasks, such as predictions based on specific attack traits, require specific metrics. In this section, we summarize and evaluate the metrics that are typically used in the literature.

The most important metric for evaluating prediction methods is their accuracy. As we have seen in many surveyed papers, the authors often include the accuracy as the percentage of successfully predicted events or situations. However, accuracy can be understood broadly and not all the papers use it in a formal sense. Often, we can see confusion matrix as a more descriptive metric of a prediction method. The confusion matrix is used for the evaluation of intrusion detection. Hence it is natural to use it in to evaluate prediction in cyber security as well. However, there are several issues with the use of confusion matrices. First, all the elements can be obtained when evaluating a method over an annotated dataset, but we can never be sure about the results when evaluating the methods over live network data. Second, different methods may use different criteria for true and false positives and negatives. For example, if a certain exploit is predicted to happen at a certain time on a specific host, but the attacker exploits another target or the time of the attack is significantly different, it is quite unclear whether we should consider such events as true positives. Finally, in predictive analytics and other fields of research, precision and recall values are often used instead of the full confusion matrix, but calculated from it. Precision is defined as tp / ($tp + fp$), while recall as tp / ($tp + fn$). Precision and recall are favored to prevent the accuracy paradox, i.e., a situation in which a predictive model with a given level of accuracy may have greater predictive power than models with high accuracy. These metrics were often used to evaluate statistical methods and methods based on machine learning, that we surveyed in the literature review. To sum up, even though many surveyed papers use similar metrics, they are hardly comparable due different works going into different levels of details or using less formal definitions of prediction accuracy.

Time criteria were used for evaluation of attack prediction methods by Kholidy *et al.*, who measured the time difference between the prediction and the predicted attack [38]–[40]. Thus, it is possible to estimate when is the attack going to appear and how much time there is to prepare an appropriate defense. On the one hand, the time delay between individual attack steps can be inferred from the history of attacks in most of the attack prediction methods. On the other hand, the time criterion may be used as an indicator of the practical usability of a prediction method. Thus, the time criterion should be considered especially by practitioners who require some time to react to a prediction.

E. Open and Resolved Problems

In the introduction and the literature survey in Sections IV–VII, we have mentioned a number of problems associated with attack prediction and forecasting. Many of these problems were common to multiple attack prediction methods. For example, if a method depends on an attack model, the model has to be created and maintained. Similarly, if a security situation is formally represented, there is a need to consider all the factors contributing to it, which is not always straightforward. Here we recapitulate minor problems which were successfully approached and which remain open.

An example of a successfully resolved problem is the generation and maintenance of attack models or attack plan libraries. The first attack prediction methods depended on attack plan libraries that had to be populated by human experts. It was tedious to formally represent all the possible attack paths and if so, the model parameters, such as transition probabilities in graph models, were hard to accurately be obtained. Often, a model library built upon historical records were proposed, which enabled realistic model parameters but still required laborious manual work by experts. However, the introduction of data mining into the cyber security domain created a breakthrough for attack predictions. Using data mining, an attack plan library can be constructed automatically and continuously updated. Data mining became especially popular for constructing graph-based models, for example [14], [15], [32], [37]. Data mining closely relates to machine learning, which became another popular method to attack prediction. Machine learning-supported methods do not need an external model as they construct their own internal representation of cyber security events and predictive rules during the learning phase. However, human experts still play a vital role in constructing attack models and consulting the results [88]. Further, a current research trend is using deep machine learning, which has not been observed in the surveyed literature yet. We expect to see deep learning-based prediction methods in cyber security in the near future.

Although the problems outlined earlier in this section have been resolved, many other issues remain. The major issue is how can prediction methods react to new trends in cyber security, e.g., novel attack vectors and security paradigms. Even though we cannot effectively predict 0-day attacks, its attack progression is typically similar to some of the known attacks, thus making the actual attack predictable to some extent. However, how can we react to paradigm shifts and novel attack vectors that arose with the development of the Internet of Things (IoT), cyber-physical systems, software-defined networking (SDN), and other current trends? Indeed, the first attempts to predict attacks in these novel paradigms have already been proposed [34], [96]. Nevertheless, it is definitely interesting to see how we can adapt the general methods to work under emerging paradigms in networking and security.

IX. Conclusion & Outlook

In this paper, we presented a literature survey of attack prediction methods. The problem was set in a context of research on intrusion detection and cyber situational awareness. A taxonomy of methods was provided, and each category was described in detail and evaluated. The final evaluation compared the methods and discussed related problems and lessons learned. Herein, we conclude our findings on the theory and practice of attack prediction and suggest future events in the field.

Three important findings emerged from the literature review. First, many of the prediction methods in cyber security are using a model to represent and project the future state of an attack or a security situation. Although there is an apparent division of the models given by their use case (attack projection more often uses discrete models, while forecasting network security situation uses continuous models predominantly), the two main use cases often complement each other and overlap in many cases. Second, we have seen many new approaches based on data mining and machine learning, which substantially change the state of the research in cyber security predictions. Data mining resolves the dependence on artificially provided prediction models, while machine learning challenges the model-based approaches in general. Finally, we have encountered many problems related to the evaluation of predictions in cyber security. In the context of empirical datasets, popular datasets are old, unreliable, and created for other purposes, while evaluations in live networks are not reproducible. We do not even have a common set of metrics to compare the methods.

In the future, we are likely going to see further improvements of attack prediction and its utilization in practice. Keeping in mind that attack prediction is one step behind intrusion detection, we outline a few directions in which the research will be held. First, a transition in processing the network data and alerts from batches to stream data processing has already started, and we may expect further utilization of Big Data analytics [109], [119]. Second, in the near future, we are going to see research on attack prediction in a collaborative environment, such as collaborative intrusion detection systems or alert sharing platforms. Predicting attacks in such an environment is a natural next step of the research in this area [86], [120]. Finally, we are going to see more and more data mining and machine learning in cyber security [89] and the attack prediction is no exception. Specifically, we will know better if machine learning alone can be used to learn about the attacks and predict them at the same time, or if data mining and machine learning will be used only to learn about the attacks and the prediction will still use pattern matching.

To conclude this paper, the issue of attack prediction is an interesting research problem that has been approached many times by a number of researchers. Although many solutions have been proposed, there is still no definite answer on how to effectively and precisely predict cyber attacks. Attack prediction is not yet used in practice and sometimes seen as rather misleading [121], but it is still an open and an imperative, desirable research problem [1], [3], [120].

References

[1] A. Kott, *Towards Fundamental Science of Cyber Security*. New York, NY, USA: Springer, 2014, pp. 1–13.

[2] A. A. Ramaki and R. E. Atani, "A survey of IT early warning systems: Architectures, challenges, and solutions," *Security Commun. Netw.*, vol. 9, no. 17, pp. 4751–4776, 2016.

[3] S. J. Yang, H. Du, J. Holsopple, and M. Sudit, *Attack Projection*. Cham, Switzerland: Springer Int., 2014, pp. 239–261.

[4] A. A. Ahmed and N. A. K. Zaman, "Attack intention recognition: A review," *IJ Netw. Security*, vol. 19, no. 2, pp. 244–250, 2017.

[5] M. Abdlhamed, K. Kifayat, Q. Shi, and W. Hurst, *Intrusion Prediction Systems*. Cham, Switzerland: Springer Int., 2017, pp. 155–174.

[6] Y.-B. Leau and S. Manickam, *Network Security Situation Prediction: A Review and Discussion*. Heidelberg, Germany: Springer, 2015, pp. 424–435.

[7] X. Wei and X. Jiang, "Comprehensive analysis of network security situational awareness methods and models," in *Proc. IEEE 2nd Int. Symp. Instrum. Meas. Sensor Netw. Autom. (IMSNA)*, 2013, pp. 176–179.

[8] I. A. Gheyas and A. E. Abdallah, "Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis," *Big Data Anal.*, vol. 1, no. 1, p. 6, Aug. 2016.

[9] M. Abdlhamed, K. Kifayat, Q. Shi, and W. Hurst, "A system for intrusion prediction in cloud computing," in *Proc. Int. Conf. Internet Things Cloud Comput.*, Cambridge, U.K., 2016, pp. 1–35.

[10] C. W. Geib and R. P. Goldman, "Plan recognition in intrusion detection systems," in *Proc. DARPA Inf. Survivability Conf. Exp. II (DISCEX)*, vol. 1, 2001, pp. 46–55.

[11] T. Hughes and O. Sheyner, "Attack scenario graphs for computer network threat analysis and prediction," *Complexity*, vol. 9, no. 2, pp. 15–18, 2003.

[12] X. Qin and W. Lee, "Attack plan recognition and prediction using causal networks," in *Proc. 20th Annu. Comput. Security Appl. Conf.*, Dec. 2004, pp. 370–379.

[13] E. Bou-Harb, M. Debbabi, and C. Assi, "Cyber scanning: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1496–1519, 3rd Quart., 2014.

[14] Z.-T. Li, J. Lei, L. Wang, and D. Li, "A data mining approach to generating network attack graph for intrusion prediction," in *Proc. 4th Int. Conf. Fuzzy Syst. Knowl. Disc. (FSKD)*, vol. 4, Aug. 2007, pp. 307–311.

[15] H. Farhadi, M. AmirHaeri, and M. Khansari, "Alert correlation and prediction using data mining and HMM," *ISeCure*, vol. 3, no. 2, pp. 77–101, 2011.

[16] A. Hernández *et al.*, "Security attack prediction based on user sentiment analysis of Twitter data," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Mar. 2016, pp. 610–617.

[17] K. Shu, A. Sliva, J. Sampson, and H. Liu, "Understanding cyber attack behaviors with sentiment information on social media," in *Social, Cultural, and Behavioral Modeling*. Cham, Switzerland: Springer Int., 2018, pp. 377–388.

[18] P. Shao, J. Lu, R. K. Wong, and W. Yang, "A transparent learning approach for attack prediction based on user behavior analysis," in *Information and Communications Security*. Cham, Switzerland: Springer Int., 2016, pp. 159–172.

[19] M. R. Endsley, "Situation awareness global assessment technique (SAGAT)," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, 1988, pp. 789–795.

[20] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[21] A. Kott, C. Wang, and R. F. Erbacher, *Cyber Defense and Situational Awareness*, vol. 62. Cham, Switzerland: Springer, 2014.

[22] C.-J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, "NICE: Network intrusion detection and countermeasure selection in virtual network systems," *IEEE Trans. Depend. Secure Comput.*, vol. 10, no. 4, pp. 198–211, Jul./Aug. 2013.

[23] I. Kotenko and A. Chechulin, "A cyber attack modeling and impact assessment framework," in *Proc. 5th Int. Conf. Cyber Conflict (CYCON)*, Jun. 2013, pp. 1–24.

[24] P. Cao, K.-W. Chung, Z. Kalbarczyk, R. Iyer, and A. J. Slagell, "Preemptive intrusion detection," in *Proc. Symp. Bootcamp Sci. Security*, Raleigh, NC, USA, 2014, pp. 1–21.

[25] P. Cao, E. Badger, Z. Kalbarczyk, R. Iyer, and A. Slagell, "Preemptive intrusion detection: Theoretical framework and real-world measurements," in *Proc. Symp. Bootcamp Sci. Security*, Urbana, IL, USA, 2015, pp. 1–5.

[26] A. A. Ramaki, M. Amini, and R. E. Atani, "RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection," *Comput. Security*, vol. 49, pp. 206–219, Mar. 2015.

[27] M. GhasemiGol, A. Ghaemi-Bafghi, and H. Takabi, "A comprehensive approach for network attack forecasting," *Comput. Security*, vol. 58, pp. 83–105, May 2016.

[28] M. GhasemiGol, H. Takabi, and A. Ghaemi-Bafghi, "A foresight model for intrusion response management," *Comput. Security*, vol. 62, pp. 73–94, Sep. 2016.

[29] N. Polatidis, E. Pimenidis, M. Pavlidis, and H. Mouratidis, "Recommender systems meeting security: From product recommendation to cyber-attack prediction," in *Engineering Applications of Neural Networks*. Cham, Switzerland: Springer Int., 2017, pp. 508–519.

[30] N. Polatidis, E. Pimenidis, M. Pavlidis, S. Papastergiou, and H. Mouratidis, "From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks," in *Evolving Systems*. Heidelberg, Germany: Springer, May 2018.

[31] J. Wu, L. Yin, and Y. Guo, "Cyber attacks prediction model based on Bayesian network," in *Proc. IEEE 18th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2012, pp. 730–731.

[32] A. A. Ramaki, M. Khosravi-Farmad, and A. G. Bafghi, "Real time alert correlation and prediction using Bayesian networks," in *Proc. IEEE 12th Int. Iran. Soc. Cryptol. Conf. Inf. Security Cryptol. (ISCISC)*, 2015, pp. 98–103.

[33] A. Okutan, S. J. Yang, and K. McConky, "Predicting cyber attacks with Bayesian networks using unconventional signals," in *Proc. 12th Annu. Conf. Cyber Inf. Security Res.*, 2017, pp. 1–13.

[34] K. Huang, C. Zhou, Y.-C. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 8153–8162, Oct. 2018.

[35] A. S. Sendi, M. Dagenais, M. Jabbarifar, and M. Couture, "Real time intrusion prediction based on optimized alerts with hidden Markov model," *J. Netw.*, vol. 7, no. 2, pp. 311–321, 2012.

[36] S. Shin, S. Lee, H. Kim, and S. Kim, "Advanced probabilistic approach for network intrusion forecasting and detection," *Expert Syst. Appl.*, vol. 40, no. 1, pp. 315–322, 2013.

[37] Y. Zhang, D. Zhao, and J. Liu, "The application of Baum–Welch algorithm in multistep attack," *Sci. World J.*, vol. 2014, May 2014, Art. no. 374260.

[38] H. A. Kholidy, A. Erradi, and S. Abdelwahed, "Attack prediction models for cloud intrusion detection systems," in *Proc. 2nd Int. Conf. Artif. Intell. Model. Simulat. (AIMS)*, Nov. 2014, pp. 270–275.

[39] H. A. Kholidy, A. Erradi, S. Abdelwahed, and A. Azab, "A finite state hidden Markov model for predicting multistage attacks in cloud systems," in *Proc. IEEE 12th Int. Conf. Depend. Auton. Secure Comput. (DASC)*, Aug. 2014, pp. 14–19.

[40] H. A. Kholidy, A. M. Yousof, A. Erradi, S. Abdelwahed, and H. A. Ali, "A finite context intrusion prediction model for cloud systems with a probabilistic suffix tree," in *Proc. Eur. Model. Symp. (EMS)*, Oct. 2014, pp. 526–531.

[41] S. Abraham and S. Nair, "Exploitability analysis using predictive cybersecurity framework," in *Proc. IEEE 2nd Int. Conf. Cybern. (CYBCONF)*, Jun. 2015, pp. 317–323.

[42] A. Bar, B. Shapira, L. Rokach, and M. Unger, "Identifying attack propagation patterns in honeypots using Markov chains modeling and complex networks analysis," in *Proc. IEEE Int. Conf. Softw. Sci. Technol. Eng. (SWSTE)*, 2016, pp. 28–36.

[43] A. Bar, B. Shapira, L. Rokach, and M. Unger, "Scalable attack propagation model and algorithms for honeypot systems," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2016, pp. 1130–1135.

[44] V. Lisý, R. Píbil, J. Stiborek, B. Bosanský, and M. Pechoucek, "Game-theoretic approach to adversarial plan recognition," in *Proc. ECAI*, 2012, pp. 546–551.

[45] R. Píbil, V. Lisý, C. Kiekintveld, B. Bošanský, and M. Pěchouček, "Game theoretic model of strategic honeypot selection in computer networks," in *Decision and Game Theory for Security*. Heidelberg, Germany: Springer, 2012, pp. 201–220.

[46] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proc. Workshop New Security Paradigms*, Charlottesville, VA, USA, 1998, pp. 71–79.

[47] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proc. IEEE Symp. Security Privacy*, 2002, pp. 273–284.

[48] H. Debar and A. Wespi, "Aggregation and correlation of intrusion-detection alerts," in *Proc. Int. Workshop Recent Adv. Intrusion Detect.*, 2001, pp. 85–103.

[49] N. Polatidis and C. K. Georgiadis, "A multi-level collaborative filtering method that improves recommendations," *Expert Syst. Appl.*, vol. 48, pp. 100–110, Apr. 2016.

[50] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using Bayesian attack graphs," *IEEE Trans. Depend. Secure Comput.*, vol. 9, no. 1, pp. 61–74, Jan./Feb. 2012.

[51] P. Passeri. (2017). *Hackmageddon Information Security Timelines and Statistics*. Accessed: Sep. 5, 2018. [Online]. Available: http://www.hackmageddon.com/

[52] J. Nash, "Non-cooperative games," *Ann. Math.*, vol. 54, no. 2, pp. 286–295, 1951.

[53] V. Conitzer and T. Sandholm, "Complexity results about Nash equilibria," in *Proc. 18th Int. Joint Conf. Artif. Intell.*, Acapulco, Mexico, 2003, pp. 765–771.

[54] S. C. Kontogiannis and P. G. Spirakis, "Well supported approximate equilibria in bimatrix games," *Algorithmica*, vol. 57, no. 4, pp. 653–667, 2010.

[55] H. Tsaknakis and P. G. Spirakis, "An optimization approach for approximate Nash equilibria," *Internet and Network Economics*. Heidelberg, Germany: Springer, 2007, pp. 42–56.

[56] H. Park, S.-O. D. Jung, H. Lee, and H. P. In, "Cyber weather forecasting: Forecasting unknown Internet worms using randomness analysis," in *Information Security and Privacy Research*. Heidelberg, Germany: Springer, 2012, pp. 376–387.

[57] Z. Zhan, M. Xu, and S. Xu, "Characterizing honeypot-captured cyber attacks: Statistical framework and case study," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1775–1789, Nov. 2013.

[58] A. Silva, E. Pontes, F. Zhou, A. Guelf, and S. Kofuji, "PRBS/EWMA based model for predicting burst attacks (Brute Froce, DoS) in computer networks," in *Proc. 9th Int. Conf. Digit. Inf. Manag. (ICDIM 2014)*, Sep./Oct. 2014, pp. 194–200.

[59] A. B. Abdullah, T. R. Pillai, and L. Z. Cai, "Intrusion detection forecasting using time series for improving cyber defence," *Int. J. Intell. Syst. Appl. Eng.*, vol. 3, no. 1, pp. 28–33, 2015.

[60] T. R. Pillai, S. Palaniappan, A. Abdullah, and H. M. Imran, "Predictive modeling for intrusions in communication systems using GARMA and ARMA models," in *Proc. 5th Nat. Symp. Inf. Technol. Towards New Smart World (NSITNSW)*, Feb. 2015, pp. 1–6.

[61] J. Freudiger, E. De Cristofaro, and A. E. Brito, *Controlled Data Sharing for Collaborative Predictive Blacklisting*. Cham, Switzerland: Springer Int., 2015, pp. 327–349.

[62] Y.-Z. Chen, Z.-G. Huang, S. Xu, and Y.-C. Lai, "Spatiotemporal patterns and predictability of cyberattacks," *PLoS ONE*, vol. 10, no. 6, Jun. 2015, Art. no. e0131501.

[63] Z. Zhan, M. Xu, and S. Xu, "Predicting cyber attack rates with extreme values," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1666–1677, Aug. 2015.

[64] P. Sokol and A. Gajdoš, *Prediction of Attacks Against Honeynet Based on Time Series Modeling*. Cham, Switzerland: Springer Int., 2018, pp. 360–371.

[65] G. Werner, S. Yang, and K. McConky, "Time series forecasting of cyber attack intensity," in *Proc. 12th Annu. Conf. Cyber Inf. Security Res.*, Oak Ridge, TN, USA, 2017, pp. 1–18.

[66] S. Dowling, M. Schukat, and H. Melvin, "Using analysis of temporal variances within a honeypot dataset to better predict attack type probability," in *Proc. 12th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2017, pp. 349–354.

[67] A. Okutan, G. Werner, K. McConky, and S. J. Yang, "POSTER: Cyber attack prediction of threats from unconventional resources (CAPTURE)," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, Dallas, TX, USA, 2017, pp. 2563–2565.

[68] Z. Lin, L. Xiujie, M. Jing, S. Wenchang, and W. Xiufang, "The prediction algorithm of network security situation based on Grey correlation entropy Kalman filtering," in *Proc. IEEE 7th Joint Int. Inf. Technol. Artif. Intell. Conf. (ITAIC)*, Dec. 2014, pp. 321–324.

[69] Y.-B. Leau and S. Manickam, "A novel adaptive Grey Verhulst model for network security situation prediction," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, pp. 90–95, 2016.

[70] Y.-B. Leau and S. Manickam, "An enhanced adaptive Grey Verhulst prediction model for network security situation," *Int. J. Comput. Sci. Netw. Security (IJCSNS)*, vol. 16, no. 5, pp. 13–20, 2016.

[71] Y. Liu *et al.*, "Cloudy with a chance of breach: Forecasting cyber security incidents," in *Proc. USENIX Security Symp.*, Washington, DC, USA, 2015, pp. 1009–1024.

[72] D. Ju-Long, "Control problems of Grey systems," *Syst. Control Lett.*, vol. 1, no. 5, pp. 288–294, 1982.

[73] F.-S. Zhang, F. Liu, W.-B. Zhao, Z.-A. Sun, and G.-Y. Jiang, "Application of Grey Verhulst model in middle and long term load forecasting," *Power Syst. Technol.*, vol. 5, pp. 37–40, 2003.

[74] R. Zheng, D. Zhang, Q. Wu, M. Zhang, and C. Yang, "A strategy of network security situation autonomic awareness," in *Network Computing and Information Security*. Heidelberg, Germany: Springer, 2012, pp. 632–639.

[75] F. Chen, Y. Shen, G. Zhang, and X. Liu, "The network security situation predicting technology based on the small-world echo state network," in *Proc. 4th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, 2013, pp. 377–380.

[76] Y. Zhang, S. Jin, X. Cui, X. Yin, and Y. Pang, *Network Security Situation Prediction Based on BP and RBF Neural Network*. Heidelberg, Germany: Springer, 2013, pp. 659–665.

[77] W. Xing-Zhu, "Network intrusion prediction model based on RBF features classification," *Int. J. Security Appl.*, vol. 10, no. 4, pp. 241–248, 2016.

[78] H. Zhang, Q. Huang, F. Li, and J. Zhu, "A network security situation prediction model based on wavelet neural network with optimized parameters," *Digit. Commun. Netw.*, vol. 2, no. 3, pp. 139–144, 2016.

[79] F. He *et al.*, "Mixed wavelet-based neural network model for cyber security situation prediction using MODWT and Hurst exponent analysis," in *Network and System Security*. Cham, Switzerland: Springer Int., 2017, pp. 99–111.

[80] X. Cheng and S. Lang, "Research on network security situation assessment and prediction," in *Proc. 4th Int. Conf. Comput. Inf. Sci. (ICCIS)*, 2012, pp. 864–867.

[81] G. K. Jayasinghe, J. S. Culpepper, and P. Bertok, "Efficient and effective realtime prediction of drive-by download attacks," *J. Netw. Comput. Appl.*, vol. 38, pp. 135–149, Feb. 2014.

[82] S. O. Uwagbole, W. J. Buchanan, and L. Fan, "Applied machine learning predictive analytics to SQL injection attack detection and prevention," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, May 2017, pp. 1087–1090.

[83] S. O. Uwagbole, W. J. Buchanan, and L. Fan, "An applied pattern-driven corpus to predictive analytics in mitigating SQL injection attack," in *Proc. 7th Int. Conf. Emerg. Security Technol. (EST)*, Sep. 2017, pp. 12–17.

[84] C. Fachkha *et al.*, "Investigating the dark cyberspace: Profiling, threat-based analysis and correlation," in *Proc. 7th Int. Conf. Risks Security Internet Syst. (CRiSIS)*, Oct. 2012, pp. 1–8.

[85] Y.-H. Kim and W. H. Park, "A study on cyber threat prediction based on intrusion detection event for APT attack detection," *Multimedia Tools Appl.*, vol. 71, no. 2, pp. 685–698, Jul. 2014.

[86] M. Husák and J. Kašpar, "Towards predicting cyber attacks using information exchange and data mining," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 536–541.

[87] K. Soska and N. Christin, "Automatically detecting vulnerable websites before they turn malicious," in *Proc. USENIX Security Symp.*, 2014, pp. 625–640.

[88] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, and K. Li, "AI^2: Training a big data machine to defend," in *Proc. IEEE 2nd Int. Conf. Big Data Security Cloud (BigDataSecurity) IEEE Int. Conf. High Perform. Smart Comput. (HPSC) IEEE Int. Conf. Intell. Data Security (IDS)*, New York, NY, USA, Apr. 2016, pp. 49–54.

[89] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.

[90] J.-B. Lai *et al.*, "WNN-based network security situation quantitative prediction method and its optimization," *J. Comput. Sci. Technol.*, vol. 23, no. 2, pp. 222–230, 2008.

[91] A. Jantan, M. Rasmi, M. I. Ibrahim, and A. H. A. Rahman, *A Similarity Model to Estimate Attack Strategy Based on Intentions Analysis for Network Forensics*. Heidelberg, Germany: Springer, 2012, pp. 336–346.

[92] M. Rasmi and A. Jantan, "A new algorithm to estimate the similarity between the intentions of the cyber crimes for network forensics," *Procedia Technol.*, vol. 11, pp. 540–547, 2013.

[93] A. AlEroud and G. Karabatis, "Context infusion in semantic link networks to detect cyber-attacks: A flow-based detection approach," in *Proc. IEEE Int. Conf. Semantic Comput.*, Jun. 2014, pp. 175–182.

[94] A. AlEroud and G. Karabatis, "Methods and techniques to identify security incidents using domain knowledge and contextual information," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, May 2017, pp. 1040–1045.

[95] C.-B. Jiang, I.-H. Liu, Y.-N. Chung, and J.-S. Li, "Novel intrusion prediction mechanism based on honeypot log similarity," *Int. J. Netw. Manag.*, vol. 26, on. 3, pp. 156–175, 2016.

[96] A. AlEroud and I. Alsmadi, "Identifying cyber-attacks on software defined networks: An inference-based intrusion detection approach," *J. Netw. Comput. Appl.*, vol. 80, pp. 152–164, Feb. 2017.

[97] D. Kwon, J. W.-K. Hong, and H. Ju, "DDoS attack forecasting system architecture using Honeynet," in *Proc. 14th Asia–Pac. Netw. Oper. Manag. Symp. (APNOMS)*, Sep. 2012, pp. 1–4.

[98] D. Kwon, H. Kim, D. An, and H. Ju, "DDoS attack volume forecasting using a statistical approach," in *Proc. TODO*, 2017, pp. 1083–1086.

[99] C. Fachkha, E. Bou-Harb, and M. Debbabi, "Towards a forecasting model for distributed denial of service activities," in *Proc. 12th IEEE Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, Aug. 2013, pp. 110–117.

[100] A. Olabelurin, S. Veluru, A. Healing, and M. Rajarajan, "Entropy clustering approach for improving forecasting in DDoS attacks," in *Proc. IEEE 12th Int. Conf. Netw. Sens. Control (ICNSC)*, Apr. 2015, pp. 315–320.

[101] G.-Y. Hu *et al.*, "A method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm," *Appl. Soft Comput.*, vol. 48, pp. 404–418, Nov. 2016.

[102] G.-Y. Hu and P.-L. Qiao, "Cloud belief rule base model for network security situation prediction," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 914–917, May 2016.

[103] H. Wei *et al.*, "A new BRB model for cloud security-state prediction based on the large-scale monitoring data," *IEEE Access*, vol. 6, pp. 11907–11920, 2017.

[104] D. Mahjoub and T. Mathew. (Nov. 2015). *SPRank and IP Space Monitoring at BruCON & Hack.lu*. Accessed: Sep. 5, 2018. [Online]. Available: https://umbrella.cisco.com/blog/2015/11/19/sprank-and-ip-space-monitoring/

[105] A. Dalton, B. Dorr, L. Liang, and K. Hollingshead, "Improving cyber-attack predictions through information foraging," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Boston, MA, USA, Dec. 2017, pp. 4642–4647.

[106] M. Rasmi and A. Jantan, *Attack Intention Analysis Model for Network Forensics*. Heidelberg, Germany: Springer, 2011, pp. 403–411.

[107] H. Wei *et al.*, "A new BRB model for security-state assessment of cloud computing based on the impact of external and internal environments," *Comput. Security*, vol. 73, pp. 207–218, Mar. 2018.

[108] H. T. Elshoush and I. M. Osman, "Alert correlation in collaborative intelligent intrusion detection systems—A survey," *Appl. Soft Comput.*, vol. 11, no. 7, pp. 4349–4365, 2011.

[109] S. Suthaharan, "Big data classification: Problems and challenges in network intrusion prediction with machine learning," *SIGMETRICS Perform. Eval. Rev.*, vol. 41, no. 4, pp. 70–73, Apr. 2014.

[110] R. P. Lippmann *et al.*, "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation," in *Proc. DARPA Inf. Survivability Conf. Expo. (DISCEX)*, vol. 2, 2000, pp. 12–26.

[111] *DARPA Intrusion Detection Data Sets*, MIT Lincoln Lab., Lexington, MA, USA. Accessed: Sep. 5, 2018. [Online]. Available: https://www.ll.mit.edu/ideval/data/

[112] The UCI KDD Archive. (Oct. 1999). *KDD Cup 1999 Data*. Accessed: Sep. 5, 2018. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[113] M. V. Mahoney and P. K. Chan, "An analysis of the 1999 DARPA/Lincoln Laboratory evaluation data for network anomaly detection," in *Recent Advances in Intrusion Detection*. Heidelberg, Germany: Springer, 2003, pp. 220–237.

[114] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Security Defense Appl.*, Ottawa, ON, Canada, Jul. 2009, pp. 1–6.

[115] D. S. Fava, S. R. Byers, and S. J. Yang, "Projecting cyberattacks through variable-length Markov models," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 359–369, Sep. 2008.

[116] SANS. (2017). *DShield: Internet Storm Center*. Accessed: Sep. 5, 2018. [Online]. Available: https://www.dshield.org/

[117] M. Albanese, E. Battista, S. Jajodia, and V. Casola, "Manipulating the attacker's view of a system's attack surface," in *Proc. IEEE Conf. Commun. Netwo. Security*, San Francisco, CA, USA, Oct. 2014, pp. 472–480.

[118] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, 2013, pp. 413–424.

[119] A. Kott, A. Swami, and P. McDaniel, "Security outlook: Six cyber game changers for the next 15 years," *Computer*, vol. 47, no. 12, pp. 104–106, Dec. 2014.
[120] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," *ACM Comput. Surveys*, vol. 47, no. 4, pp. 1–55, May 2015.
[121] A. Chuvakin. (Mar. 2016). *Sad Hilarity of Predictive Analytics in Security?* Accessed: Sep. 5, 2018. [Online]. Available: http://blogs.gartner.com/anton-chuvakin/2016/03/31/sad-hilarity-of-predictive-analytics-in-security/

Martin Husák is currently pursuing the Ph.D. degree in computer systems and technology with the Faculty of Informatics, Masaryk University, where he is a Researcher with the Institute of Computer Science, a member of the University's Security Team (CSIRT-MU), and a contributor to the Honeynet Project. Recently, he was also a Visiting Researcher with Florida Atlantic University. His thesis addresses the problem of early detection and prediction of network attacks using information sharing. His research interests are related to cyber situational awareness and threat intelligence with a special focus on the effective sharing of data from honeypots and network monitoring.

Jana Komárková is currently pursuing the Ph.D. degree in computer systems and technology with the Faculty of Informatics, Masaryk University, with the thesis on decision support in network defense, where she is a Researcher with the Institute of Computer Science and a member of the University's Security TEAM (CSIRT-MU). Her main research interests are cyber defense, attack impact assessment, attack mitigation, and cyber situational awareness.

Elias Bou-Harb is currently an Assistant Professor at the computer science department at Florida Atlantic University. Previously, he was a visiting research scientist at Carnegie Mellon University. Elias is also a research scientist at the National Cyber Forensic and Training Alliance (NCFTA) of Canada. Elias holds a Ph.D. degree in computer science from Concordia University, Montreal, Canada. His research and development activities and interests focus on the broad area of operational cyber security, including, attacks detection and characterization, Internet measurement, cyber security for critical infrastructure and mobile network security.

Pavel Čeleda received the Ph.D. degree in informatics from the University of Defence, Brno, Czech Republic. He is an Associate Professor with Masaryk University. His main research interests include cyber security, flow monitoring, situational awareness, and research and development of network security devices. He has been participating in a number of academic, industrial, and defense projects. He is a Principal Investigator of the KYPO cyber range project and a Co-PI of the CyberSecurity, CyberCrime, and Critical Information Infrastructures Center of Excellence (C4e). He is a head of CSIRT-MU.